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 section, four entities are included: registration center (RC), user (Ui), gateway (GW), and home device (HDj). In this case, Ui and HDj are register through RC, and GW helps Ui and HDj 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>
<thead>
<tr>
<th>Symbols</th>
<th>definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID,j, PWi</td>
<td>U’s identity and password</td>
</tr>
<tr>
<td>PIDi</td>
<td>U’s temporary identity</td>
</tr>
<tr>
<td>SIDj</td>
<td>HDj’s identity</td>
</tr>
<tr>
<td>RIDi, DIDj</td>
<td>Pseudo identity of U,i, HDj</td>
</tr>
<tr>
<td>a, b, c</td>
<td>Master key of RC, GW, HDj</td>
</tr>
<tr>
<td>Cj, Rj</td>
<td>Challenge and response of PUF</td>
</tr>
<tr>
<td>ω</td>
<td>Fuzzy verifier</td>
</tr>
<tr>
<td>PUF(·)</td>
<td>PUF operation</td>
</tr>
<tr>
<td>SK</td>
<td>Session key</td>
</tr>
<tr>
<td>Gen(·)/Rep(·)</td>
<td>Generation/ reproduction function</td>
</tr>
<tr>
<td>h(·)</td>
<td>Hash function</td>
</tr>
<tr>
<td>⊕</td>
<td>Exclusive operation</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.1. System Establishment Phase.

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

2.2. Home Device Registration Phase.

Step 1. HDj calculates Xj = h(SIDj || b), Rj = PUF(Cj), Gen(Rj) = (Dj,j, HS,j), where SIDj is the unique identity of HDj and transmits \{SIDj, Cj, Xj\} to RC over a secure channel.

Step 2. On receiving \{SIDj, Cj, Xj\}, RC calculates and stores HDjCj = h(SIDj || s), and then calculates KHDj = h(hj || SIDj || s), DIDj = h(SIDj || hj || KHDj), PDj = h(KHDj || Xj), Bj = hj ⊕ h(DIDj || t). Thereafter, RC transmits \{DIDj, Cj, PDj, Bj\} to GW over a secure channel for GW to store, and then transmits \{DIDj, KHDj, hj\} securely to HDj.

Step 3. On receiving them, HDj calculates Hj = D.j ⊕ hj and stores \{HSj, Hj, KIDj\} into its memory.

2.3. User Registration Phase.

Step 1. Ui selects IDi and PWi, and generates random number r1, then calculates the PIDi = h(IDi || r1), PPWi = h(PIDi || PWi || r1) and transmits \{IDi, PIDi\} to RC over a secure channel.

Step 2. Upon receiving \{IDi, PIDi\}, RC calculates and verifies that UCi = h(PIDi || s) existed in its database. If it exists, RC registers the termination phase. Otherwise, RC saves UCi into its database, selects a fuzzy verification value ωi, calculates: PU,i = h(IDi || s), KUCi = h(PU,i || t), RIDi = h(PIDi || KUCi), yi = h(RIDi || t), and then stores \{RIDi, PIDi, PU,i, yi\} into GW’s memory, and sends \{ωi, RIDi, KUCi\} to Ui over the secure channel.

Step 3. After receiving the message, Ui calculates: V'i = h(PIDi || PPWi) mod ω, A1 = RIDi ⊕ h(r1 || PIDi), A2 = KUCi ⊕ h(IDi || PPWi || r1), X1 = r1 ⊕ h(IDi || PWi), Y1 = yj ⊕ h(IDj || rj), and stores \{X1, Y1, V1, ωj, A1, A2\} into the smart card.

2.4. Login and Authentication Phase.

Step 1. Ui enters the IDi, PWi into the smart card. The smart card calculates r1 = Xj ⊕ h(IDj || PWi), PID'i = h(ID'i || r1), PPWi = h(PIDi || PWi || r1), V'i = h(PIDi || PPWi) mod ω and verifies that V'i is equal to V1. If it is not equal, this phase is terminated. Otherwise, Ui generates random number ai, and calculates yj = Yj ⊕ h(IDj || rj), RIDi = A1 ⊕ h(r1 || PIDi), KUCi = A1 ⊕ h(IDi || PPWi || r1), M1 = DIDi ⊕ h(KUCi || PIDi), M2 = a1 ⊕ h(KUCi || DIDi), V'i = h(a1 || PIDi || DIDi), and transmits \{RIDi, M1, M2, V'i\} to GW over the public channel.

