Research Article

Two-Factor Authentication and Key Agreement Schemes for Smart Home Fingerprint Characteristics

Zhenpeng Liu 1, Zeyuan Li 1, Qingwen Zhang 1, Shuhui Dong 1, Jiahang Liu 1, and Yonggang Zhao 2

1School of Electronic Information Engineering, Hebei University, Baoding, Hebei 071002, China
2School of Management Engineering and Business, Hebei University of Engineering, Handan, Hebei 056038, China

Correspondence should be addressed to Yonggang Zhao; ygzhao@hbu.edu.cn

Received 28 September 2021; Revised 7 March 2022; Accepted 8 March 2022; Published 24 March 2022

Academic Editor: Jose M. Barcelo-Ordinas

Copyright © 2022 Zhenpeng Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Aiming at the potential security threat of personal information disclosure in smart homes, a two-factor authentication and key protocol scheme based on fingerprint feature was designed to ensure privacy and secure communication in a smart home environment. The scheme consisted of fingerprint authentication and a key protocol. Fingerprint features were extracted by fuzzy processor to ensure the stability of fingerprint features and effectively prevent the failure of fingerprint extraction caused by subtle changes. The key protocol was used to ensure the security of the communication process. Through performance comparison and security analysis, it was proved that the proposed scheme can meet the security requirements.

1. Introduction

As an important branch of the Internet of Things (IoT), a smart home brings great convenience to people’s life, but privacy protection also ushers in a great challenge. The sensors in smart homes are associated with a large number of user privacy, and there is a risk of privacy leakage in the process of data generation, transmission and processing. Therefore, the protection of user privacy has become an urgent problem in the smart home industry. If privacy security cannot be guaranteed, the popularity of smart home is bound to be seriously resisted. Most smart devices in the home are resource-limited, so the traditional public key cryptography systems such as RSA (Rivest Shamir Adleman) are not suitable for modern smart home devices, while the birth of lightweight authentication schemes provides the possibility for cryptography authentication. In recent years, many scholars have conducted research in the field of user identity authentication and key agreement.

Authentication and key negotiation protocols based on elliptic curve and symmetric and modular arithmetic encryption have been proposed. [1, 2, 3] These schemes are susceptible to different security attacks and have high computational and communication overhead. Wu et al. [4] have proposed an improved scheme based on elliptic curve cryptosystem and one-way hash function, which provides a variety of IoT security features. Song et al. [5] believe that Wu et al.’s scheme is vulnerable to user impersonation and denial of service (DoS) attacks. Renuka et al. [6] have presented a smart medical application authentication scheme based on elliptic curves, but this scheme cannot provide intractability. Li et al. [7] have integrated the Internet of Things with the industrial field and proposed an identity authentication protocol based on elliptic curve to ensure the security of wireless sensor networks in the industrial Internet of Things environment. Although this solution can resist various types of attacks, its communication overhead is very large. Gupta et al. [8] have proposed a lightweight authentication and key agreement protocol based on one-way hash function and XOR (exclusive OR) operation. However, it is not efficient in terms of storage and communication costs. Li et al. [9] proposed a three-factor user authentication protocol based on elliptic curve passwords. They claimed that their scheme is resistant to various security attacks and can correct biometric errors using fuzzy processing techniques. Liu et al. [10] have proposed an authentication protocol
based on elliptic curve, which lacks user preverification and uses two XOR values of unequal length. Shin et al. [11] proposed an authentication and key negotiation scheme that can protect user privacy in a 5G-integrated IoT environment, where users establish session keys via Elliptic Curve Diffie-Hellman (ECDH). Ali et al. [12] proposed a biometric-based authentication and access control protocol for wireless multimedia sensor networks using elliptic curve ciphers. They claim that their scheme is resistant to privileged insider, stolen smart card, and offline password guessing attacks. Ying and Nayak [13] have proposed a multiserver authentication key agreement scheme based on elliptic curve, which uses self-authenticated encryption technology for 5G networks. However, Haq et al. [14] have pointed out that this scheme may not be able to withstand offline password guessing attacks, user simulation attacks, and offline identity guessing attacks. Li et al. [15] have proposed an anonymous message authentication protocol in 5G framework by using discrete logarithm problem and the Diffie-Hellman problem. The verification of BAN (Burrows-Abadi-Needham) protocols shows that their protocols have good computing performance. Khan et al. [16] have proposed a cryptographic-based anonymous lightweight key agreement framework for smart grids using elliptic curve cryptography and secure hash functions. After analysis and verification, we have found loopholes in the login and authentication stages of [16].

