Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 4, No. 2, 2023

Analysis and Improvement of PUF-based Secure Anonymous User Authentication Scheme in Smart Home Environment

Xinyu Zuo [1], Zhangang Wang [2, *], Anqian Li [1], Yuyan Huo [1] and Shufang Niu [2]

[1] School of Software, Tiangong University, Tianjin 300387, China
[2] School of Computer Science and Technology, Tiangong University, Tianjin 300387, China
*** Corresponding author:** Zhangang Wang (Email: wangzhangang@tiangong.edu.cn)

Abstract: With the rapid development of IoT technology, smart home is attracting much attention due to its convenience and comfort. In 2022, CHO et al. proposed an anonymous user authentication scheme using PUFs in smart home environment. However, this paper conducts a security analysis and finds that CHO et al.'s scheme cannot resist tracking attacks, replay attacks and cannot reach session keys. In order to overcome the shortcomings of CHO et al.'s scheme, this paper proposes an improved PUF-based secure anonymous user authentication scheme. After security analysis and comparison with related authentication schemes in terms of security and computational cost, it is demonstrated that the improved scheme is resistant to a variety of attacks and can achieve secure and efficient authentication.

Keywords: Smart Home; Authentication Scheme; Security.

1. Introduction

In recent years, Internet of Things (IoT) technology has developed rapidly, and smart home, as a typical application of IoT, has attracted much attention because of its convenient and comfortable features [1]. Smart home system can control various household appliances through mobile phones, TVs, computers and other devices to achieve remote control and management of household appliances and improve people's quality of life. At the same time, smart home system can realize comprehensive monitoring of home security system, which enables people to enjoy a more comfortable, healthy and happy life under the premise of ensuring home security.

However, as communication between entities in the smart home environment relies on common channel, which is vulnerable to eavesdropping and impersonation attacks [2-5]. The security of the smart home is an issue. Also, in smart home environment, attackers can use controlled devices to perform malicious acts due to the low security of resource-constrained smart devices. Therefore, authentication as well as communication security in smart home environment is very important.

In 1981, Lamport et al. [6] proposed a remote user authentication scheme using a password table. In recent years, with the popularity of IoT applications, scholars have proposed many authentication schemes for smart home environment [7-10]. In 2021, Zou et al. proposed an authentication scheme based on elliptic curve cryptography (ECC) in smart home environment, and in 2022, CHO et al. [11] claimed that Zou et al.'s [12] authentication scheme is vulnerable to forgery and session key compromise attacks and proved that the scheme of Zou et al. does not guarantee mutual authentication between home users and home devices. Then, CHO et al. proposed a secure anonymous authentication scheme using physical unclonable functions (PUFs) [13]. However, after analysis, this paper found several security problems in CHO et al.'s scheme. Firstly, a maliciously controlled home device is able to compute the key credentials for mutual authentication between the user and the gateway as well as the user's updated pseudo-identity. Secondly, certain messages delivered via the public channel are not authenticated. Thirdly, no timestamp is used in CHO et al.'s scheme, which does not guarantee the freshness of the delivered messages. Finally, the gateway does not know the identity of the device when the home device sends a request to the gateway. Therefore, the scheme of CHO et al. is not secure.

In order to overcome the shortcomings of CHO et al's scheme, an improved scheme is proposed in this paper. In the user registration phase of the improved scheme, the key credentials for mutual authentication between the user and the gateway are further protected. In the login and authentication phase, the updated pseudo-identity of the user calculated by the gateway is improved, timestamps are added, etc. Also, this paper compares the security and computational cost of the improved scheme with existing similar schemes.

1.1. Contribution

The contributions of this paper are summarized as follows:

(1) The scheme of CHO et al. [11] is improved, and the security and privacy problems inherent in smart home security schemes are solved.

(2) Time stamps and random numbers are added to the improved scheme to enhance the security of the scheme.

(3) The security and computational cost of the improved scheme are compared with other similar schemes. The results show that the improved scheme is superior to other similar schemes in terms of security and computational cost.

1.2. Organization

The rest of the paper is organized in the following way. Section II reviews the scheme of CHO et al. [11], Section III analyses the safety problems in the CHO et al.'s scheme, Section IV proposes a new and improved scheme, Section V analyses the safety of the improved scheme, and Section VI analyses the performance of the improved scheme. Finally,

Section VII is the conclusion.

2. Review of CHO et al.'s Scheme

In this section, the paper quickly reviews CHO et al.'s scheme. In this scheme, four entities are included: registration center (RC), user (U_i), gateway (GW), and home device (HD_j). In this case, U_i and HD_j are register through RC, and GW helps U_i and HD_j to authenticate with each other and agree on a session key.

The scheme of CHO et al. [11] consists of five phases namely: system establishment phase, home device registration phase, user registration phase, login and authentication phase and password update phase. For the sake of brevity, we do not describe password update phase here. The symbols used in this paper and their definitions are shown in Table 1.