Step 2. On receiving \{RIDi, M1, M2, V'i\}, GW retrieves \{PIDi, PU,i\} from the database according to RIDi, and calculates DIDIj = M1 ⊕ h(h(PU,i || t) || PIDi), ai = M2 ⊕ h(PU,i || t) || DIDi), V'i = h(a1 || PIDi || DIDi) and checks if V'i is equal to V1, if not, terminate this phase. If equal, GW retrieves \{Cj, PDi, Bj\} from the database according to DIDi and generates random number a2. Then, GW calculates h1 = Bj ⊕ h(IDi || t), M3 = (a1 || a2 || Cj) ⊕ PDj, M4 = h(PU,i || t) ⊕ hj, V2 = h(a1 || a2 || Cj || RIDi) and transmits \{RIDi, M3, M4, V2\} to HDj.

Step 3. After receiving \{RIDi, M3, M4, V2\}, HDj calculates (a1 || a2 || Cj) = M2 ⊕ h(KUCi || h(SIDj || s) || hj), V'i' = h(a1 || a2 || Cj || RIDi) and checks whether V'i' is equal to V2, and terminates this phase if it is not. Otherwise, HDj generates random number a3, and calculates Rj = Rep(Rj, HS,j), h3 = D.j ⊕ hj, h(PU,i || t) = M1 ⊕ hj, SK = h(h(PU,i || t) || a1 || a2 || a3),
$M_j = a_j \oplus h(K_{u,j}) \| h(SID) \| h(b) \| h(j)$, $V_j = h(SK \| a_j \| h(PU_j \| t))$, and transmits $\{M_j, V_j\}$ to GW.

Step 4. After receiving $\{M_j, V_j\}$, GW calculates $a_i = M_j \oplus h(PD_i \| h(j))$, $SK = h(PU_j \| t) \| a_j \| a_i \| a_j$;

$V_j' = h(SK \| a_j \| h(PU_j \| t))$, and checks whether $V_j'$ is equal to $V_j$, and terminates this phase if it is not. Otherwise, GW calculates $RID_{new} = h(a_j \| RID_j)$, $M_0 = (a_j \| a_i \| h(h(PU_j \| t)) \| y_j)$, $V_i = h(SK \| RID_{new} \| a_i \| a_i)$, and transmits $\{M_0, V_i\}$ to UI.

Step 5. After receiving $\{M_0, V_i\}$, UI computes $(a_j \| a_i \| C_i) = M_0 \oplus h(K_{u,i}) \| h(SID) \| h(b))$. After obtaining $a_j$, HD$_j$ is able to calculate $RID_{new} = h(a_j \| RID_j)$ of UI. Assuming that HD$_j$ is controlled, a malicious attacker can perform a tracking attack on UI 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 $\{RID_j, M_j, M_i, V_j\}$ transmitted by GW to HD$_j$ in the second step of the login and authentication phase, and thereafter pretends that GW transmits again to HD$_j$. On receiving $\{RID_j, M_j, M_i, V_j\}$, HD$_j$ computes $(a_j \| a_i \| C_i) = M_j \oplus h(K_{u,j}) \| h(SID) \| h(b))$, $V_j = h(a_j \| a_i \| C_i \| RID_j)$, and verifies $V_j' = V_j$, 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 $\{RID_j, M_j, M_i, V_j\}$ to the HD$_j$, where $M_j = h(PU_j \| t) \oplus h_j$ is not authenticated. Since there is no timestamp, a malicious attacker can intercept $M_j$ and tamper it to $M'_j$. HD$_j$ receives it and computes the wrong $h(PU_j \| t) = M_j' \oplus h_j$;

then computes $SK' = h(h(PU_j \| t) \| a_j \| a_i \| a_i)$, $V_j' = h(SK' \| a_j \| h(PU_j \| t))$, and sends $\{M_j', V_j\}$ to GW. On receiving it, GW recovers $a_j = M'_j \oplus h(PD_i \| h_j)$ and computes $SK = h(h(PU_j \| t) \| a_j \| a_i \| a_j)$. Since the SK computed by HD$_j$ and GW do not match, GW fails in verifying $V_j'$ and terminates this phase. As a result, HD$_j$ and UI cannot agree on a session key.


