Wuhan University
Journal of Natural Sciences

2023, Vol.28 No.6, 523-530

Article ID 1007-1202(2023)06-0523-08
DOI https://doi.org/10.1051/wujns/2023286523

A Lightweight Anonymous Authentication and Key Negotiation Scheme in Smart Home Environments

ZUO Xinyu[1], WANG Zhangang[2†], LI Anqian[1], HUO Yuyan[1], NIU Shufang[2]
1. School of Software, Tiangong University, Tianjin 300387, China;
2. School of Computer Science and Technology, Tiangong University, Tianjin 300387, China

Abstract: With the rapid development of Internet of Things (IoT) technology, smart home users can access and control smart devices remotely to enjoy convenient and efficient services. However, sensitive data collected by smart devices is vulnerable to attacks such as eavesdropping and simulation when transmitted through public channels. At the same time, the security of resource-constrained smart devices is low, and attackers may use the controlled devices to carry out malicious operations further. To address the aforementioned existing security issues, this paper proposes a lightweight user anonymous authentication scheme for resource-constrained smart home environments. At the same time, the security analysis is carried out to further prove the proposed scheme's security. Finally, the performance analysis between the proposed scheme and the existing similar schemes proves that the proposed scheme has advantages in calculation cost and safety characteristics.

Key words: smart home; security; lightweight; authentication scheme
CLC number: TP309.2

0 Introduction

In recent years, applications based on Internet of Things (IoT) technology, such as smart homes, intelligent healthcare, and smart cities, have received much attention[1]. Among them, smart home systems optimize household resources through remote control smart devices, such as monitoring the operation status of monitoring devices, remotely starting or shutting down devices, and monitoring the working status of safety monitoring devices. The first value of the smart home is the convenience and comfort of living[2]; for example, you can use voice or an APP to control the lighting, curtains, and other equipment at home or monitor the temperature and humidity at home in real-time through our terminal devices. The second value is safety, for example, the ability to monitor the home in real-time so that in the event of an accident, users can be informed of the situation at home and seek help from the relevant personnel.

Received date: 2023-05-28
Foundation item: Supported by Research Project of Undergraduate Teaching Reform and Quality Construction in Tianjin Colleges and Universities in 2023 (B231005806)
Biography: ZUO Xinyu, female, Master candidate, research direction: cryptography. E-mail: zuoxy0211@163.com
† To whom correspondence should be addressed. E-mail: wangzhangang@tiangong.edu.cn

The third value is energy saving, as the smart home can actively or passively adjust the devices' time and area of use according to users' frequency of use and habits. Smart homes simplify our lives while relying on technological development, making life more convenient and less stressful [3].

However, with the development of smart homes, user data and privacy become the focus of attackers[4]. In a smart home environment, entities communicate over a common channel, and messages can be maliciously eavesdropped, inserted, or deleted by an attacker. This allows adversaries to attempt various security attacks, including man-in-the-middle (MITM), user impersonation, and replay attacks [5-7]. Through these attacks, an attacker can access a user's true identity and information, thus threatening the user's anonymity and privacy [8]. In addition, an attacker can perform a device capture attack by capturing physically accessible smart devices, thereby compromising the entire system [9].

In the past few years, various security threats, such as monitoring electricity usage and malicious control appliances, have continuously occurred in actual smart home environments, severely affecting the trust in smart homes. At the same time, robust encryption algorithms are unsuitable for deployment in smart home environments due to the resource-constrained nature of most smart devices.

In order to improve the security of various network environments, scholars at home and abroad have carried out many related researches [10]. In 1981, Lamport [11] first proposed a remote user authentication scheme using a password table and claimed that the scheme was secure. In 2000, Hwang and Li [12] discovered that Lamport's scheme was vulnerable to a password table modification attack. They then proposed a remote user authentication scheme based on the El Gamal public key encryption method without using a password table. So far, there have been many remote user authentication schemes. In 2008, Jeong *et al* [13] proposed an authentication scheme specifically for home networks. However, this scheme does not protect user identity and is vulnerable to attacks such as smart card loss attacks and node capture attacks. In 2019, Shuai *et al* [14] proposed a smart home environment certification scheme based on elliptic curve cryptograpy (ECC). However, Xu *et al* [15] pointed out that Shuai *et al* 's scheme had security problems, such as offline password guessing attacks and internal privilege attacks. In 2021, Kaur and Kumar [16] proposed a scheme based on two-factor authentication and claimed their scheme was resistant to potential security attacks. However, in the same year, Yu *et al* [17] proved that the scheme proposed by Kaur and Kumar was not resistant to key leakage attacks and impersonation attacks and could not meet the security requirements of mutual authentication. Yu *et al* [17] proposed a smart home three-factor anonymous authentication scheme using lightweight symmetric encryption primitives and claim that their scheme is resistant to various known security attacks.