Table 1. Symbols

Symbols	definitions
ID_i, PW_i	U_i's identity and password
PID_i	U_i's temporary identity
SID_j	HD_j's identity
RID_i, DID_j	Pseudo identity of U_i,HD_j
s, t, b	Master key of RC, GW, HD_j
C_j, R_j	Challenge and response of PUF
ω	Fuzzy verifier
$PUF(\cdot)$	PUF operation
SK	Session key
a_1, a_2, a_3	Random nonce
$Gen(\cdot)/\mathrm{Re}p(\cdot)$	Generation / reproduction function
$h(\cdot)$	Hash function
$\oplus$	Exclusive operation
$\|\|$	Connection operation

2.1. System Establishment Phase.

Before deploying GW and HD_j, RC generates t as the master key for the gateway GW and C_j as the challenge value for HD_j. Afterwards, RC stores C_j securely in the memory of HD_j. RC selects the hash function, and generates b as the secret value for HD_j.

2.2. Home Device Registration Phase.

Step 1. HD_j calculates $X_j = h(SID_j \| b)$, $R_j = PUF(C_j)$, $Gen(R_j) = (D_j, HS_j)$, where SID_j is the unique identity of HD_j and transmits $\{SID_j, C_j, X_j\}$ to RC over a secure channel.

Step2. On receiving $\{SID_j, C_j, X_j\}$, RC calculates and stores $HDC_j = h(SID_j \| s)$, and then calculates $K_{HD_j} = h(h_j \| SID_j \| s)$, $DID_j = h(SID_j \| h_j \| K_{HD_j})$, $PD_j = h(K_{HD_j} \| X_j)$, $B_j = h_j \oplus h(DID_j \| t)$. Thereafter, RC transmits $\{DID_j, C_j, PD_j, B_j\}$ to GW over a secure channel for GW to store, and then transmits $\{DID_j, K_{HDj}, h_j\}$ securely to HD_j.

Step 3. On receiving them, HD_j calculates $H_j = D_j \oplus h_j$ and stores $\{HS_j, H_j, K_{HDj}\}$ into the its memory.

2.3. User Registration Phase.

Step 1. U_i selects ID_i and PW_i and generates random number r_i, then calculates the $PID_i = h(ID_i \| r_i)$, $PPW_i = h(PID_i \| PW_i \| r_i)$ and transmits $\{ID_i, PID_i\}$ to RC over a secure channel.

Step 2. Upon receiving $\{ID_i, PID_i\}$, RC calculates and verifies that $UC_i = h(PID_i \| s)$ existed in its database. If it exists, RC terminates the registration phase. Otherwise, RC saves UC_i into its database, selects a fuzzy verification value ω, calculates: $PU_i = h(ID_i \| s)$, $K_{UG_i} = h(PU_i \| t)$, $RID_i = h(PID_i \| K_{UG_i})$, $y_i = h(RID_i \| t)$, and then stores $\{RID_i, PID_i, PU_i, y_i\}$ into GW's memory , and sends $\{\omega, RID_i, K_{UGi}, y_i\}$ to U_i over the secure channel.

Step 3. After receiving the message, U_i calculates: $V_i = h(PID_i \| PPW_i) \bmod \omega$, $A_1 = RID_i \oplus h(r_i \| PID_i)$, $A_2 = K_{UG_i} \oplus h(ID_i \| PPW_i \| r_i)$, $X_i = r_i \oplus h(ID_i \| PW_i)$, $Y_i = y_i \oplus h(ID_i \| r_i)$, and stores $\{X_i, Y_i, V_i, \omega, A_1, A_2\}$ into the smart card.

2.4. Login and Authentication Phase.

Step 1. U_i enters the $ID_i^{'}, PW_i^{'}$ into the smart card. The smart card calculates $r_i = X_i \oplus h\left(ID_i^{'} \| PW_i^{'}\right)$, $PID_i^{'} = h(ID_i^{'} \| r_i)$, $PPW_i^{'} = h(PID_i^{'} \| PW_i^{'} \| r_i)$, $V_i^{'} = h(PID_i^{'} \| PPW_i^{'}) \bmod \omega$ and verifies that V_i' is equal to V_i. If it is not equal, this phase is terminated. Otherwise, U_i generates random number a_1 and calculates $y_i = Y_i \oplus h(ID_i \| r_i)$, $RID_i = A_1 \oplus h(r_i \| PID_i)$, $K_{UG_i} = A_2 \oplus h(ID_i \| PPW_i \| r_i)$, $M_1 = DID_j \oplus h(K_{UG_i} \| PID_i)$, $M_2 = a_1 \oplus h(K_{UG_i} \| DID_j)$, $V_1 = h(a_1 \| DID_j \| PID_i)$, and transmits $\{RID_i, M_1, M_2, V_1\}$ to GW over the public channel.

