Robust ECC-based Three-factors Authentication and Key Agreement for Smart Home

Xiaoming Huang[1,2], Tao Zhang[3], Wenying Zheng[4], Huijie Yang[3], Yunpeng Song[5]*

[1] School of Computer Science and Engineering,
University of Electronic Science and Technology of China, China
[2] Chengdu Rongwei Software Service Co., Ltd., China
[3] School of Information Science and Engineering, Zhejiang Sci-Tech University, China
[4] School of Computer Science and Technology, Zhejiang Sci-Tech University, China
[5] Industry Development Center of Zhejiang Province, China
apride@gmail.com, tzhang1704@126.com, zhengwy0501@126.com, hjyang03@126.com, 33256491@qq.com

Abstract

With the deep exploration into artificial intelligence (AI) technology, smart home has become a major development trend. Authentication and key agreement (AKA) protocols are widely used in smart home for communication between users and devices as an important means to protect communication security. However, traditional AKA protocols cannot meet the needs of smart home environments in terms of both security and overhead. To reduce the cost of deploying AI-based devices, a practical ECC-based AKA protocol is proposed, which can achieve secure authentication among users, gateway nodes and AI-based devices and generate session key. Moreover, biometrics are implanted through specific devices and adopted as an authentication factor to resist password leakage attack. The security is proven by using Real-Or-Random (ROR) along with informal security analysis. Furthermore, the widely accepted AVISPA is used to verify whether the protocol can resist active attacks. Finally, experimental simulations are completed between the proposed protocol and the related works the results show that ours keeps a balance in security and performance.

Keywords: Internet of Things, Replay attack, Key agreement, Session key

1 Introduction

Recently, the rise of artificial intelligence [1] is changing the way people live and work, smart home is gradually coming into the limelight. The concept of a smart home intertwines diverse AI-powered devices [2] within households using IoT technology. This integration offers a plethora of functionalities and utilities, ranging from controlling home appliances to facilitating anti-theft alarms and environmental monitoring. Different from the traditional way of living, smart home provides a wide range of information interaction. The information interaction of smart devices changes people's lifestyles while bringing challenges in information security between users and devices.

In actuality, there are multiple passive and active attacks [3] between communication of users and devices. These attacks bring significant challenges to secure communications. Eavesdropping attacks [4] can cause information transmitted on public channels to be accessed by malicious adversaries to analyze sensitive information. Man-in-the-middle attacks [5] cause messages transmitted on public channels to be intercepted by malicious adversaries and forged messages sent to entities. In addition to the above attacks, there are various other attacks (e.g., replay attacks, capture attacks, etc.). At present, authentication and key agreement (AKA) is widely used for multiparty authentication and secure communication in smart home. The identifier and password are used as authentication factors to verify the user's legitimacy. However, there are instances where users' identifiers and passwords have been compromised. This will result in malicious users being able to access IoT devices in smart home and thus compromise sensitive information. Therefore, design a secure AKA will protect smart home communication security.

Ensuring the security of users and smart homes is a paramount concern in contemporary technological landscapes. Users are increasingly required to employ a diverse range of authentication factors, transcending traditional identifiers and passwords, to access smart home systems. This multifaceted approach serves to mitigate the inherent risks associated with compromising user secrets and upholds the imperative of preserving privacy. Biometrics emerges as a pivotal authentication factor in this context, harnessing distinctive user characteristics to effectively counteract password guessing attacks. By leveraging these inherent biological or behavioral traits, the authentication process attains a heightened level of security, enhancing the robustness of smart home access mechanisms. In the realm of information transmission between users and devices, particularly across public channels, the AKA protocol [6] assumes a critical role.

*Corresponding Author: Yunpeng Song; Email: 33256491@qq.com
DOI: https://doi.org/10.70003/160792642025072604008

This protocol is strategically designed to proactively address and mitigate potential information leakage on these public channels. Its meticulous implementation serves as a safeguard against unauthorized access and reinforces the overall security posture of smart home systems. Furthermore, the establishment and nurturing of trust between users and AI-based devices necessitate the deployment of comprehensive multiparty authentication protocols. This sophisticated authentication process culminates in the generation of a secure key. The resultant secure key not only fortifies the communication framework between the involved entities but also guarantees the integrity and confidentiality of data exchanges within the smart home ecosystem.

On the flip side, the integration of resource-constrained smart devices into the smart home ecosystem necessitates a nuanced approach to alleviate the overhead typically associated with conventional AKA protocols. The burgeoning popularity of lightweight devices stems from their convenience, catering to the preferences of modern consumers. This trend underscores the intrinsic challenge faced by smart home devices: their inherent limitation in executing computationally intensive operations due to constrained computational capabilities and restricted storage resources. The imperative, therefore, lies in the development and implementation of a lightweight, efficient AKA protocol tailored explicitly to accommodate the constraints imposed by resource-constrained smart devices. Such protocol optimization serves as a linchpin for propelling the trajectory of smart home technology, ensuring seamless integration and sustained advancement within this burgeoning domain. Achieving a delicate balance between stringent security requirements and resource limitations constitutes a pivotal endeavor in enabling the proliferation and sustained functionality of these resource-constrained yet indispensable smart devices within the smart home ecosystem. Resource-constrained smart devices need to be considered to reduce the overhead of traditional AKA protocols. Lightweight devices are more and more popular because of the convenience they bring to people. It means that smart home devices cannot afford expensive computing operations and have limited storage resources. Developing a lightweight and efficient AKA protocol is crucial to advancing the growth of smart home technology.

1.1 Motivations of This Paper

First, smart home systems involve users' personal privacy and security, including devices such as door locks and surveillance cameras. However, a malicious adversary can gain unauthorized access without secure authentication and the establishment of session keys. This will result in privacy leakage or loss of property of the user. Therefore, a secure AKA protocol in smart home is designed to provide authentication and data encryption protection.

Second, as the trend towards smart homes continues to grow, there is an increasing demand for efficient communication protocols that can facilitate seamless interactions between different devices within a home. However, the computing resources of AI devices deployed in smart homes are often limited due to cost, power, and space constraints. This can make it challenging to develop communication protocols that can effectively meet the needs of wireless sensor devices while still remaining lightweight and efficient. To address this challenge, there is a need to design a lightweight protocol that can enable AI-based devices to communicate with other devices in a smart home environment. Such a protocol should be able to operate efficiently within the constraints of the computing resources available in AI-based devices, while still providing the necessary functionality and performance.