To sum up, in order to ensure security and reduce the cost of computing, storage, and other resources required by authentication schemes, scholars have carried out relatively sufficient research. Therefore, a lightweight, anonymous authentication scheme is essential to counteract security issues and securely use smart home services.

The contributions of this paper are summarized as follows:

1) An authentication and key negotiation scheme is proposed to address the security and privacy issues inherent in traditional smart home security schemes[18].

2) Timestamps and random numbers are incorporated into the design to help stop many attacks, such as replay attacks and denial of service attacks.

3) The performance and security of the proposed scheme was compared with other schemes. The results show that the proposed scheme outperforms similar schemes regarding security and computational cost.

The rest of the paper is organized in the following way. Section 1 shows the proposed scheme. Section 2 contains the security analysis of the proposed scheme. Section 3 includes the performance of the proposed scheme, and finally, Section 4 is the conclusion.

1 Proposed Scheme

We propose a lightweight anonymous authentication and key negotiation scheme for a smart home environment that includes four entities: the user, the home gateway, the smart device, and the authority. Among them, the gateway is a bridge for mutual authentication and key negotiation between the user and the smart device, and the authority is a fully trusted third-party entity responsible for generating essential parameters during the system set up phase and for registering the user and the smart device. For ease of understanding, we show the symbols used in the scheme in Table 1.

Table 1 Symbols and definition

Symbol	Explanation
U_i	User
SD_j	Smart device
GW	Home gateway
TA	Authority
ID_i, ID_j, ID_G	Identity of U_i, SD_j, GW
PID_i, PID_j	Pseudo identity of U_i, SD_j
PW_i	U_i's password
BIO_i	U_i's biometric
σ_i, τ_i	Fuzzy parameters
K_G	Private key of GW
K_S	Private key of SD_j
r_i, r_j, n_i, n_j, n_k, n_s	Random numbers
p	A large prime number
$\oplus$, $\|\|$	Exclusive operation, Connection operation
$h(\cdot)$	Hash function

1.1 Set Up Phase

At this phase, the authority generates security parameters for GW and SD_j.

Step 1 The TA selects a unique identity ID_G for the GW, generates a private key K_G, and stores ID_G, K_G in the memory of GW.

Step 2 The TA selects a unique identity ID_j for the SD_j, generates a private key K_S, and stores ID_j, K_S in the memory of SD_j.

1.2 Registration Phase

At this phase, U_i and SD_j send registration requests to TA. After receiving registration requests, the TA will generate confidential credentials for U_i and SD_j. At this stage, the message is transmitted through a secure channel, as shown in Fig. 1 and Fig. 2.

1.2.1 User registration phase

Step 1 The U_i selects unique ID_i and PW_i, imprints BIO_i, generates $r_i \in Z_q^*$, computes Gen (BIO_i) = (σ_i, τ_i), $PPW_i = h\ (PW_i \ \| \ \sigma_i)$, and $PID_i = h\ (ID_i \ \| \ \sigma_i)$, and sends $\{ID_i, PID_i, PPW_i, r_i\}$ to TA through a private channel.

Step 2 The TA computes $X_i = h\ (ID_i \ \| \ K_G \ \| \ r_i)$, $Y_i = X_i \oplus PPW_i$, and stores $\{ID_i, PID_i, r_i\}$ in the memory of GW, and sends $\{Y_i\}$ to U_i.