Step 2. On receiving $\{RID_i, M_1, M_2, V_1\}$, GW retrieves $\{PID_i, PU_i\}$ from the database according to RID_i and calculates $DID_j = M_1 \oplus h(h(PU_i \| t) \| PID_i)$, $a_1 = M_2 \oplus h(h(PU_i \| t) \| DID_j)$, $V_1^{'} = h(a_1 \| DID_j \| PID_i)$. and checks if V_1' is equal to V_1, if not, terminate this phase. If equal, GW retrieves $\{C_j, PD_j, B_j\}$ from the database according to DID_j and generates random number a_2. Then, GW calculates $h_j = B_j \oplus h(DID_j \| t)$, $M_3 = (a_1 \| a_2 \| C_j) \oplus PD_j$, $M_4 = h(PU_i \| t) \oplus h_j$, $V_2 = h(a_1 \| a_2 \| C_j \| RID_i)$ and transmits $\{RID_i, M_3, M_4, V_2\}$ to HD_j.

Step 3. After receiving $\{RID_i, M_3, M_4, V_2\}$, HD_j calculates $(a_1 \| a_2 \| C_j) = M_3 \oplus h(K_{HD_j} \| h(SID_j \| b))$, $V_2^{'} = h(a_1 \| a_2 \| C_j \| RID_i)$ and checks whether V_2' is equal to V_2, and terminates this phase if it is not. Otherwise, HD_j generates random number a_3 and calculates $R_j = PUF(C_j)$, $D_j = Rep(R_j, HS_j)$, $h_j = D_j \oplus H_j$, $h(PU_i \| t) = M_4 \oplus h_j$, $SK = h(h(PU_i \| t) \| a_1 \| a_2 \| a_3)$,

$M_5 = a_3 \oplus h(h(K_{HD_j} \| h(SID_j \| b)) \| h_j)$, $V_3 = h(SK \| a_3 \| h(PU_i \| t))$, and transmits $\{M_5, V_3\}$ to GW.

Step 4. After receiving $\{M_5, V_3\}$, GW calculates $a_3 = M_5 \oplus h(PD_j \| h_j)$, $SK = h(h(PU_i \| t) \| a_1 \| a_2 \| a_3)$; $V_3' = h(SK \| a_3 \| h(PU_i \| t))s$, and checks whether V_3' is equal to V_3, and terminates this phase if it is not. Otherwise, GW calculates $RID_i^{new} = h(a_2 \| RID_i)$, $M_6 = (a_2 \| a_3) \oplus h(h(PU_i \| t) \| y_i)$, $V_4 = h(SK \| RID_i^{new} \| a_2 \| a_3)$, and transmits $\{M_6, V_4\}$ to U_i.

Step 5. After receiving $\{M_6, V_4\}$, U_i computes $(a_2 \| a_3) = M_6 \oplus h(K_{UG_i} \| y_i)$, $RID_i^{new} = h(a_2 \| RID_i)$, $SK = h(K_{UG_i} \| a_1 \| a_2 \| a_3)$, $V_4' = h(SK \| RID_i^{new} \| a_2 \| a_3)$. If V_4' is equal to V_4, U_i computes $A_1^{new} = RID_i^{new} \oplus h(r_i \| PID_i)$, then replaces A_1 with A_1^{new}.

3. Weaknesses of CHO et al.'s Scheme

3.1. Tracking Attack

In the login and authentication phase of the CHO et al.'s [11] scheme, U_i transmits $\{RID_i, M_1, M_2, V_1\}$ to GW over the public channel, where $M_1 = DID_j \oplus h(K_{UG_i} \| PID_i)$. Since DID_j, K_{UGi} and PID_i are invariant, M_1 can be tracked.

Furthermore, GW transmits RID_i and $M_3 = (a_1 \| a_2 \| C_j) \oplus PD_j$ to HD_j via the public channel in the second step of the login and authentication phase, and then HD_j calculates $(a_1 \| a_2 \| C_j) = M_3 \oplus h(K_{HD_j} \| h(SID_j \| b))$. After obtaining a_2, HD_j is able to calculate $RID_i^{new} = h(a_2 \| RID_i)$ of U_i. Assuming that HD_j is controlled, a malicious attacker can perform a tracking attack on U_i when it next authenticates with other home devices.

3.2. Replay Attack

Since no timestamp is used in the scheme of CHO et al. [11] to guarantee the freshness of the transmitted messages, an attacker can intercept $\{RID_i, M_3, M_4, V_2\}$ transmitted by GW to the HD_j in the second step of the login and authentication phase, and thereafter pretends that GW transmits again to HD_j. On receiving $\{RID_i, M_3, M_4, V_2\}$, HD_j computes $(a_1 \| a_2 \| C_j) = M_3 \oplus h(K_{HD_j} \| h(SID_j \| b))$, $V_2' = h(a_1 \| a_2 \| C_j \| RID_i)$, and verifies $V_2' \stackrel{?}{=} V_2$, the verification can be passed and HD_j will continue with subsequent computations. Therefore, the scheme of CHO et al. [11] is not resistant to replay attacks.