Jiang et al. [17] have proposed a lightweight three-factor authentication and key agreement scheme for network integrated wireless sensor networks based on the Rabin cryptosystem. This scheme is difficult to implement and deploy in practical applications. Jung et al. [18] have proposed an efficient and securely enhanced key anonymous authentication protocol scheme. Fang et al. [19] have proposed a three-factor user authentication protocol in combination with smart cards and passwords while introducing biometrics. Sharma and Kalra [20] have proposed a lightweight authentication scheme for a cloud-based IoT environment. However, this solution was vulnerable to internal attacks and did not support anonymity and intractability. Jia et al. [21] proposed an anonymity-protected authentication scheme based on a fog architecture. However, if the private key of the server is lost, all the key material can be exported. And if the session information is leaked at the user side, it is vulnerable to session-specific ad hoc message attacks. Patonico et al. [22] introduced another mutual authentication key protocol for fog architecture that achieves anonymity, unlinkability, but also provides protection to satisfy full forward confidentiality. However, if a device is compromised by a stolen key, then that device may also be hijacked by an attacker. Shabisha et al. [23] propose a symmetric key-based authentication scheme that provides anonymity and unlinkability to the fog architecture and is independent of user interaction. Zhang and Liu [24] have proposed a multi-factor authentication protocol for short-distance communication between smart devices, but the protocol proposed in the article is suitable for short-distance communication that does not rely on additional hardware. Zhang et al. [25] have proposed a three-factor identity authentication scheme based on security outlines and Chebyshev polynomials, which can effectively solve the problems of repeated registration attacks, improper biometric processing, and low system robustness. Safkhani and Vasilakos [26] have proposed an ultralight authentication scheme based on radio frequency identification, but this scheme cannot maintain good forward and backward confidentiality. Roy et al. [27] designed an anonymous authentication protocol based on chaotic mapping using a fuzzy extractor for biometric feature extraction to be used in crowdsourced IoT, but the scheme could not provide perfect forward security in case of leakage of their private key. Amin et al. [28] have proposed an anonymous mutual authentication protocol for mobile users. He pointed out that the program can resist mobile device loss attacks and user impersonation attacks. However, the analysis found that the Amin’s solutions still cannot achieve the claimed security and are vulnerable to node capture attacks. Qu et al. [29] optimized the Amin scheme, designed a three-factor wireless sensor authentication key agreement scheme, and used BAN logic [30] and heuristic analysis to prove the security of the scheme. Islam et al. [31] proposed a provably secure three-factor protocol. However, since smart cards store incorrect password authentication parameters, the protocol is not resistant to offline password guessing attacks and is highly susceptible to password exposure, leading to key compromise user simulation attacks, and does not provide smart card revocation, making three-factor security and other security goals practically impossible to achieve. Cho [32] has proposed a hierarchical key tree efficient group key agreement protocol based on computational differential-Hellman hypothesis, which can be applied to frequently moving environments. Kumar, Vinod et al. [33] have proposed a scalable and efficient distributed key management protocol based on a trigeminal tree, which can reduce communication, computing, and storage costs. Masud et al. [34] proposed a lightweight user authentication scheme based on IOT-medicine. They claim that their scheme prevents simulation attacks and replay attacks and provides data privacy and anonymity. Wazid et al. [35] have proposed a lightweight authentication scheme based on bit XOR operation and one-way hashing function for the edge IoT environment (LDAK-EIOT). This scheme cannot withstand forgery attack, has poor scalability, and the password in the scheme cannot be updated locally. Zhou et al. [36] have also proposed a similar scheme, but the proposed scheme is vulnerable to security attacks such as replay attacks and internal attacks.

Recently, some scholars have proposed using physical unclonable function (PUF) for mutual authentication of the system [37]. PUF [38] refers to the introduction of random differences in integrated circuits during the manufacturing process. Just like human fingerprints, each PUF has its own unique physical characteristics. PUF is almost impossible to replicate, so the research on using PUF-enabled devices to achieve mutual authentication in identity authentication schemes is very successful. But its flaw is that it cannot verify the identity of the user who uses it. Chen et al. [39] proposed an effective mutual authentication and key negotiation scheme in a wireless sensor network environment using PUFs and biometrics. Gope
et al. [40] tried to input the user’s biometric thumbprint into the PUF, and then generated a biometric key to verify the user’s identity. In the proposed scheme, fingerprint biometrics are directly input to PUF during the registration phase and the authentication phase. However, this solution does not support noisy PUF environments. Fingerprint biometrics will change slightly over time, and subtle disturbances in the input will cause unpredictable PUF output, so the result of this scheme is unreliable. In addition, in this scenario, the user needs to provide a password to complete registration and authentication. This will increase the complexity of the system and also bring security risks to the system. In response to the problems above, this paper has proposed an authentication and key agreement scheme based on fingerprint characteristics and PUF while using a fuzzy processor to extract fingerprints to solve the problem of fingerprint extraction failure caused by weak fingerprint differences.