Step 3 U_i now computes $A_1 = r_i \oplus h\ (PID_i \ \| \ PPW_i)$, $Auth_i = h\ (PID_i \ \| \ PPW_i \ \| \ r_i)$ and stores $\{Auth_i, Y_i, A_1, \tau_i\}$ into U_i's terminal device.

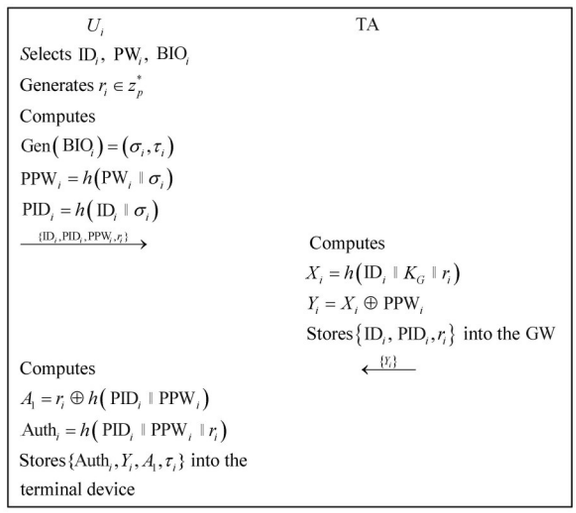

Fig. 1 User registration phase

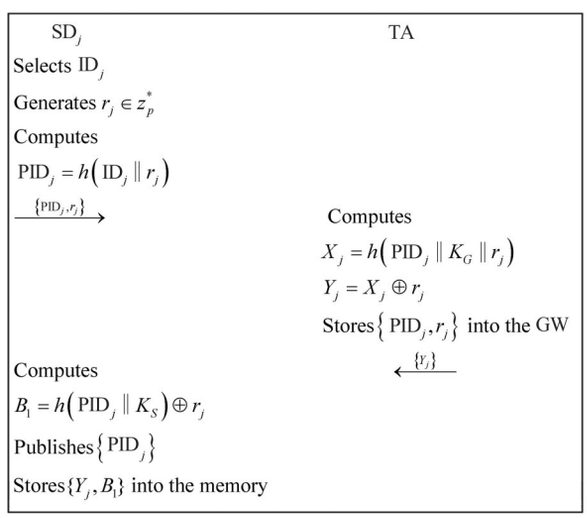

Fig. 2 Smart device registration phase

1.2.2 Smart device registration phase

Step 1 The SD_j generates $r_j \in Z_q^*$, and computes $PID_j = h\ (ID_j \ \| \ r_j)$ and sends PID_j, r_j to TA through a private channel.

Step 2 The TA computes $X_j = h\ (PID_j \ \| \ K_G \ \| \ r_j)$, $Y_j = X_j \oplus r_j$, and stores PID_j, r_j in the memory of GW, and sends Y_j to SD_j.

Step 3 SD_j now computes $B_1 = r_i \oplus h\ (PID_j \ \| \ K_S)$ and, discloses PID_j to the U_i and stores $\{Y_j, B_1\}$ in the memory of SD_j.

1.3 Login and Authentication Phase

Once the registration phase is complete, U_i and SD_j achieve mutual authentication with the assistance of GW by the following steps. After successful authentication, a

session key is negotiated between U_i and SD_j, as shown in Fig. 3.