In the third step of the login and authentication phase, CHO et al.’s [11] scheme does not work properly because $\{M_j, V_j\}$ transmitted from HD$_j$ to GW lacks the identity information of UI and HD$_j$. When HD$_j$ transmits $\{M_j, V_j\}$ to GW, GW computes $a_j = M_j \oplus h(PD_i \| h_j)$.

However, GW does not know which HD$_j$ is transmitting the message at this point. If GW wants to find PD$_i$ and PU$_i$, it must ask HD$_j$ for its identity information as well as that of UI with whom it has agreed on a session key. The message $\{M_j, V_j\}$ sent by HD$_j$ to GW is clearly missing $RID_j, DID_j$. 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 authentication phase in this section, as follows.

4.1. User Registration Phase.

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

$U_i \rightarrow RC$

Selects $ID_i, PW'_i$,

Generates $r_i$, Computes $PID_i = h(ID_i \| r_i)$, $PPW'_i = h(PID_i \| PW'_i \| r_i)$, $K_{u,i} = h(PU_i \| t \| r_i)$,

Computes $RID_i = h(PID_i \| K_{u,i})$, $y_i = h(RID_i)$.

Stores $\{RID_i, PID_i, PU_i, r_i\}$ into the GW

Fig 1. User registration phase

Step 1. UI 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
\[ K_{ij} = h(PU_i \| t \| r_j) \] for \( U_i \), where \( s \) is the master key of RC and \( t \) is the master key of GW, and then calculates \( RID = h(PID_i \| K_{ij}) \) and \( y_i = h(RID \| t) \). Afterwards, RC transmits \{RID, PIDo, PUo, r1\} to GW over a secure channel, and GW receives the information and stores it in memory. Then, RC sends \{RID, PIDo, KUo, y1\} 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:

\[ A_i = RID \oplus h(t \| PID_i) \]

\[ A_k = K_{ij} \otimes h(ID_i \| PPW_i \| r_j) \]

\[ X_i = r_t \oplus h(ID_i \| PPW_i) \]

\[ Y_i = y_j \oplus h(ID_i \| r_j) \]

and finally stores \( \{X_i, Y_i, V_i, A_j, A_j\} \) 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 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. The specific steps are as follows:

Step 1. \( U_i \) enters IDo and PPW in its mobile device, and the mobile device calculates \( r_t = X_i \oplus h(ID_i \| PPW_i) \), \( PID_i = h(ID_i \| r_t) \), \( PPW_i = h(PID_i \| PPW_i \| r_t) \), \( V_i = h(PID_i \| PPW_i) \), 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 \( y_j = Y_i \oplus h(ID_i \| r_j) \), \( RID = A_i \oplus h(rID \| PID_i) \), \( K_{ij} = A_j \oplus h(ID_i \| PPW_i \| r_j) \), and selects DIDo of HD to be accessed and calculates \( M_1 = DID \oplus h(K_{ij} \| PID_i \| T_1) \), \( M_2 = a_1 \oplus h(K_{ij} \| DID \| T_1) \), \( V'_1 = h(a_1 \| DID \| PID_i \| T_1) \) and verifies \( V_1 \neq V'_1 \), if the condition is not valid, GW terminates this phase. Otherwise, GW successfully authenticates \( U_i \) and retrieves \{CID, \( P_D, B_2\}\) according to DIDo and generates random number \( a_2 \) and timestamp \( T_2 \), calculates \( h_j = B_2 \oplus h(DID \| t) \), \( M_1 = (a_1, a_2, a_2 \| C_2 \| PPW_i \| r_1) \), \( M_2 = h_j \oplus h(PU_i \| t \| r_1) \), \( M_3 = h_j \oplus h(DID \| T_2) \), and finally transmits \{RID, M3, M4, V2, T2\} to HD over the public channel.