The main contributions of this paper are as follows:

1. Propose a two-factor authentication and key agreement scheme based on fingerprints. This solution not only meets various security requirements but also uses lightweight operations such as XOR and hash functions, which is very suitable for resource-constrained smart home network environments.

2. Use BAN logic to prove the safety of the proposed scheme. And using objective third-party evaluation criteria compared with existing schemes, it is shown that the scheme is able to meet the required security performance and resist various attacks.

2. Smart Home Two-Factor Authentication and Key Agreement Scheme

2.1. Scheme Description. The scheme uses a fuzzy extractor to generate the user keystore $K_u$ from the fingerprint biometric template obtained in the registration phase and restore $K_u$ from the fingerprint biometric template obtained in the login phase. In the fuzzy extraction technology, when a biometric $B$ is input, a key $K_u$ can be generated in a fault-tolerant way. When the input $B'$ and $B$ differ little, the key $K_u$ output by the fuzzy extractor remains unchanged. When biometric $B'$ is input to restore $K_u$, an auxiliary public information $P$ is generally required.

The fuzzy extraction technology consists of the following two algorithms:

1. Random number generation algorithm $Gen(B) = (K_u, P)$. Enter the user biometric $B$ into $Gen(\cdot)$, and the output is a key $K_u$ and an auxiliary string $P$.

2. Random number recovery algorithm $Rep(B', P) = K_u$. Enter the user’s biometric $B'$ and auxiliary string $P$ into $Rep(\cdot)$, and $Rep(\cdot)$ outputs the key $K_u$.

Figure 1 shows the system model of the smart home two-factor solution.

In the scheme, the user’s biometric information will not be stored on any device, which can completely eliminate the risk of the biometric information being leaked. The system model includes three types of entities: the user, the home gateway, and the sensor. No password and session key negotiation is required between the user and the sensor. The scheme consists of three stages: registration, login, and mutual authentication and key agreement. The symbols and meanings used in this paper are shown in Table 1.

2.2. Adversary Model. We refer to the adversary models of Qiu et al. [41], Kwon et al. [42], and Wang et al. [43] and assumed that the adversary’s capabilities are as follows:

1. Steal information from smart devices by extracting parameters from smart devices using power analysis techniques.

2. Pretend to be a normal user as well as register as a legitimate user.

3. Steal user biometrics from end devices and clone them to perform impersonation attacks.

4. Performing various attacks such as password guessing attack, session-specific temporary information attack, and man-in-the-middle attack.

5. Intercept, modify, delete, or resend messages from open channels (unsecured channels).

2.3. Interactive Process Description of Each Stage

2.3.1. Registration Stage. The registration phase is divided into four steps to realize the communication between sensor $S_j$ and user $U_i$ through secure channels. The green section in Figure 2 shows the interaction between the user and the sensor during the registration phase.

Step 1: The user selected identity $ID_i$, and input fingerprint $F_i$ into the device. The user can be extracted from the input fingerprint $F_i$, fingerprint biometric template, and randomly generated a challenge $C_i$ and a random number $N_i$.

Step 2: Client computes PUF output $R_i = PUF_i(C_i)$; the user key $K_u$ and secondary data $Gen(\cdot)$, of which $(K_u, FA) = FE.Gen(F_i)$ were obtained from fingerprint biometric template by using fuzzy processor. Then, calculate $W = h(ID_i \parallel K_u)$, $C_i' = C_i \oplus h(K_u)$, $AID_i = ID_i \oplus h(K_u \parallel N)$. Finally, the user sent $\{AID_i, (C_i', R_i), W\}$ and a registration request $Reg_i$ to the server over the secure channel.

Step 3: After the server receives the registration request from the user, it first checks the uniqueness of $AID_i$. Then, the server randomly generates private key $K_s$ and random user number $e$ and uses the data transmitted by the client to calculate $E_i = h(K_s || e) \oplus W$. Store $\{AID_i, (C_i', R_i), e, K_s\}$ to the server and send $E_i$ back to the client via a secure channel.