Finally, it is crucial to strike a balance between security and computational overhead to successfully deploy the designed protocols in real-world scenarios. The protocol should not only prioritize security but also take into account the computational costs for both the user and device sides, to ensure that it meets the practical requirements of the AKA protocol.

1.2 Our Contributions

To solve the above problems, a robust ECC-based AKA protocol is proposed, which can achieve one-to-many authentication of users and devices and generate session key. Furthermore, user's biometric is adopted as an authentication factor. The main contributions are summarized as follows:

1) ***An ECC-based multi-party authentication protocol is proposed, which can achieve anonymous and untraceable.*** ECC technology is used to construct the authentication protocol. Complete one-to-many authentication and generate session key based on elliptic curve. Biometrics are further adopted as an authentication factor to prevent privacy leakage in two-factor authentication. More importantly, the user's identity information is protected.

2) ***Session key security is proved under the ROR model.*** This paper employs the DY threat model, endowing the adversary with formidable capabilities. Furthermore, an informal security analysis within the proposed protocol is presented. This analysis serves to illustrate that the protocol not only exhibits resilience against prevalent attacks but also guarantees the security of session keys.

3) ***The formalization tool is employed to verify the protocol's ability to resist MIMT attacks.*** To verify the security, the AVISPA tool is used to test whether the protocol can resist attacks like MITM. The test result shows that it can successfully resist replay and MITM attacks.

4) ***For security and performance, comparison of proposed protocol with related works has been done and the result shows that it has better practicality.*** The proposed protocol has undergone thorough analysis and comparison with other related works. The comparison results show that it has better usability, making it a more reliable and efficient means of authentication for smart home. Overall, the comparison analysis highlights the strengths and advantages of the proposed protocol and confirms its potential as a leading solution in a smart home environment.

2 Related Work

Multi-factor AKA is a security mechanism that uses multiple factors, such as passwords, biometrics, and hardware devices to accomplish authentication. Many protocols design approaches have emerged for multi-factor AKA, including cryptography-based, biometric-based, hardware device-based, etc. The protocol design methods mainly consider the synergy between different factors and security. Since Lamport's pioneering work on password-based authentication in 1981 [7], a multitude of studies have delved into authentication methodologies. Hammi et al. introduced an OTP-based authentication system leveraging Elliptic Curve Cryptography (ECC), where the One-Time Password (OTP) serves as a basis for generating a key enabling secure communication. The first category is commonly utilized in various two-party authentication schemes, but these methods have been limited to functioning within a single server environment. In 2013, Guo [8] introduced a two factor AKA based on the principles of chaotic theory. However, Lin et al. [9] point out that it cannot satisfy user anonymity and strong forward security. To meet the security requirements, an enhanced chaotic mapping-based AKA protocol is proposed. In 2018, Chebyshev, one-way functions and symmetric encryption and decryption were used to construct the AKA protocol in Chatterjee et al. [10]. However, the protocol was noted to be unable to meet the three-factor security. Sensitive information is compromised when two of the three factors are leaked.

In 2022, Tan et al. [11] proposed aggregate authentication mechanism which can handle exceptions. Although, it improves the security of the protocol in some aspects. However, it still does not satisfy the user's need for protocol security (e.g., anonymity). It effectively implements user access to devices in the IIoT. Although it satisfies most of the security, it does not achieve perfect forward security. In 2018, Irshad 2018 [12] proposes a chaos mapping-based authentication protocol for multi-cloud environments. However, it does not consider the three elements leakage problem, which can lead to information leakage.

At the same time, a lot of work was done on protecting data privacy. In 2021, Shen et al. [13] proposed an untraceable data sharing which achieves data privacy. In 2022, Yang et al. [14] proposed a location-based data sharing dependent on OT technology.

3 Preliminaries

In this section, the description of symbols and preliminary knowledge are given. The notation applied in this paper is illustrated in Figure 1 and fuzzy extractor technology is demonstrated as follows.

Notation	Description
Us_i	The ith user
$Auth$	Authority
$Gano$	Gateway node
$Smde_j$	The jth device
SC_i	Smartcard
$Ide_i, Paw_i, Biom_i$	Identifier,password and biometric of Us_i
$H(\cdot)$	One-way hash function
$Gene, Reco$	Functions of fuzzy extractor
$\|, \oplus$	Connection and exclusive-OR operation
Tis_1, Tis_2, Tis_3	Timestamp
ΔT	Maximum transmission delay
$\eta_i, \theta_j, \varpi_i, \xi_i, \varrho_j, \psi_j$	Random number
α	The secret value
SK	Session key

Figure 1. Notations

3.1 Fuzzy Extractor

Fuzzy extractor is a widely embraced method for extracting biological characteristics. This technique primarily comprises two functions: generation and recovery. Here are the formal definitions of these functions:

$(\sigma, \tau) = Gene(Biom)$: When the biometric $Biom$ is input, the generator function outputs a secret value σ and an auxiliary parameter τ.

$\sigma' = Reco(Biom', \tau)$: When the biometric $Biom'$ and the auxiliary parameter τ are input, the recovery function outputs the secret value σ'.

3.2 Dolev-Yao Adversary Model

The DY adversary model is commonly used to analyze protocol security. A strong adversary $\mathcal{A}$ is defined in this model, and the detailed adversary capabilities are described as follows.

1) Complete control: An adversary can intercept, modify, delay, and inject arbitrary messages and can observe the communication completely.

2) Computational Capabilities: The adversary has computational capabilities and is capable of performing arbitrarily complex computations, including decrypting encrypted data.

3) Network Capabilities: The adversary has easy access to all communications and messages in the network.

4 The Proposed Protocol

The specific construction is described in the following subsections. Each stage is structured as follows.

4.1 Registration Phase

Before users and devices joined the smart home system, they need to complete registration from the authority. Accordingly, this phase is divided into user device registration. As shown in Figure 2, the description of the registration is presented as follows.