3.3. Man in the Middle Attack.

In the second step of the login and authentication phase, GW transmits $\{RID_i, M_3, M_4, V_2\}$ to the HD_j, where $M_4 = h(PU_i \| t) \oplus h_j$ is not authenticated. Since there is no timestamp, a malicious attacker can intercept M_4 and tamper it to M_4'. HD_j receives it and computes the wrong $h(PU_i \| t)' = M_4' \oplus h_j$;

then computes $SK' = h(h(PU_i \| t)' \| a_1 \| a_2 \| a_3)$, $V_3' = h(SK' \| a_3 \| h(PU_i \| t)')$ and sends $\{M_5, V_3'\}$ to GW. On receiving it, GW recovers $a_3 = M_5 \oplus h(PD_j \| h_j)$ and computes $SK = h(h(PU_i \| t) \| a_1 \| a_2 \| a_3)$. Since the SK computed by HD_j and GW do not match, GW fails in verifying V_3' and terminates this phase. As a result, HD_j and U_i cannot agree on a session key.

3.4. Not Working Properly.

In the third step of the login and authentication phase, CHO et al.'s [11] scheme does not work properly because $\{M_5, V_3\}$ transmitted from HD_j to GW lacks the identity information of U_i and HD_j. When HD_j transmits $\{M_5, V_3\}$ to GW, GW computes $a_3 = M_5 \oplus h(PD_j \| h_j)$, $SK = h(h(PU_i \| t) \| a_1 \| a_2 \| a_3)$. However, GW does not know which HD_j is transmitting the message at this point. If GW wants to find PD_j and PU_i, it must ask HD_j for its identity information as well as that of U_i with whom it has agreed on a session key. The message $\{M_5, V_3\}$ sent by HD_j to GW is clearly missing RID_i, DID_j. Therefore, the scheme does not work properly.

4. Proposed Scheme

In order to overcome the security vulnerabilities of the CHO et al.'s scheme, an improved scheme is proposed in this paper. The system establishment and home device registration phases of the improved scheme are the same as those of CHO et al.'s scheme, so we only describe user registration phase and login and authentication phase in this section, as follows.

4.1. User Registration Phase.

U_i is registered via its own mobile device and the registration process is as follows:

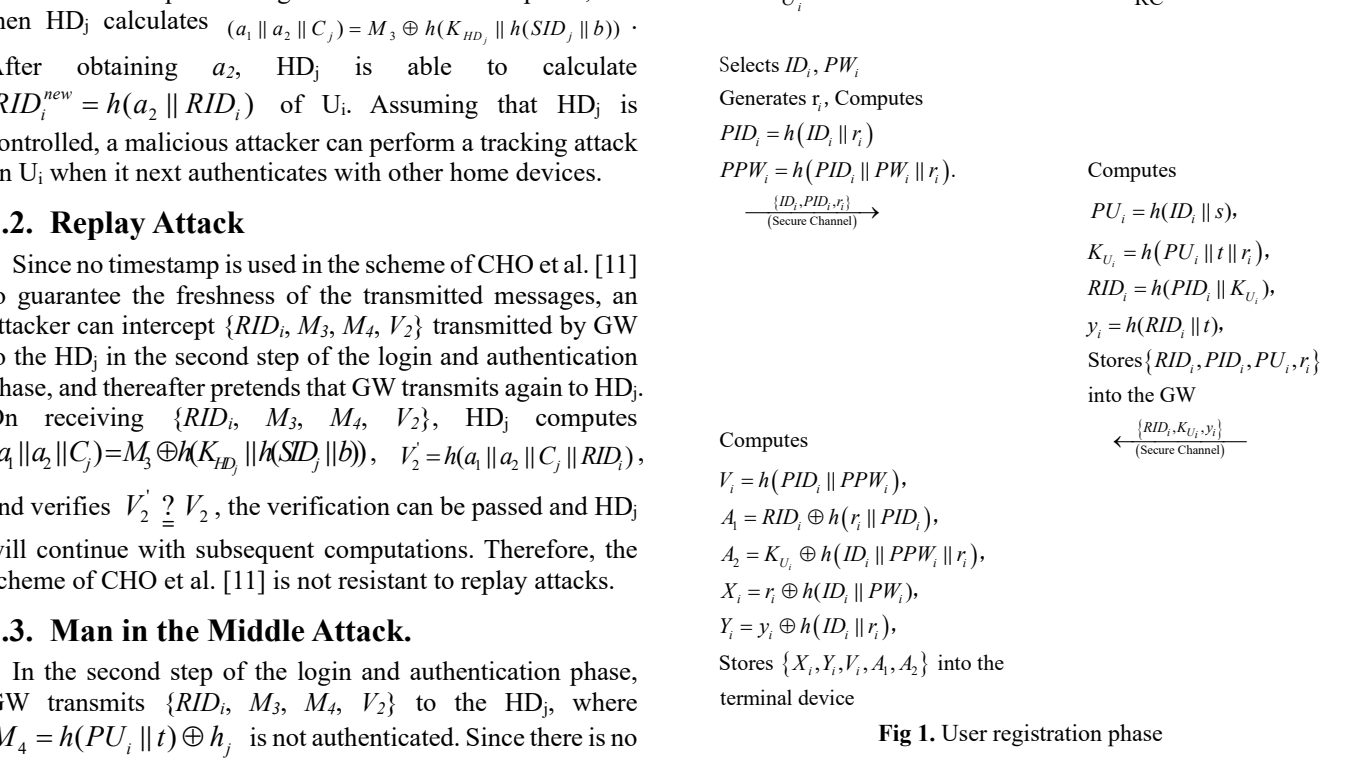

Fig 1. User registration phase

Step 1. U_i selects ID_i and PW_i and generates random number r_i via its mobile device, calculates $PID_i = h(ID_i \| r_i)$ and $PPW_i = h(PID_i \| PW_i \| r_i)$ and transmits $\{ID_i, PID_i, r_i\}$ to the RC via a secure channel.

Step 2. After receiving $\{ID_i, PID_i, r_i\}$, RC calculates the secret value $PU_i = h(ID_i \| s)$ and the secret credential

$K_{U_i} = h(PU_i \| t \| r_i)$ for U_i, where s is the master key of RC and t is the master key of GW, and then calculates $RID_i = h(PID_i \| K_{U_i})$ and $y_i = h(RID_i \| t)$. Afterwards, RC transmits $\{RID_i, PID_i, PU_i, r_i\}$ to GW over a secure channel, and GW receives the information and stores it in memory. Then, RC sends $\{RID_i, PID_i, KU_i, y_i\}$ to U_i over the secure channel.

Step 3. After receiving the message, U_i's mobile device calculates $V_i = h(PID_i \| PPW_i)$, and computes: $A_1 = RID_i \oplus h(r_i \| PID_i)$, $A_2 = K_{U_i} \oplus h(ID_i \| PPW_i \| r_i)$, $X_i = r_i \oplus h(ID_i \| PW_i)$, $Y_i = y_i \oplus h(ID_i \| r_i)$, and finally stores $\{X_i, Y_i, V_i, A_1, A_2\}$ into the mobile device. The detailed process is shown in Figure 1.

4.2. Login and Authentication Phase.

In this phase, U_i and HD_j achieve mutual authentication with the assistance of GW and agree on a session key SK, which is used to complete future confidential communication between U_i and HD_j. The specific steps are as follows:

Step 1. U_i enters $ID_i^{'}$ and $PW_i^{'}$ in its mobile device, and the mobile device calculates $r_i = X_i \oplus h(ID_i^{'} \| PW_i^{'})$, $PID_i^{'} = h(ID_i^{'} \| r_i)$, $PPW_i^{'} = h(PID_i^{'} \| PW_i^{'} \| r_i)$, $V_i^{'} = h(PID_i^{'} \| PPW_i^{'})$, and compares it with V_i stored in the mobile device, if they are equal, U_i logs in successfully. The mobile device then initiates the authentication process, the mobile device generates random number a_1 and timestamp T_1, calculates $y_i = Y_i \oplus h(ID_i \| r_i)$, $RID_i = A_1 \oplus h(r_i \| PID_i)$, $K_{U_i} = A_2 \oplus h(ID_i \| PPW_i \| r_i)$, and selects DID_j of HD_j to be accessed and calculates $M_1 = DID_j \oplus h(K_{U_i} \| PID_i \| T_1)$, $M_2 = a_1 \oplus h(K_{U_i} \| DID_j)$, $V_1 = h(a_1 \| DID_j \| PID_i \| T_1)$, and transmits $\{RID_i, M_1, M_2, V_1, T_1\}$ to GW over public channel.