Step 4: After receiving $E_i$, the client computes $V = h(ID_i \parallel K_u \parallel N)$, $N^* = N \oplus h(ID_i)$ and $FA^* = h(ID_i \parallel N) \oplus F_A$. Finally, the user stores the information $\{h(\cdot), E_i, V, N^*, FA^*\}$ to the mobile device.
2.3.2. Landing Stage. During the login stage, the user needs to enter his identity \(ID_i\) and the fingerprint used in the registration stage. After the user mobile device extracts the fingerprint template \(F_i\), the following steps are performed. The yellow part in Figure 2 shows the interaction between the user and the sensor during the login stage.

Step 1: After the client verifies the user’s identity successfully, it can retrieve the stored information in the device, decode, and calculate \(N = N^* \oplus h(ID_i)\) and \(FA = h(ID_i \| N) \oplus FA^*\).

Step 2: Use the fuzzy processor to extract the key \(K_u\), where \(K_u = FE.Rec(F_i, FA)\).
Step 3: Calculate whether \( h(ID_i) \| K_u \| N = V \) is true. If not, the login will be terminated. If so, the login request can be continued.

Step 4: The client generates a random number \( N_u \) at first and then computes the value of \( W = h(ID_i) \| K_u \), \( K = E_i \oplus W \), \( A_1 = N_u \oplus K \). \( AID = ID_i \oplus h(K_u) \| N \), \( A_3 = (K \| AID) \| N_u \), \( AID' = AID_1 \oplus N_u \) in turn.

The user completes the login request by sending a message \( \{AID'_1, A_1, A_2 \} \) to the server.

2.3.3. Authentication and Key Negotiation Stage. After the server receives the \( \{AID'_1, A_1, A_2 \} \), it begins mutual authentication and session key negotiation. The pink section in Figure 2 shows this process visually.

Step 1: The server first decodes \( N_u \) from \( N_u = C_i \oplus h(K_u) \| e \), then computes \( AID = AID_1 \oplus N_u \).

Step 2: The server checks the validity of \( AID \), if invalid, the challenge-response pair \( (C_i, R_i) \) is retrieved and loaded. Otherwise, the session is terminated.

Step 3: Calculate and verify that \( A_2 = h(h(K_u) \| e) \| AID) \| N_u \) is true. Validation continues if it is valid, or terminates the session if it is not.

Step 4: The server generates a random number \( n \), computes \( A_3 = N_u \oplus h(K_u) \| e \), \( A_4 = h(h(K_u) \| e) \| AID) \| N_u \| N_2 \), \( A_5 = C_i \oplus h(N_u \| N_2) \), then sends a composite response message to the user.

Step 5: After the user receives message \( \{A_3, A_4, A_5 \} \), first decode \( N_u \) from \( N_u = A_3 \oplus K_u \), and then verify whether \( A_4 = h(K) \| AID) \| N_u \| N_2 \) is true. If the formulais true, it will go on; if not, it will terminate.

Step 6: Calculate challenge \( C_i = A_3 \oplus h(N_u \| N_2) \oplus h(K_u) \| e \), response \( R_i = PUF(C_i) \). \( X_{uw} = FE.Gen(R_i) \), \( A_6 = h(K) \| N_u \| N_2 \| M \), session secret keys \( SK = h(AID) \| X_{uw} \| N_u \| N_2 \) and \( A_7 = h(SK) \| X_{uw} \| N_2 \| M \), where \( M \) is the secondary data. Finally, sent \( \{A_6, A_7 \} \) to the server.

Step 7: After the server receives \( \{A_6, A_7 \} \), Decodes the auxiliary data \( M = A_6 \oplus h(K_u) \| e) \| N_2 \), then calculates \( X_{uw} = FE.Rec(R_i, M) \) and \( SK = h(AID) \| X_{uw} \| N_u \| N_2 \), and finally verifies whether \( A_2 = h(SK) \| X_{uw} \| N_2 \) is true. If so, the authentication is successful; otherwise, the authentication fails.

3. Security Analysis and Discussion

3.1. Evaluation Metrics. In order to make a fair comparison, we compared the proposed scheme with existing schemes using objective, third-party evaluation criteria. Given the redundancy and ambiguity of earlier sets of criteria, we referred to the sets of criteria provided by Wang et al. [44], Gope et al. [40], Erdem et al. [45], and Smet et al. [46] and concluded that the proposed scheme should satisfy the following evaluation metrics:

\( C1: \) No password verifier-table: user’s password should not be stored in the sensors and gateway devices where the validity of the user’s password information can be checked through the database provided by the service provider.

\( C2: \) Password friendly: users can set and change passwords by their own.