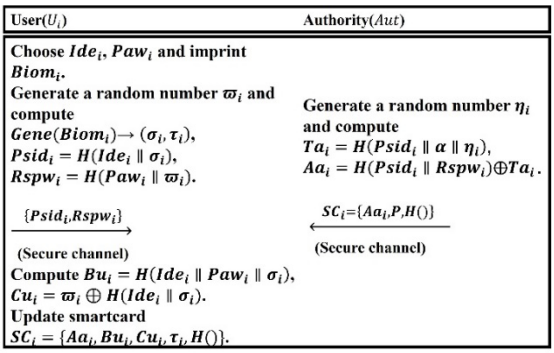

Figure 2. Registration phase

1) **User registration**: Initially, Us_i chooses Ide_i, Paw_i and implants $Biom_i$ with a special device. Then, Us_i computes $Gene(Biom_i) \rightarrow (\sigma_i, \tau_i)$, $Psid_i = H(Ide_i \| \sigma_i)$ and $Rspw_i = H(Paw_i \| \varpi_i)$, where ϖ_i is randomly generated by Us_i. After $Psid_i$ and $Rspw_i$ have been calculated, the tuple $\{Psid_i, Rspw_i\}$ is sent to *Auth* through the secure channel. Once the message from Us_i is received, *Auth* computes $Ta_i = H(Psid_i \| \alpha \| \eta_i)$ and $Aa_i = H(Psid_i \| Rspw_i) \oplus Ta_i$. Note that α is the secret value and η_i is the random number chosen by *Auth*. Then, the smartcard $SC_i = \{Aa_i, H(), P\}$ is sent to Us_i, where P is the generator. Once SC_i from *Auth* is received, Us_i computes $Bu_i = H(Ide_i \| Paw_i \| \sigma_i)$ and $Cu_i = \varpi_i \oplus H(Ide_i \| \sigma_i)$. Finally, Us_i updates $SC_i = \{Aa_i, Bu_i, Cu_i, \tau_i, H(), P\}$ when the above parameters are computed.
2) **Device registration**: For each $Smde_j$, *Auth* computes $Sa_i = H(\alpha \| \theta_j)$ and sends Sa_i to $Smde_j$ through the reliable channel. Once receiving Sd_i from *Auth*, $Smde_j$ stores Sa_i in the local database.

4.2 Login and Authentication Phase

First, Us_i reads SC_i through device and completes login. After the identity of Us_i is verified, mutual authentication is completed between Us_i, *Gano* and $Smde_j$ and *SK* is generated. As shown in Figure 3, this phase is described as follows.

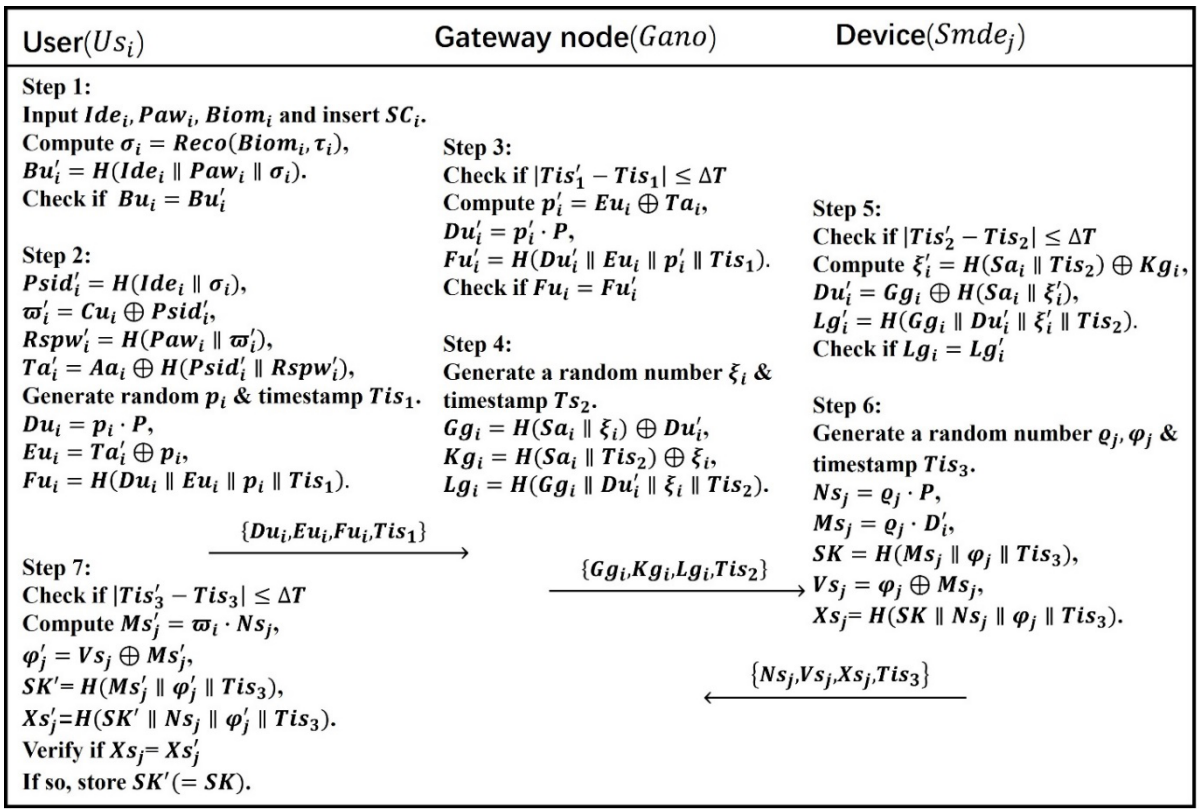

Figure 3. Login and authentication phase

S_1: First, Us_i inputs Ide_i, Paw_i, $Biom_i$ and insert SC_i. Then, Us_i computes $\sigma_i = Reco(Biom_i, \tau_i)$ and $Bu'_i = H(Ide_i \| Paw_i \| Biom_i)$. As soon as Bu'_i has been calculated, Us_i determines whether $Bu'_i = Bu_i$ holds. If it does not hold, the system interrupts.