Step 2. Upon receiving $\{RID_i, M_1, M_2, V_1, T_1\}$, GW first checks $|T_c - T_1| \le \triangle T$, where T_c is the current timestamp. If the message is fresh, GW retrieves the corresponding $\{PID_i, PU_i, r_i\}$ stored in memory based on RID_i, and computes $K_{U_i} = h(PU_i \| t \| r_i)$, $DID_j = M_1 \oplus h(K_{U_i} \| PID_i)$, $a_1 = M_2 \oplus h(K_{U_i} \| DID_j)$, $V_1^{'} = h(a_1 \| DID_j \| PID_i \| T_1)$ and verifies $V_1^{'} \stackrel{?}{=} V_1$, if the condition is not valid, GW terminates this phase. Otherwise, GW successfully authenticates U_i and retrieves $\{C_j, PD_j, B_j\}$ according to DID_j and generates random number a_2 and timestamp T_2, calculates $h_j = B_j \oplus h(DID_j \| t)$, $M_3 = (a_1 \| a_2 \| C_j) \oplus PD_j$, $M_4 = h(PU_i \| t) \oplus h_j$, $V_2 = h(a_1 \| a_2 \| C_j \| M_4 \| RID_i \| T_2)$, and finally, transmits $\{RID_i, M_3, M_4, V_2, T_2\}$ to HD_j over the public channel.

Step 3. Upon receiving $\{RID_i, M_3, M_4, V_2, T_2\}$, HD_j checks $|T_c - T_2| \le \triangle T$, If the message is fresh, HD_j computes $X_j = h(SID_j \| b)$, $(a_1 \| a_2 \| C_j) = M_3 \oplus h(K_{D_j} \| X_j)$, $V_2^{'} = h(a_1 \| a_2 \| C_j \| M_4 \| RID_i \| T_2)$, verifies $V_2^{'} \stackrel{?}{=} V_2$, and if the verification passes, GW authentication is successful. HD_j generates random number a_3 and timestamp T_3, computes $R_j = PUF(C_j)$, $D_j = \mathrm{Re}\, p(R_j, HS_j)$, $h_j = D_j \oplus H_j$, $h(PU_i \| t) = M_4 \oplus h_j$, $SK = h(h(PU_i \| t) \| a_1 \| a_2 \| a_3)$, $M_5 = a_3 \oplus h(h(K_{D_j} \| X_j) \| h_j)$, $V_3 = h(SK \| a_3 \| h(PU_i \| t) \| T_3)$, and transmits $\{M_5, V_3, T_3, RID_i, DID_j\}$ to GW over the public channel.

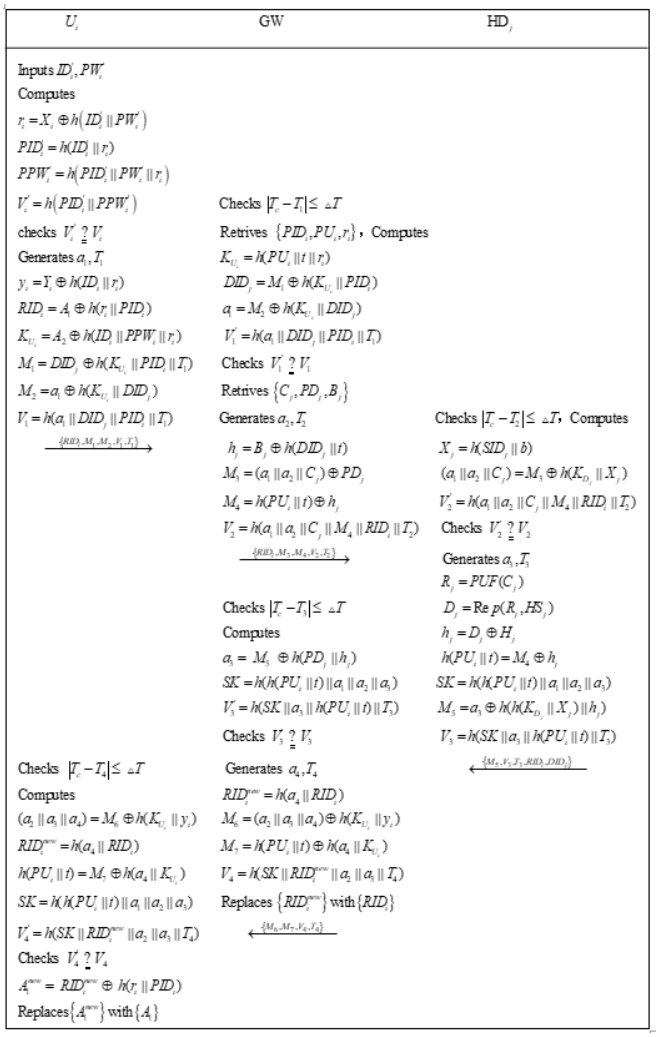

Fig 2. Login and authentication phase

Step 4. Upon receiving $\{M_5, V_3, T_3, RID_i, DID_j\}$, GW checks $|T_c - T_3| \le \triangle T$, If the message is fresh, GW computes $a_3 = M_5 \oplus h(PD_j \| h_j)$, $SK = h(h(PU_i \| t) \| a_1 \| a_2 \| a_3)$, $V_3^{'} = h(SK \| a_3 \| h(PU_i \| t) \| T_3)$, verifies $V_3^{'} \stackrel{?}{=} V_3$, and if the condition is not valid, GW terminates this phase. Otherwise, GW successfully authenticates HD_j and generates random number a_4 and timestamp T_4, computes $RID_i^{new} = h(a_4 \| RID_i)$ for U_i as well as $M_6 = (a_2 \| a_3 \| a_4) \oplus h(K_{U_i} \| y_i)$, $M_7 = h(PU_i \| t) \oplus h(a_4 \| K_{U_i})$, $V_4 = h(SK \| RID_i^{new} \| a_2 \| a_3 \| T_4)$, and replaces RID_i in the database with RID_i^{new} and finally, transmits $\{M_6, M_7, V_4, T_4\}$ to U_i over the public channel.