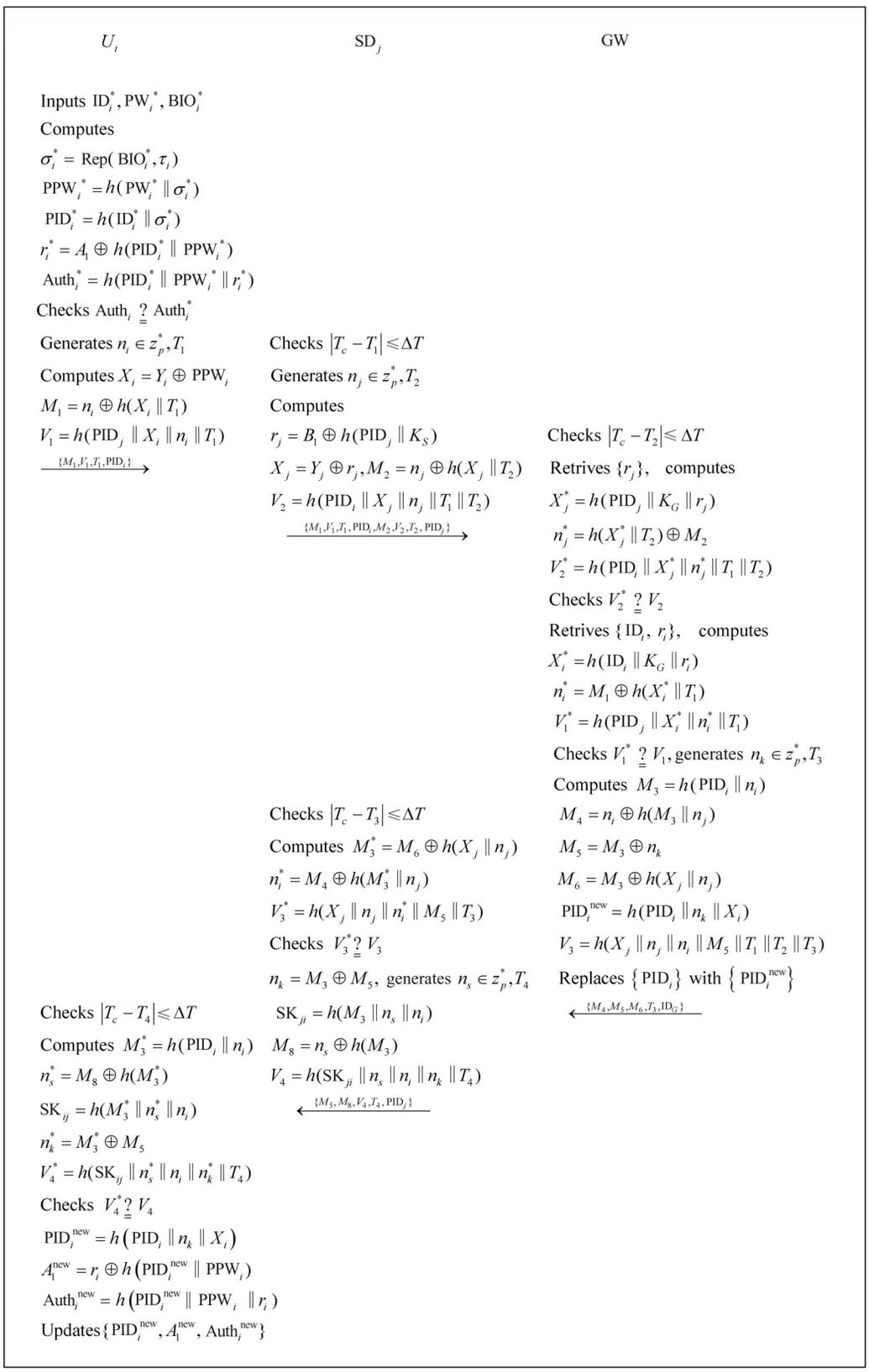

Fig. 3 Login and authentication phase

Step 1 U_i inputs ID_i^*, PW_i^*, BIO_i^*, the terminal device computes $\sigma_i^* = \text{Rep}(BIO_i^*, \tau_i)$, $PPW_i^* = h(PW_i^* \| \sigma_i^*)$, $PID_i^* = h(ID_i^* \| \sigma_i^*)$, $r_i^* = A_1 \oplus h(PID_i^* \| PPW_i^*)$, and $Auth_i^* = h(PID_i^* \| PPW_i^* \| r_i^*)$. Now, U_i's terminal device checks the equality $Auth_i \stackrel{?}{=} Auth_i^*$, and if the validation is unsuccessful, the session is terminated. Otherwise, $ID_i^* = ID_i$, $PW_i^* = PW_i$, $BIO_i^* = BIO_i$, U_i generates $n_i \in z_p^*$ and the current timestamp T_1. Then, U_i computes $X_i = Y_i \oplus PPW_i$, $M = n_{i1} \oplus h(X_i \| T_1)$, and $V_1 = h(PID_j \| X_i \| n_i \| T_1)$ and sends $\{M_1, V_1, T_1, PID_i\}$ to SD_j.