S_2: If the above equation holds, Us_i computes $Psid'_i = H(Ide_i \| \sigma_i)$, $\varpi'_i = Cu_i \oplus Psid'_i$, $Rspw'_i = H(Paw_i \| \varpi'_i)$ and $Ta'_i = Aa_i \oplus H(Psid'_i \| Rspw'_i)$. Then, Us_i generates the random number p_i and the timestamp Tis_1. Us_i computes $Du_i = p_i \cdot P$, $Eu_i = Ta'_i \oplus p_i$ and $Fu_i = H(Du_i \| Eu_i \| p_i \| Tis_1)$. After Du_i, Eu_i and Fu_i have been computed, the tuple $\{Du_i, Eu_i, Fu_i, Tis_1\}$ is sent to *GWN* through the public channel.

S_3: Once receiving $\{Du_i, Eu_i, Fu_i, Tis_1\}$ from U_i, *Gano* verifies whether the equation $|Tis'_1 - Tis_1| \leq \Delta T$ holds. *GWN* computes $p'_i = Eu_i \oplus Ta_i$, $Du'_i = p'_i \cdot P$ and $Fu'_i = H(Du'_i \| Eu_i \| p'_i \| Tis_1)$. As soon as Fu'_i has been calculated, *Gano* determines whether $Fu'_i = Fu_i$ holds. If it does not hold, the system interrupts.

S_4: If the above equation holds, *Gano* computes $Gg_i = H(Sa_i \| \xi_i) \oplus Du'_i$, $Kg_i = H(Sa_i \| Tis_2) \oplus \xi_i$ and $Lg_i = H(Gg_i \| Kg_i \| \xi_i \| Tis_2)$, where ξ_i is the random number and Tis_2 is the timestamp. After G_i, K_i and L_i have been computed, the tuple $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ is sent to $Smde_j$ through the public channel.

S_5: Once receiving $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ from *Gano*, $Smde_j$ verifies whether the equation $|Tis'_2 - Tis_2| \le \Delta T$ holds. $Smde_j$ computes $\xi'_i = H(Sa_i \| Tis_2) \oplus Kg_i$, $Du'_i = Gg_i \oplus H(Sa_i \| \xi'_i)$ and $Lg'_i = H(Gg_i \| Du'_i \| \xi'_i \| Tis_2)$. As soon as Lg'_i has been calculated, $Smde_j$ determines whether $Lg'_i = Lg_i$ holds. If it does not materialize, the system interrupts.

S_6: If the above equation holds, $Smde_j$ computes $Ns_j = \varrho_j \cdot P$, $Ms_j = \varrho_j \cdot Du'_i$, $SK = H(Ms_j \| \varphi_j \| Tis_3)$, $Vs_j = \varphi_j \oplus Ms_j$ and $Xs_j = H(SK \| Ns_j \| \varphi_j \| Tis_3)$, where ϱ_j and φ_j are the random numbers and Tis_3 is the timestamp generated by $Smde_j$. After Ns_j, Vs_j and Xs_j have been computed, the tuple $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ is sent to Us_i through the public channel.

S_7: Once receiving $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ from $Smde_j$, Us_i verifies whether the equation $|Tis'_3 - Tis_3| \le \Delta T$ holds. Us_i computes $Ms'_j = p_j \cdot Ns_j$, $\varphi'_j = Vs_j \oplus Ms'_j$, $SK' = H(Ms'_j \| \varphi'_j \| Tis_3)$ and $Xs'_j = H(SK' \| Ns_j \| \varphi'_j \| Tis_3)$. As soon as Xs'_j has been calculated, Us_i determines whether $Xs'_j = Xs_i$ holds. If so, Us_i stores SK'.

4.3 Update Phase

In this paper, Ide_i, Paw_i, $Biom_i$ updates are considered. As shown in Figure 4, this phase is divided into 2 steps.

S_1: First, Us_i inputs Ide_i, Paw_i, $Biom_i$ and insert SC_i. Then, Us_i computes $\sigma_i = Reco(Biom_i, \tau_i)$ and $Bu'_i = H(Ide_i \| Paw_i \| \sigma_i)$. As soon as Bu'_i has been calculated, Us_i determines whether $Bu'_i = Bu_i$ holds. If it does not hold, the system interrupts. Us_i computes $Psid_i = H(Ide_i \| \sigma_i)$ and $Rspw_i = H(Paw_i \| \varpi_i)$.

S_2: U_i chooses new Ide^*_i, Paw^*_i and implants new $Biom^*_i$. Then, Us_i computes $(\sigma^*_i, \tau^*_i) = Gene(Biom^*_i)$, $Psid^*_i = H(Ide^*_i \| \sigma^*_i)$, $Rspw^*_i = H(Paw^*_i \| \varpi_i)$, $Aa^*_i = Aa_i \oplus H(Psid_i \| Rspw_i) \oplus H(Psid^*_i \| Rspw^*_i)$, $Bu^*_i = H(Ide^*_i \| Paw^*_i \| \sigma^*_i)$ and $Cu^*_i = Cu_i \oplus H(Ide_i \| \sigma_i) \oplus H(Ide^*_i \| \sigma^*_i)$. After the above parameters have been calculated, Us_i replaces Aa_i, Bu_i, Cu_i and τ_i with Aa^*_i, Bu^*_i, Cu^*_i and τ^*_i in SC_i.

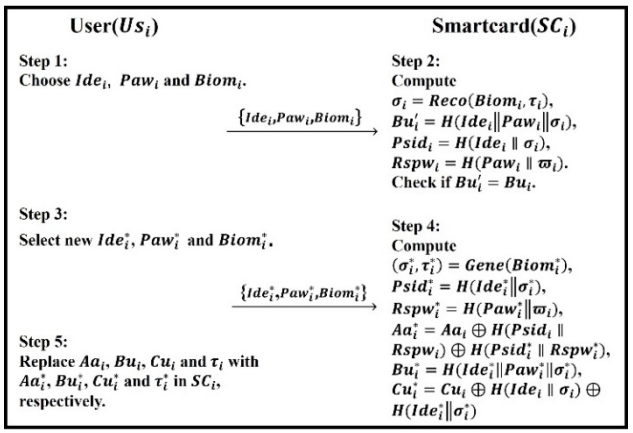

Figure 4. Update phase

5 Security Analysis

We prove the security of *SK* through ROR model and give a non-formal analysis to show that ours can resist a variety of attacks.