Step 5. upon receiving $\{M_6, M_7, V_4, T_4\}$, U_i checks $|T_c - T_4| \le \triangle T$. If the message is fresh, the U_i computes $(a_2 \| a_3 \| a_4) = M_6 \oplus h(K_{U_i} \| y_i)$, $RID_i^{new} = h(a_4 \| RID_i)$, $h(PU_i \| t) = M_7 \oplus h(a_4 \| K_{U_i})$, $SK = h(h(PU_i \| t) \| a_1 \| a_2 \| a_3)$ and

$V_4^{'} = h(SK \| RID_i^{new} \| a_2 \| a_3 \| T_4)$, verifies $V_4^{'} \stackrel{?}{=} V_4$, If they are not equal, U_i terminates this phase, otherwise, it indicates that the U_i successfully authenticates HD_j and agrees on the session key, and then computes $A_1^{new} = RID_i^{new} \oplus h(r_i \| PID_i)$ and updates it in the mobile device to update it.

5. Security Analysis

In this section, the paper presents security analysis of the improved scheme, demonstrating that our scheme is secure and resistant to known attacks.

5.1. Anonymity and Untraceability

Section 3.1 of this paper refers to a tracing attack on the CHO et al.'s [11] scheme. In this case, attacker A can intercept the message $\{RID_i, M_1, M_2, V_1\}$ transmitted by U_i to GW, because M_1 is invariant, attacker A can perform a tracing attack on U_i.

Furthermore, attacker A can take control of HD_j and use its a_2 which calculated in the third step of the login and authentication phase and the RID_i received from GW to calculate the updated U_i's identity RID_i^{new}. Thus, the next time U_i authenticates with other home devices, a tracking attack is carried out.

However, the improved scheme concatenates the timestamp T_1 in the calculation of the message M_1, so that M_1 is different for each transmission. Also, GW uses a random number a_4 that only the U_i can compute when updating the pseudo-identity of U_i. Therefore, in the improved scheme, even the same user has different identity information in different sessions. From the above analysis, it is easy to see that the improved scheme achieves anonymity and untraceability of the user.

5.2. Mutual Authentication.

In the login and authentication phase, U_i and HD_j authenticate each other with the assistance of the GW. Firstly, GW verifies that V_1' is equal to V_1, if it is, then both U_i and GW have the correct secret credentials K_{Ui} and GW successfully authenticates U_i's identity. Similarly, HD_j, GW and U_i authenticate $V_2^{'} \stackrel{?}{=} V_2$, $V_3^{'} \stackrel{?}{=} V_3$ and $V_4^{'} \stackrel{?}{=} V_4$ respectively in each session. When all authentication passes, the three achieve mutual authentication and compute the session key. Thus, the improved scheme provides mutual authentication between U_i, GW, and HD_j.

5.3. Impersonation Attack.

Since attacker A does not know the secret credentials K_{Ui} and K_{Dj} for authentication between U_i and HD_j and GW, it cannot successfully impersonate legitimate U_i and HD_j to generate authentication request and response messages, so the improved scheme can resist impersonation attacks.

5.4. Replay Attack.

In the improved scheme, because each received message is authenticated with a timestamp, attacker A cannot perform a replay attack. For example, U_i adds the current timestamp T_1 to each message transmitted, GW will determine whether $|T_c - T_1| \leq \triangle T$ holds, if it does, it will continue to authenticate the other messages received, otherwise, it will terminate this phase.

5.5. Man in the Middle Attack

Section 3.3 of this paper mentions a man-in-the-middle attack on the CHO et al.'s scheme [11]. In this case, attacker A can tamper with M_4 by intercepting the message $\{RID_i, M_3, M_4, V_2\}$ transmitted by GW to HD_j in the second step of the login and authentication phase, and making it impossible for U_i and HD_j to agree on a session key. However, in the improved scheme, M_4 is added to the authentication message V_2, and if attacker A intercepts and tampers with message M_4, HD_j will fail at authentication and terminate this phase. Thus, the improved scheme is resistant to man-in-the-middle attacks.