Step 3. Upon receiving \{RID, M3, M4, V2, T2\}, HD checks \( T_2 - T_1 \leq \Delta T \), If the message is fresh, HD computes \( X_j = h(SID_j \| b) \), \( a_2 \| a_2 \| C_j \| M_3 \| RID \| T_2 \), and finally computes \( R_j = PUF(C_j) \), \( D_j = Re_p(R_j, HS_j) \), \( h_j = D_j \oplus H_j \), \( h(PU_j \| t) = M_4 \oplus h_j \), \( SK = h(h(PU_j \| t) \| a_1 \| a_2 \| a_2) \), \( M_5 = a_2 \oplus h(K_{ij} \| X_i) \), \( V_3 = h(SK \| a_2 \| h(PU_j \| t) \| T_2) \), and transmits \{M5, V3, T3, RID, DID\} to GW over the public channel.

![Fig 2. Login and authentication phase](image-url)
In the login and authentication phase, Ui and HDj authenticate each other with the assistance of the GW. Firstly, GW verifies that $V'_i$ is equal to $V_i$, if it is, then both Ui and GW have the correct secret credentials $K_{Ui}$ and GW successfully authenticates Ui's identity. Similarly, HDj, GW and Ui authenticate $V'_2 = V_2$, $V'_3 = V_3$ and $V'_4 = V_4$ 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 Ui, GW, and HDj.

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$_j$\} transmitted by Ui to GW, because $M_i$ is invariant, attacker A can perform a tracing attack on Ui.

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

However, the improved scheme concatenates the timestamp $T_j$ in the calculation of the message $M_j$, so that $M_i$ is different for each transmission. Also, GW uses a random number $a_i$ that only the Ui can compute when updating the pseudo-identity of Ui. 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, Ui and HDj authenticate each other with the assistance of the GW. Firstly, GW verifies that $V'_i$ is equal to $V_i$, if it is, then both Ui and HDj agrees on the session key, and then computes $A_{new} = RID_{new} \oplus h(t_i \| PID_i)$ and updates it in the mobile device to update it.

5.3. Impersonation Attack

Since attacker A does not know the secret credentials $K_{Ui}$ and $K_{Dj}$ for authentication between Ui and HDj and GW, it cannot successfully impersonate legitimate Ui and HDj 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, Ui adds the current timestamp $T_j$ to each message transmitted, GW will determine whether $|T_i - T_j| \leq \Delta T$ 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 $M_i$ by intercepting the message \{RID$_i$, M$_1$, M$_2$, V$_2$\} transmitted by GW to HDj in the second step of the login and authentication phase, and making it impossible for Ui and HDj to agree on a session key. However, in the improved scheme, $M_i$ is added to the authentication message $V_2$, and if attacker A intercepts and tampers with message $M_i$, HDj 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 Ui and HDj 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 are 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>
<thead>
<tr>
<th>Table 2. Security features comparisons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schemes</td>
</tr>
<tr>
<td>[14]</td>
</tr>
<tr>
<td>[15]</td>
</tr>
<tr>
<td>[12]</td>
</tr>
<tr>
<td>[11]</td>
</tr>
<tr>
<td>Improved</td>
</tr>
</tbody>
</table>

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 $T_h$, $T_s$, $T_{app}$, $T_{pu}$, 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 $T_h=0.0026\text{ms}$, $T_f=1.989\text{ms}$, $T_{rpm}=1.989\text{ms}$, $T_p=0.12\text{ms}$ and $T_s=0.00325\text{ms}$.

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](image)

<table>
<thead>
<tr>
<th>Schemes</th>
<th>User</th>
<th>Home device</th>
<th>Gateway</th>
<th>Cost($\text{ms}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[14]</td>
<td>$2T_{\text{com}}+2T_f+7T_h$</td>
<td>$T_h+2T_f$</td>
<td>$T_{\text{rpm}}+3T_h+8T_f$</td>
<td>6.0307</td>
</tr>
<tr>
<td>[15]</td>
<td>$2T_{\text{com}}+6T_h$</td>
<td>$3T_h$</td>
<td>$T_{\text{rpm}}+7T_h$</td>
<td>6.0086</td>
</tr>
<tr>
<td>[12]</td>
<td>$3T_{\text{com}}+6T_h$</td>
<td>$2T_{\text{com}}+6T_f+7T_h$</td>
<td>$T_{\text{com}}+6T_h$</td>
<td>11.9808</td>
</tr>
<tr>
<td>Improved scheme</td>
<td>$15T_h$</td>
<td>$T_p+T_f+7T_h$</td>
<td>$12T_h$</td>
<td>2.1974</td>
</tr>
</tbody>
</table>

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