5.1 Formal Proof

Theorem 1: $\mathcal{A}$ corrupts the security of *SK* at the PPT time is defined as

$$Adv_{\mathcal{A}} \le \frac{q_h^2}{|H|} + \frac{q_s}{2^{l-1}|D|} + 2Adv_{\mathcal{A}}^{DL} \quad (1)$$

Proof: We prove the above theorem through games form, where $|H|$ is the size of $H()$ and $|H|$ is the size of PW_i. Every game is constructed as follows.

G_0: In $Game_0$, the initial attack will be launched and $\mathcal{A}$ will get the oracle query. Therefore, the probability of winning this game is equal to $\mathcal{A}$ successfully attacking the protocol. We can obtain the following equation.

$$Adv_{\mathcal{A}} = \left| Pr[G_0] - \frac{1}{2} \right| \quad (2)$$

G_1: There is no difference between $Game_0$ and $Game_1$, except for the results of the Oracle enquiry. In $Game_1$, the results of Oracle queries are stored in a list. The corresponding information in the list is returned when $\mathcal{A}$ initiates the query. If it does not exist in the list, a random number will be returned to $\mathcal{A}$. So, we can express this equation in the following way.

$$\Pr[G_1] = \Pr[G_0] \quad (3)$$

G_2: $\mathcal{A}$ can launch an eavesdropping attack differently from $Game_1$. This means that $\mathcal{A}$ can get the tuples $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ sent in the public channel. Then, $\mathcal{A}$ can verify through an oracle query whether output is *SK* or a random value. It is not hard to find that calculating $SK = H(Ms_j \| \varphi_j \| Tis_3)$ without Ms_j and φ_j is difficult. Note that $Ms_j = \varrho_j \cdot Du'_i$ and φ_j is the random number chosen by $Smde_j$. However, messages sent on public channels do not reveal anything about Ms_j and φ_j. So, we can express this equation in the following way.

$$\Pr[G_2] = \Pr[G_1] \quad (4)$$

$Game_3$: $\mathcal{A}$ can launch an active forgery attack differently from $Game_2$. $\mathcal{A}$ can verify collisions by accessing the H Oracle query. In order to forge the correct $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$, $\mathcal{A}$ needs to know η_i, θ_i, ϖ_i, ξ_i, ϱ_j and φ_j. Based on the birthday paradox, we can express this equation in the following way.

$$\left|Pr\left[G_3\right]-Pr\left[G_2\right]\right| \le \frac{q_h^2}{2|H|} \quad (5)$$

G_4: $\mathcal{A}$ can get the information stored in the $SC_i = \{Aa_i, Bu_i, Cu_i, \tau_i, H(), Gene(), Reco(), P\}$ by asking through the Oracle. $\mathcal{A}$ needs to obtain ϖ_i to guess the correct Paw_i, where $Aa_i = H(Psid_i \| Rspw_i) \oplus Ta_i$, $Bu_i = H(Ide_i \| Paw_i \| \sigma_i)$ and $Cu_i = \varpi_i \oplus H(Ide_i \| \sigma_i)$. If we set $\mathcal{A}$ to ask at most q_s times, the probability of $\mathcal{A}$ winning $Game_4$ is as follows.

$$\left|Pr\left[G_4\right]-Pr\left[G_3\right]\right| \le \frac{q_s}{2^l|D|} \quad (6)$$

G_5: $\mathcal{A}$ tries to compute SK by analyzing the intercepted $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ and solving the discrete logarithm problem. It means that $\mathcal{A}$ needs to obtain M_j and v_j to compute $SK = H(Ms_j \| \varphi_j \| Tis_3)$, where $Ms_j = \varrho_j \cdot Du'_i$ and $Du'_i = p'_i \cdot P$. Suppose that even if $\mathcal{A}$ obtains P to compute SK it needs to obtain ϱ_j and p_i. In other words, $\mathcal{A}$ needs to solve the DL problem to compute SK. Therefore, the probability of $\mathcal{A}$ winning G_5 is described as follows.

$$\left|Pr\left[G_5\right]-Pr\left[G_4\right]\right| \le Adv_{\mathcal{A}}^{DL} \quad (7)$$

Finally, A can get $Pr[G_5] = 1/2$ by asking through the Oracle. Theorem is proved by the change of inequality.

$$Adv_{\mathcal{A}} \le \frac{q_h^2}{|H|} + \frac{q_s}{2^{l-1}|D|} + 2Adv_{\mathcal{A}}^{DL} \quad (8)$$

5.2 Informal Analysis

5.2.1 Internal Privilege Attack

In this paper, Us_i sends $\{Psid_i, Rspw_i\}$ to $Auth$ for registration, where $Psid_i = H(Ide_i \| \sigma_i)$, $Rspw_i = H(Paw_i \| \varpi_i)$ and ϖ_i is random chosen by Us_i. Assuming that $\mathcal{A}$ is an insider attacker obtaining $\{Psid_i, Rspw_i\}$, $\mathcal{A}$ is unable to obtain any information related to Ide_i and Paw_i without the random number ϖ_i. Most importantly, we use collision-resistant H for all our calculations. As a result, internal privilege attacks can be effectively resisted.

5.2.2 Anonymity and Untraceability

As described above, information transmitted and revealed on public channels will not reveal the user's credentials. Equally, the data housed within $SC_i = \{Aa_i, Bu_i, Cu_i, \tau_i, H(), P\}$ has not revealed the user's credentials. Furthermore, $\mathcal{A}$ cannot acquire Ide_i from the intercepted $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ without η_i, θ_i, ϖ_i, ξ_i, ϱ_j and φ_j. Based on the collision resistance, $\mathcal{A}$ similarly cannot acquire obtain an Ide_i from the computed result. As a result, anonymity and untraceability can be effectively achieved.