5.6. Forward Confidentiality

The session key computed between U_i and HD_j may be corrupted by attacker A. However, attacker A cannot find significant correlations between past, present and future session keys because they contain random numbers a_1, a_2 and a_3 that are different in each session of the improved scheme. Thus, the improved scheme guarantees forward security.

6. Performance Evaluation

In this section, the performance of the improved scheme is evaluated and we compare it with the schemes of Naoui et al. [14], Shuai et al. [15], Zou et al. [12], and CHO et al. [11] in terms of both safety characteristics and computational cost.

6.1. Security Features

As shown in Table 2, the security features of the improved solution were compared with the other solutions. The result shows that the other solutions have one or more security vulnerabilities. Therefore, the security of the improved scheme has a great advantage over the other schemes.

Table 2. Security features comparisons

Schemes	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
[14]	NO	YES	NO	YES	YES	YES	YES	YES	YES	YES
[15]	YES	YES	YES	YES	NO	YES	NO	YES	NO	YES
[12]	YES	YES	NO	YES	NO	YES	YES	YES	YES	YES
[11]	YES	NO	YES	YES	YES	NO	NO	NO	YES	YES
Improved scheme	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES

Note.A1: Anonymity; A2: Untraceability; A3: Mutual authentication; A4: Terminal device lost/stolen attack; A5: Session key disclosure attack; A6: Impersonation attack; A7: Replay attack; A8: Man in the Middle Attack; A9: Offline password guessing attack; A10: Forward confidentiality.

6.2. Computation Cost

In this subsection, this paper uses T_h, T_f, T_{epm}, T_{puf}, and T_s to denote the consumption time for one-way hash functions, fuzzy extractors, ECC point multiplication, PUF, and symmetric key encryption/decryption, respectively.

According to the scheme of Xia et al. [1], each time is defined as T_h=0.0026ms, T_f=1.989ms, T_{epm}=1.989ms, T_p=0.12ms and T_s=0.00325ms.

Table 3 depicts the computational costs of the improved scheme compared to several other schemes for different entities in the login and authentication phase. Although the improved scheme has a slightly higher computational cost than CHO et al.'s scheme, it is more secure than CHO et al.'s scheme and can resist various attacks. In addition, the improved scheme also has an advantage in terms of computational cost compared to several other schemes, satisfying the requirement of lightweight and able to be applied to resource-constrained smart home environment.

Table 3. Computation cost comparisons

Schemes	User	Home device	Gateway	Cost(ms)
[14]	$2T_{epm}+2T_s+7T_h$	T_s+2T_h	$T_{epm}+3T_s+8T_h$	6.0307
[15]	$2T_{epm}+6T_h$	$3T_h$	$T_{epm}+7T_h$	6.0086
[12]	$3T_{epm}+6T_h$	$2T_{emp}+6T_h$	$T_{epm}+6T_h$	11.9808
[11]	$15T_h$	$T_p+Tf+7T_h$	$12T_h$	2.1974
Improved scheme	$16T_h$	$T_p+T_f+7T_h$	$14T_h$	2.2052

7. Summary

In this paper, we first review the scheme of CHO et al. and perform a security analysis on it, pointing out that it cannot resist a variety of malicious attacks such as tracking attacks and replay attacks. To address these security problems, we propose an improved PUF-based secure anonymous authentication scheme in a smart home environment, and demonstrate that the improved scheme is secure and has a low computational cost.

References

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

[2] Kwon D K, Yu S J, Lee J Y, et al. WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks. Sensors, 2021, 21(3): 936.

[3] 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. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(3): 2316-2330.

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

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

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

[7] Kumar P, Gurtov A, Iinatti J, et al. Lightweight and secure session-key establishment scheme in smart home environments. IEEE Sensors Journal, 2015, 16(1): 254-264.

[8] Wazid M, Das A K, Odelu V, et al. Secure remote user authenticated key establishment protocol for smart home environment. IEEE Transactions on Dependable and Secure Computing, 2017, 17(2): 391-406.

[9] Wazid M, Das A K, Kumar N, et al. Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment. IEEE Internet of Things Journal, 2018, 6(2): 3572-3584.

[10] Alzahrani B A, Barnawi A, Albarakati A, et al. SKIA-SH: A symmetric key-based improved lightweight authentication scheme for smart homes. Wireless Communications and Mobile Computing, 2022, 2022.

[11] Cho Y, Oh J, Kwon D, et al. A secure and anonymous user authentication scheme for IoT-Enabled smart home environments using PUF. IEEE Access, 2022, 10: 101330-101 346.

[12] Zou S, Cao Q, Wang C, et al. A robust two-factor user authentication scheme based ECC for smart home in IoT. IEEE Systems Journal, 2021, 16(3).

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

[14] Naoui S, Elhdhili M E, Saidane L A. Lightweight and secure password based smart home authentication protocol: LSP-SHAP. Journal of Network and Systems Management, 2019, 27: 1020-1042.

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