Step 2 On receiving $\{M_1, V_1, T_1, PID_i\}$, SD_j checks $|T_C - T_1| \leqslant \Delta T$, where T_C is the current timestamp recorded at SD_j and ΔT is the allowable time delay. On the successful timestamp validation, SD_j extracts B_1, Y_j and computes $r_j = B_1 \oplus h(PID_j \| K_S)$, and $X_j = Y_j \oplus r_j$. Then, SD_j generates $n_j \in z_p^*$ and the current timestamp T_2, and computes $M_2 = n_j \oplus h(X_j \| T_2)$ and $V_2 = h(PID_i \| X_j \| n_j \| T_1 \| T_2)$, and sends $\{M_1, V_1, T_1, PID_i, M_2, V_2, T_2, PID_j\}$ to GW.

Step 3 On receiving $\{M_1, V_1, T_1, PID_i, M_2, V_2, T_2, PID_j\}$, GW checks $|T_C - T_2| \leqslant \Delta T$, and on successful validation of timestamp, GW retrieves $\{r_j\}$ from its memory and computes $X_j^* = h(PID_j \| K_G \| r_j)$, $n_j^* = h(X_j^* \| T_2) \oplus M_2$ and $V_2^* = h(PID_i \| X_j^* \| n_j^* \| T_1 \| T_2)$. Now, GW checks the validity $V_2^* \stackrel{?}{=} V_2$, and the session is terminated if the validation is unsuccessful. Otherwise, GW authenticates the identity of SD_j and $X_j^* = X_j$, $n_j^* = n_j$, and GW retrieves $\{ID_i, r_i\}$ from its memory and computes $X_i^* = h(ID_i \| K_G \| r_i)$, $n_i^* = M_1 \oplus h(X_i^* \| T_1)$ and $V_1^* = h(PID_j \| X_i^* \| n_i^* \| T_1)$.

Then, GW checks the validity of $V_1^* \stackrel{?}{=} V_1$, and if the validation is not successful, the session is terminated. Otherwise, GW authenticates the identity of U_i and $X_i^* = X_i$, $n_i^* = n_i$, and GW generates $n_k \in z_p^*$ and the current timestamp T_3, and computes $M_3 = h(PID_i \| n_i)$, $M_4 = n_i \oplus h(M_3 \| n_j)$, $M_5 = M_3 \oplus n_k$, $M_6 = M_3 \oplus h(X_j \| n_j)$, $V_3 = h(X_j \| n_j \| n_i \| M_5 \| T_3)$, $PID_i^{new} = h(PID_i \| n_k \| X_i)$ and replaces $\{PID_i\}$ with $\{PID_i^{new}\}$. GW now sends $\{M_4, M_5, M_6, T_3, ID_G\}$ to SD_j.

Step 4 On receiving $\{M_4, M_5, M_6, T_3\}$, SD_j checks $|T_C - T_3| \leqslant \Delta T$, and on successful validation of timestamp, SD_j computes $M_3^* = M_6 \oplus h(X_j \| n_j)$, $n_i^* = M_4 \oplus h(M_3^* \| n_j)$, and $V_3^* = h(X_j \| n_j \| n_i^* \| M_5 \| T_3)$. Now, SD_j checks the validity of $V_3^* \stackrel{?}{=} V_3$, and if the validation is unsuccessful, the session is terminated. Otherwise, SD_j authenticates the identity of GW and $M_3^* = M_3$, $n_i^* = n_i$, and SD_j computes $n_k = M_3 \oplus M_5$. Then, SD_j genetates $n_s \in z_p^*$ and the current timestamp T_4, and computes $SK_{ji} = h(M_3 \| n_s \| n_i)$, $M_8 = n_s \oplus h(M_3)$, and $V_4 = h(SK_{ji} \| n_s \| n_i \| n_k \| T_4)$, and sends $\{M_5, M_8, V_4, T_4, PID_j\}$ to U_i.