5.2.3 Stolen Smartcard Attack

Assume that the data $\{Aa_i, Bu_i, Cu_i, \tau_i, H(), P\}$ housed within SC_i is accessed by $\mathcal{A}$ through a powerful tool, where $Aa_i = H(Psid_i \| Rspw_i) \oplus Ta_i$, $Bu_i = H(Ide_i \| Paw_i \| \sigma_i)$ and $Cu_i = \varpi_i \oplus H(Ide_i \| \sigma_i)$. Even though τ_i is acquired, $\mathcal{A}$ cannot recover σ_i without Bio_i. Moreover, both Aa_i, Bu_i and Cu_i are blinded using hashes or random numbers. Therefore, even if the data $\{Aa_i, Bu_i, Cu_i, \tau_i, H(), Gene(), Reco(), P\}$ housed within SC_i is accessed, $\mathcal{A}$ is still unable to access any valid information.

5.2.4 U_i Impersonation Attack

Assume that the tuple $\{Du_i, Eu_i, Fu_i, Tis_1\}$ sent by Us_i is acquired by $\mathcal{A}$. $\mathcal{A}$ tries to launch an impersonation attack to convince the $Gano$ that it is a legitimate user. $\mathcal{A}$ needs to forge the legal $Du_i = p_i \cdot P$, $Eu_i = Ta'_i \oplus p_i$ and $Fu_i = H(Du_i \| Eu_i \| p_i \| Tis_1)$, where $Ta'_i = H(Psid_i \| \alpha \| \eta_i)$ is generated with the secret value α of $Auth$. Although $\mathcal{A}$ can randomly generate Ta'_i, it cannot pass $Gano$'s validation. As a result, Us_i impersonation attacks can be effectively resisted.

5.2.5 *GWN* Impersonation Attack

Assume that the tuple $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ sent by $Gano$ is acquired by $\mathcal{A}$. $\mathcal{A}$ tries to launch an impersonation attack to convince the $Smde_j$ that it is a legitimate node. $\mathcal{A}$ needs to forge the legal $Gg_i = H(Sa_i \| \xi_i) \oplus Du'_i$, $Kg_i = H(Sa_i \| Tis_2) \oplus \xi_i$, and $Lg_i = H(Gg_i \| Kg_i \| \xi_i \| Tis_2)$, where ξ_i is the random number and Tis_2 is the timestamp. Although $\mathcal{A}$ can randomly generate n_i to compute $\{Gg_i, Kg_i, Lg_i, Tis_2\}$, it cannot pass $Smde_j$'s validation. As a result, $Gano$ impersonation attacks can be effectively resisted.

5.2.6 SD_j Impersonation Attack

Assume that the tuple $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ sent by $Smde_j$ is acquired by $\mathcal{A}$. $\mathcal{A}$ tries to launch an impersonation attack to convince the Us_i that it is a legitimate device. $\mathcal{A}$ needs to forge the legal $Ns_j = \varrho_j \cdot P$, $Ms_j = \varrho_j \cdot Du'_i$, $SK = H(Ms_j \| \varphi_j \| Tis_3)$, $Vs_j = \varphi_j \oplus Ms_j$ and $Xs_j = H(SK \| Ns_j \| \varphi_j \| Tis_3)$, where ϱ_j and φ_j are the random numbers and Tis_3 is the timestamp generated by $Smde_j$. Although $\mathcal{A}$ can randomly generate ϱ_j and φ_j to compute $\{Ns_j, Vs_j, Xs_j, Tis_3\}$, it cannot pass Us_i's validation. As a result, $Smde_j$ impersonation attacks can be effectively resisted.

5.2.7 Replay Attack

Suppose all authentication messages $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ transmitted through the public channel are intercepted by $\mathcal{A}$. When $\mathcal{A}$ replays authentication information, the timestamp will be validated against the set threshold. As a result, replay attack can be effectively resisted.

5.2.8 MITM Attack

Suppose all authentication messages $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ transmitted through the public channel are intercepted by $\mathcal{A}$. Using $\{Du_i, Eu_i, Fu_i, Tis_1\}$ as an example, $\mathcal{A}$ revises it to try to convince $Gano$ that $\mathcal{A}$ is the legitimate user. In order to do this, $\mathcal{A}$ needs to forge the legal $Du_i = p_i \cdot P$, $Eu_i = Ta'_i \oplus p_i$ and $Fu_i = H(Du_i \| Eu_i \| p_i \| Tis_1)$, where $Ta'_i = H(Psid_i \| \alpha \| \eta_i)$ is generated with the secret value α of $Auth$. Although $\mathcal{A}$ can randomly generate Ta'_i, it cannot pass $Gano$'s validation. The remaining authentication messages $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ remain unchanged. $\mathcal{A}$ lacks knowledge of the random numbers, and the secret value generated by the entity fails to pass authentication. As a result, MITM attack can be effectively resisted.

5.2.9 Multi-party Authentication

In smart home, multi-party authentication is realized among Us_i, *Gano* and $Smde_j$. *Gano* verify the legitimacy of Us_i by determining that the equation $Fu'_i = Fu_i$ holds. Meanwhile, $Smde_j$ verify the legitimacy of *Gano* by determining that the equation $Lg'_i = Lg_i$ holds. Us_i verify the legitimacy of $Smde_j$ by determining that the equation $Xs'_j = Xs_j$ holds.

5.2.10 Three-factors Security

Suppose $\mathcal{A}$ obtains any two out of the three factors, and the following scenario arises:

1) Assuming that $\mathcal{A}$ obtains Ide_i and Paw_i, $\mathcal{A}$ cannot compute the valid $Psid_i = H(Ide_i \| \sigma_i)$ and $Rspw_i = H(Paw_i \| \varpi_i)$, without σ_i and ϖ_i. Additionally, the information $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ cannot obtain any other valid information using only the Ide_i and Paw_i.
2) Assuming that $\mathcal{A}$ obtains Ide_i and Paw_i, $\mathcal{A}$ can compute $(\sigma_i, \tau_i) = Gene(Biom_i)$, $Rspw_i = H(Paw_i \| \varpi_i)$ and $\varpi'_i = Cu_i \oplus Psid'_i$. However, $\mathcal{A}$ cannot compute the valid $Rspw_i = H(Paw_i \| \varpi_i)$ and pass validation without Paw_i. Additionally, the information $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ cannot obtain any other valid information using only the Ide_i and $Biom_i$.
3) Assuming that $\mathcal{A}$ obtains Paw_i and $Biom_i$, $\mathcal{A}$ cannot compute the valid $Psid_i = H(Ide_i \| \sigma_i)$ and $Rspw_i = H(Paw_i \| \varpi_i)$, without ($Ide_i$ and ϖ_i). Additionally, the information $\{Du_i, Eu_i, Fu_i, Tis_1\}$, $\{Gg_i, Kg_i, Lg_i, Tis_2\}$ and $\{Ns_j, Vs_j, Xs_j, Tis_3\}$ cannot obtain any other valid information using only the Paw_i and $Biom_i$.