Step 5 On receiving $\{M_5, M_8, V_4, T_4, PID_j\}$, U_i checks $|T_C - T_4| \leqslant \Delta T$, and on successful validation of timestamp, U_i computes $M_3^* = h(PID_i \| n_i)$, $n_s^* = M_8 \oplus h(M_3^*)$, $SK_{ij} = h(M_3^* \| n_s^* \| n_i)$, $n_k^* = M_3^* \oplus M_5$, and $V_4^* = h(SK_{ij} \| n_s^* \| n_i \| n_k^* \| T_4)$. Now, SD_j checks the validity of $V_4^* \stackrel{?}{=} V_4$, and if the validation is not successful, the session is terminated. Otherwise, U_i authenticates the identity of SD_j and negotiates a session key with SD_j, and U_i calculates the new pseudo-identity as $PID_i^{new} = h(PID_i \| n_k \| X_i)$, $A_1^{new} = r_i \oplus h(PID_i^{new} \| PPW_i)$ and $Auth_i^{new} = h(PID_i^{new} \| PPW_i \| r_i)$, and replaces $\{PID_i, A_1, Auth_i\}$ with $\{PID_i^{new}, A_1^{new}, Auth_i^{new}\}$ in its memory.

2 Security Analysis

2.1 Anonymity

The proposed scheme generates PID_i by encrypting the U_i's identity ID_i with the secret value σ_i. After GW successfully authenticates the U_i, GW changes the existing PID_i to a new PID_i^{new} and transfers it to the U_i. Even if the attacker eavesdrops on messages transmitted through a public channel, he cannot identify the U_i's true identity ID_i. Therefore, the proposed solution satisfies user anonymity.

2.2 Untraceability

The U_i sends a message to SD_j over a public channel containing $\{M_1, V_1, T_1, PID_i\}$, which the attacker can eavesdrop on during the login and authentication phases. Because these parameters are related to random numbers and timestamps, such as n_i and T_1, which differ from session to session, the attacker cannot track a U_i's actions during the login and authentication phases. Therefore, the proposed scheme guarantees untraceable U_i.

2.3 Mutual Authentication

With GW's assistance, U_i and SD_j authenticate each other in the login and authentication phase. When GW receives message $\{M_1, V_1, T_1, PID_i, M_2, V_2, T_2, PID_j\}$, the authentication process for SD_j is immediately executed. The next step can only be performed after this verification process is successful. U_i authenticates the identity of SD_j by checking that the message SD_j returns to U_i con-

tains valid information related to the random number n_i that U_i sends to GW. Therefore, the scheme guarantees mutual authentication between entities.

2.4 Offline Password Guessing Attack

Suppose the attacker tries to guess the real password PW_i of legal U_i. In order to pass the authentication of the terminal device, the attacker must know the unique biometric information BIO_i and real identity ID_i of the legitimate user, but the BIO_i cannot be obtained. Moreover, according to Section 2.1, the attacker cannot get the ID_i based on the intercepted message, so it is difficult for the attacker to guess the real PW_i. Therefore, offline password guessing attack is not feasible in the proposed scheme.

2.5 Session Key Disclosure Attack

The attacker wants to obtain $\{M_3\}$ and random number $\{n_s, n_i\}$ to calculate a public session key $SK = h(M_3 \| n_s \| n_i)$. However, the correct session key SK cannot be calculated because the random numbers n_s and M_3 are subject to secret values by using hash and XOR functions σ_i. The random number n_i is protected by X_j and K_S using hash and XOR functions. Therefore, the scheme is safe against session key disclosure attack, because the attacker failed to calculate the public session key SK between U_i and SD_j.

2.6 Impersonation Attack

If the attacker tries to impersonate legitimate U_i and SD_j, the attacker must generate authentication request messages or authentication response messages. However, the attacker does not know the key credentials for authentication, X_i and X_j. Therefore, the proposed scheme can resist impersonation attacks because the attacker cannot successfully generate authentication requests and response messages for legitimate U_i and SD_j.

2.7 Replay Attack

Suppose the attacker eavesdrops on the messages transmitted on the public channel during the login and mutual authentication phase. If the attacker resends and reuses all the messages transmitted in the previous session, the entity receiving the message will check the freshness of the current timestamp. In addition, all messages are masked with new random numbers by using Hash and XOR functions. Therefore, this scheme can prevent replay attacks.

2.8 Verifier Stolen Attack

The proposed scheme is immune to a stolen verifier attack by a possible malicious attacker. Even if the attacker obtains the verification table $\{PID_i, r_i\}$, $\{PID_j, r_j\}$ stored in the gateway, the attacker must know GW's private key K_G for computing X_i, X_j and recovering further information. Therefore, the proposed scheme is resistant to stolen verifier attacks.

2.9 Man in the Middle Attack

In the proposed scheme, if the attacker attempts to manipulate messages transmitted through a public channel between different entities, it will be detected when the entities verify V_1, V_2, V_3, and V_4. If the attacker attempts to modify the parameters of intermediate messages, it will not succeed in these malicious attempts. Hence, the proposed scheme can resist man-in-the-middle attacks successfully.

2.10 Forward Confidentiality

The attacker may obtain the session key calculated between U_i and SD_j. However, the attacker cannot infer the previous session key based on the session key obtained this time. Because the random numbers n_i and n_s contained in them differ in each session of the proposed scheme. Therefore, the proposed scheme ensures forward security.

3 Performance Evaluation

In order to evaluate the performance of the proposed scheme, we compare it with other similar schemes in terms of computational cost and security features in this section.

3.1 Computation Cost

In this section, we compare the computation cost of the proposed scheme with several similar schemes[14,17,19,20] in recent years. According to Xia *et al*'s scheme[19], we use Th, Tf, Tepm, Tpuf, and Ts to denote the consumption time of one-way Hash functions, fuzzy extractors, ECC point multiplication, physical unclonable functions (PUF), and symmetric key encryption/decryption, respectively as shown in Table 2.

Table 3 depicts the computational overhead of the different entities in the login and authentication phases of the proposed scheme compared with several other schemes. By calculation, the scheme of Zou *et al*[20] has the highest overhead of 11.980 8 ms, while the proposed scheme has a computational overhead of 2.074 8 ms. It is clear that the proposed scheme has a significant advantage over other solutions in terms of computation cost,

satisfies the requirement of lightweight, and is suitable for resource-constrained smart home environments.

Table 2 Consumption times of different schemes

Symbol	Operation	Consumption time/ms
Th	One-way Hash function	0.002 6
Tf	Fuzzy extractor	1.989
Tepm	ECC point multiplication	1.989
Tpuf	PUF	0.12
Ts	Symmetric key operations	0.003 25

3.2 Security Features

As shown in Table 4, we have compared the security characteristics of the proposed scheme with other schemes. The result indicates that other schemes have one or more security vulnerabilities. For example, Yu *et al*'s scheme[17] is not resistant to replay attacks and so on. Therefore, the proposed scheme also has an advantage regarding security features.

4 Conclusion

This paper proposes a lightweight anonymous identity authentication scheme in the smart home environment. Security analysis shows that the proposed scheme is resistant to all known attacks. By comparing the proposed scheme with similar schemes in recent years in terms of computational cost and security features, the proposed scheme is shown to be a lightweight and efficient authentication scheme.

Table 3 Computational cost of the schemes

Scheme	User	Smart device	Home gateway	Cost/ms
Shuai *et al*[14]	2Tepm+6Th	3Th	1Tepm+7Th	6.008 6
Yu *et al*[17]	1Tf+1Ts+11Th	7Th	11Th	2.067 65
Zou *et al*[20]	3Tepm+6Th	2Tem+6Th	1Tepm+6Th	11.980 8
Xia *et al*[19]	1Tf+1Ts+10Th	1Tpuf+1Tf+3Ts+5Th	4Ts+9Th	4.186 4
Proposed scheme	1Tf+13Th	9Th	11Th	2.074 8

Table 4 Security features comparisons

Attack	Shuai *et al*[14]	Yu *et al*[17]	Zou *et al*[20]	Xia *et al*[19]	Proposed scheme
Anonymity	√	√	√	√	√
Untraceability	√	√	√	√	√
Mutual authentication	√	×	×	√	√
Terminal device lost/stolen attack	√	√	√	√	√
Session key disclosure attack	×	√	×	√	√
Impersonation attack	√	√	√	√	√
Replay attack	×	√	√	√	√
Verifier stolen attack	√	√	√	—	√
Man in the middle attack	√	√	√	√	√
Offline password guessing attack	×	√	√	√	√
Forward confidentiality	√	×	√	√	√

Note: √: Effective; ×: Ineffective; -: Not considered

References

[1] Guo Y M, Zhang Z F, Guo Y J. SecFHome: Secure remote authentication in fog-enabled smart home environment[J]. *Computer Networks*, 2022, **207**: 108818.