5.2.11 Prefect Forward Security

Within this article, perfect forward security assures that if the long-term secret value is compromised, the previously established session key remains impervious to breaches. Computing $SK = H(Ms_j \| \varphi_j \| Tis_3)$ requires Ms_j and φ_j, where $Ms_j = \varrho_j \cdot Du'_i$, $Du'_i = p'_i \cdot P$ and ϱ_j, p_i are randoms generated by $Smde_j$ and Us_i. $\mathcal{A}$ faces difficulty in obtaining the random numbers generated in each round.

6 Performance Analysis

To conduct a comprehensive evaluation of the proposed protocol's performance, we conducted both theoretical and experimental analyses, the findings of which are meticulously detailed in Table 1 and Table 2, respectively. Subsequently, empirical assessments were undertaken to gauge the runtime performance across various scenarios. The experimental results yielded compelling evidence, unequivocally demonstrating the superior performance of our protocol in comparison to alternative solutions. Specifically, our protocol exhibited notably enhanced efficiency and efficacy, substantiating its prowess in real-world application scenarios. These findings underscore the protocol's robustness and validate its potential as a frontrunner in addressing the critical requirements of modern security protocols within its domain.

Table 1. Security comparison

Security	Park 2016	Choi 2014	Nam 2014	Li 2017	Ours
Internal privilege attack	×	×	×	×	√
Anonymity	√	×	√	√	√
Untraceability	√	×	√	√	√
Stolen smartcard attack	√	×	√	√	√
U_i impersonation attack	√	√	√	√	√
GWN impersonation attack	×	√	√	√	√
SD_j impersonation attack	×	√	√	√	√
Replay attack	√	√	√	√	√
MITM attack	√	×	×	×	√
Multi-party authentication	×	√	√	√	√
Three-factors security	×	√	√	√	√
Prefect forward security	√	√	√	√	√

Table 2. Cost comparison

Protocol	User	GWN	Device	Total
Park 2016	$9T_H+2T_M$	$11T_H$	$4T_H+2T_M$	$24T_H+4T_M$
Choi 2014	$8T_H+3T_M$	$6T_H+2T_M$	$5T_H+1T_M$	$19T_H+6T_M$
Nam 2014	$4T_H+3T_M$	$4T_H+2T_M$	$4T_H+1T_M$	$12T_H+6T_M$
Li 2017	$8T_H+3T_M$	$7T_H+1T_M$	$4T_H+2T_M$	$19T_H+6T_M$
Ours	$7T_H+1T_M$	$4T_H+1T_M$	$5T_H+2T_M$	$16T_H+4T_M$

6.1 Theoretical Analysis

In terms of theoretical analysis, we compare with other related protocols through security properties and computational overhead comparison. The results of the comparison are presented in Table 1 and Table 2, where Park 2016 [15] proposed an ECC-based AKA protocol further enhances security, Choi 2014 [16] proposed a new ECC-based protocol to improve the inability of the former to realize multi-party authentication, Nam 2014 [17] enhanced Choi 2014 to ensure anonymity. Additionally, Li 2017 [18] reduced the communication overhead of Nam 2014. From Table 1 and Table 2, we can find that ours has sound security and good computational performance.

6.2 Experimental Analysis

In our experimental analysis, we validated the protocol's security using the AVISPA simulation tool. It offers support for authentication across multiple protocols and applications, encompassing Secure Transport Layer Protocol (TLS), IPSec, SSL, SSH, and Kerberos. Additionally, it presents a user-friendly graphical interface, simplifying the configuration and execution of the validation process. Detailed validation reports are also provided, aiding users in comprehending identified security issues and suggested remedies. The protocol's entities and environments are implemented using HLPSL. Our protocol underwent simulation using SPAN, with the results depicted in Figure 5. These results illustrate the protocol's effectiveness in combatting replay attacks and MITM attacks. Then, we tested the runtime of our and related protocols through the PBC library. The test result is presented in Figure 6 and shows that ours has a better performance compared to related protocols.

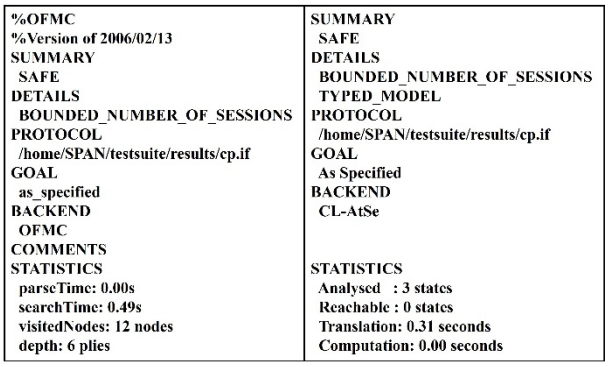

Figure 5. Simulation result

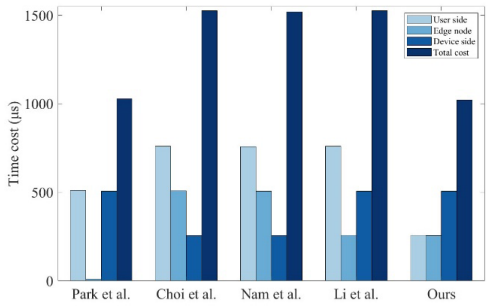

Figure 6. Test result

7 Acknowledgement

In this paper, a practical Authentication and Key Agreement protocol based on Elliptic Curve Cryptography is proposed, aimed at reducing deployment costs for AI-based devices. The proposed protocol ensures secure authentication among users, gateway nodes, and AI-based devices, while also generating a secure session key. Notably, biometrics are incorporated through specific devices, serving as an additional authentication factor to fortify against password leakage attacks. The security of the session key is substantiated using the ROR model, complemented by informal security analysis. To validate the resilience to active attacks, the widely accepted AVISPA is employed. Additionally, experimental simulations are conducted, comparing our approach with related works. The results underscore a harmonious balance between security and performance in our proposed protocol.

8 Conclusion

The work is supported by the National Natural Science Foundation of China (No. U21A20465), the National Key R&D Program of China (No. 2023YFB2703700), the National Natural Science Foundation of China (No. 62172292), and the Science Foundation of Zhejiang Sci-Tech University (ZSTU) (Nos. 23222092-Y, 22222266-Y).

References

[1] C. Zhang, Y. Lu, Study on Artificial Intelligence: The State of the Art and Future Prospects, *Journal of Industrial Information Integration*, Vol. 23, Article No. 100224, September, 2021.

[2] J. Amann, A. Blasimme, E. Vayena, D. Frey, V. I. Madai, Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective, *BMC medical informatics and decision making*, Vol. 20, Article No. 310, 2020.

[3] M. Keerthika, D. Shanmugapriya, Wireless Sensor Networks: Active and Passive Attacks-vulnerabilities and Countermeasures, *Global Transitions Proceedings*, Vol. 2, No. 2, pp. 362-367, November, 2021.

[4] W. Yang, Z. Zheng, G. Chen, Y. Tang, X. Wang, Security Analysis of a Distributed Networked System under Eavesdropping Attacks, *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 67, No. 7, pp. 1254-1258, July, 2020.

[5] A. Mallik, Man-in-the-middle-attack: Understanding in Simple Words, *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, Vol. 2, No. 2, pp. 109-134, October, 2018.

[6] T. Zhang, J. Shen, H. Yang, V. Pandi, B. B. Gupta, V. Arya, Sustainable Authentication and Key Agreement Protocol Using Chaotic Maps for Industry 5.0, *IEEE Transactions on Consumer Electronics*, pp. 1-10, December, 2023. DOI: 10.1109/TCE.2023.3339818

[7] L. Lamport, Password Authentication with Insecure Communication, *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, November, 1981.

[8] C. Guo, C. C. Chang, Chaotic Maps-based Password-authenticated Key Agreement using Smart Cards,

Communications in Nonlinear Science and Numerical Simulation, Vol. 18, No. 6, pp. 1433-1440, June, 2013.
[9] H. Y. Lin, Improved Chaotic Maps-based Password-authenticated Key Agreement using Smart Cards, *Communications in Nonlinear Science and Numerical Simulation*, Vol. 20 No. 2, pp. 482-488, February, 2015.
[10] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, A. V. Vasilakos, Secure Biometric-based Authentication Scheme using Chebyshev Chaotic Map for Multi-server Environment, *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 5, pp. 824-839, September-October, 2018.
[11] H. Tan, W. Zheng, P. Vijayakumar, K. Sakurai, N. Kumar, An Efficient Vehicle-assisted Aggregate Authentication Scheme for Infrastructure-less Vehicular Networks, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 12, pp. 15590-15600, December, 2023.
[12] A. Irshad, S. A. Chaudhry, Q. Xie, X. Li, M. S. Farash, S. Kumar, F. Wu, An enhanced and provably secure chaotic map-based authenticated key agreement in multi-server architecture, *Arabian Journal for Science and Engineering*, Vol. 43, No. 2, pp. 811-828, February, 2018.
[13] J. Shen, H. Yang, P. Vijayakumar, N. Kumar, A Privacy-preserving and Untraceable Group Data Sharing Scheme in Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 4, pp. 2198-2210, July-August, 2022.
[14] H. Yang, P. Vijayakumar, J. Shen, B. B. Gupta, A Location-based Privacy-preserving Oblivious Sharing Scheme for Indoor Navigation, *Future Generation Computer Systems*, Vol. 137, pp. 42-52, December, 2022.
[15] Y. H. Park, Y. H. Park, Three-factor User Authentication and Key Agreement using Elliptic Curve Cryptosystem in Wireless Sensor Networks, *Sensors*, Vol. 16, No. 12, Article No. 2123, December, 2016.
[16] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, Security Enhanced User Authentication Protocol for Wireless Sensor Networks using Elliptic Curves Cryptography, *Sensors*, Vol. 14, No. 6, pp. 10081-10106, June, 2014.
[17] J. Nam, M. Kim, J. Paik, Y. Lee, D. Won, A Provably-secure ECC-based Authentication Scheme for Wireless Sensor Networks, *Sensors*, Vol. 14, No. 11, pp. 21023-21044, November, 2014.
[18] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A Robust ECC-based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3599-3609, August, 2018.

Biographies

Xiaoming Huang, graduated with a master's degree, and is a PhD candidate at the University of Electronic Science and Technology of China (UESTC), senior engineer. He is currently the legal representative and general manager of Chengdu Rongwei Software Service Co., Ltd. and a member of the Blockchain Branch of Chinese Institute of Electronics (CIE).

Tao Zhang received the B.S. degrees from Nanjing University of Information Science and Technology, Nanjing, China, in 2020, where he is currently pursuing the M.S. degree with the School of Computer Science. His research interests include computer and network security, security systems, and cryptography.

Wenying Zheng received the M.E. degree in electronic engineering from Chosun University, Gwangju, South Korea, in 2009, and the Ph.D. degree in computer science from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2022. She is currently working with the School of Computer Science and Technology, Zhejiang Sci-Tech University, Hangzhou, China.

Huijie Yang received the B.S. and M.S. degrees from Nanjing University of Information Science and Technology, Nanjing, China, in 2017 and 2020, respectively, where she is working toward the Ph.D. degree with the School of Computer Science, Nanjing University of Information Science and Technology.

Yunpeng Song, received the master degrees in Detection Technology and Automation Equipment from Guangxi University in 2011, the a bachelor's degree in Electronic Science and Technology from Zhengzhou University in 2003. He is presently serving as an engineer in Zhejiang Provincial Industry Development Center.