[2] Bai L Y, Hsu C, Harn L, *et al*. A practical lightweight anonymous authentication and key establishment scheme for resource-asymmetric smart environments[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022(1): 1-11.

[3] Pirayesh J, Giaretta A, Conti M, *et al*. A PLS-HECC-based device authentication and key agreement scheme for smart home networks[J]. *Computer Networks*, 2022, **216**: 109077.

[4] Li R, Kang B Y, Mai K Q . Analysis and improvement on a Hash-based authentication scheme for multi-server architecture[J]. *Wuhan University Journal of Natural Sciences*, 2021, **26**(5): 394-404.

[5] Sutrala A K, Obaidat M S, Saha S, *et al*. Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems [J]. *IEEE Transactions on Intelligent Transportation Systems*, 2021, **23**(3): 2316-2330.

[6] Abbas G, Tanveer M, Abbas Z H, *et al*. A secure remote user authentication scheme for 6LoWPAN-based Internet of Things[J]. *PloS one*, 2021, **16**(11): e0258279.

[7] Chen C M, Deng X T, Kumar S, *et al*. Blockchain-based medical data sharing schedule guaranteeing security of individual entities[J]. *Journal of Ambient Intelligence and Humanized Computing*, 2021:1-10.

[8] Cho Y, Oh J, Kwon D, *et al*. A secure and anonymous user authentication scheme for IoT-enabled smart home environments using PUF[J]. *IEEE Access*, 2022, **10**: 101330-101346.

[9] Wang D, Wang P. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks[J]. *Ad Hoc Networks*, 2014, **20**: 1-15.

[10] Du J Q, Kang B Y, Han Y B. Improvement on a biometric based user authentication scheme in wireless sensor networks using smart cards[J]. *Wuhan University Journal of Natural Sciences*, 2020, **25**(2): 155-161.

[11] Lamport L. Password authentication with insecure communication[J]. *Communications of the ACM*, 1981, **24**(11): 770-772.

[12] Hwang M S, Li L H. A new remote user authentication scheme using smart cards[J]. *IEEE Transactions on Consumer Electronics*, 2000, **46**(1): 28-30.

[13] Jeong J, Chung M Y, Choo H. Integrated OTP-based user authentication scheme using smart cards in home networks[C]// *Proceedings of the* 41*st Annual Hawaii International Conference on System Sciences* (*HICSS* 2008). New York: IEEE, 2008: 294-294.

[14] Shuai M X, Yu N H, Wang H X, *et al*. Anonymous authentication scheme for smart home environment with provable security[J]. *Computers & Security*, 2019, **86**: 132-146.

[15] Xu M, Dong Q, Zhou M, *et al*. Security analysis on "anonymous authentication scheme for smart home environment with provable security"[J]. *Wireless Communications and Mobile Computing*, 2020, **2020**: 1-4.

[16] Kaur D, Kumar D. Cryptanalysis and improvement of a two-factor user authentication scheme for smart home[J]. *Journal of Information Security and Applications*, 2021, **58**: 102787.

[17] Yu S, Jho N, Park Y. Lightweight three-factor-based privacy-preserving authentication scheme for IoT-enabled smart homes[J]. *IEEE Access*, 2021, **9**: 126186-126197.

[18] Nyangaresi V O. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography[J]. *Journal of Systems Architecture*, 2022, **133**: 102763.

[19] Xia Y D, Qi R X, Ji S, *et al*. PUF-assisted lightweight group authentication and key agreement protocol in smart home[J]. *Wireless Communications and Mobile Computing*, 2022, **2022**: 1-15.

[20] Zou S H, Cao Q, Wang C Y, *et al*. A robust two-factor user authentication scheme-based ECC for smart home in IoT[J]. *IEEE Systems Journal*, 2021, **16**(3): 4938-4949.

□