\( C3: \) No password exposure: users are free to choose their identity and does not send \( ID \) in plain text during the registration phase. The user only submits \( AID \) and \( W \) to the server, where \( AID = ID_i \oplus h(K_u) \| N \), \( W = h(ID_i) \| K_u \). Where the secret values \( K_u \) and \( N \) are protected by hash functions, so no insider can extract the user’s secret information. In addition, the secret value \( K_u \) must be extracted through the biometric information, which can only be mastered by the user and cannot be obtained by insiders. Without the secret information of \( K_u \) and random number \( N \), no one with access to the server would have access to the user’s \( ID \).

\( C4: \) No smart card loss attack: when user’s smart card is lost, attackers cannot obtain or change the user’s password through online, offline, or hybrid guessing attack, and also cannot pretend to be a user to access the system.

\( C5: \) Resistance to known attacks:

(1) Stolen verifier attack: user’s identity and biometric information are not stored on the device, and the user identity is not contained in any message in plain text. Therefore, the attacker cannot obtain valuable user information from the device, so it can effectively prevent the leakage of sensitive information. Assuming an attacker has stolen the user’s mobile device and has extracted the value of \( h(\cdot), E_i, V, N_s, FA^* \), the hash function can be used to protect this information. With \( N_s = N \oplus h(ID_i) \). If an attacker wants to get the value of \( ID \), he needs to know the value of \( N \), and the value of \( N \) depends on the value of \( ID \), so \( ID \) and \( N \) play a mutually protective role, preventing the attacker from getting messages. If an attacker wants to get \( ID \) from other data extracted from a mobile device, he needs not only \( N \), but also \( FA \) or \( K_u \), and the thief must have the users’ biometric. Thus, it can be seen that the proposed scheme can resist Stolen verifier attack.

(2) User impersonation attack: a fake user must generate a valid login message in order to simulate a legitimate user. However, the fake user does not have access to the secret \( ID \) of the legitimate user, and therefore cannot obtain more secret values such as \( N, FA \), etc. Even if the fake user has obtained \( N \) and \( FA \), a valid login message still cannot be generated, because the user’s fingerprint template \( F_i \) only belongs to the legitimate user, and the fake user cannot obtain the legitimate user’s key \( K_u \), therefore, the fake user cannot calculate the value of \( \{AID'_1, A_1, A_2 \} \). Therefore, the scheme can resist the user impersonation attack.

(3) Offline password guessing attacks: the scheme does not need password authentication, it only uses the key \( K_u \) extracted from the user’s biometric to encrypt the user terminal data, and the attacker will never have the opportunity to perform password guessing attack, so our scheme does not have the risk of password guessing attack.

(4) Parallel session attack: assuming that the attacker already knows the temporary session information
where SK server need to independently calculate the session key authentication and key negotiation, both the user and the card and apply for a new one. This is convenient for users.

The server authenticates the user by sending a message $A4$ to the user after receiving the authentication message to respond to authentication. The server authenticates the user by sending a message $A4$ to the user, and the user responds to authentication by sending a message $A4$ to the server. Therefore, only user and $PUFi$ information with correct biometric characteristics can successfully complete mutual authentication. In addition, the scheme can resist camouflage attacks on both client and server, thus ensuring the security of mutual authentication.

C6: Sound repairability: in the event of theft or loss of a smart card, the user can request revocation of the stolen smart card and apply for a new one. This is convenient for users.

C7: Provision of key agreement: in the stage of user authentication and key negotiation, both the user and the server need to independently calculate the session key $SK$, $SK = h(AID_i || X_{us} || N_u || N_s)$, where the value of $X_{us}$ is only open to the user and the server, and it must be generated by the PUF of the user in the session, and SK cannot be calculated in the case of unknown $X_{us}$. So the attacker cannot obtain the key $SK$. So the scheme is not vulnerable to temporary information for a particular session.

C8: No clock synchronization: there is no need to keep the clock synchronized before the user and the sensor, so the user is not affected by the time when authenticating.

C9: Timely typo detection: when a user enters wrong ID and password information when logging in, the server is able to provide timely error feedback to the user.

C10: Mutual authentication: in the mutual authentication stage, the user sends a message $A_1$ to the server for authentication, and the server sends a message $A_2$ to the user after receiving the authentication message to respond to authentication. The server authenticates the user by sending a message $A_2$ to the user, and the user responds to authentication by sending a message $A_2$ to the server. Therefore, only user and $PUFi$ information with correct biometric characteristics can successfully complete mutual authentication. In addition, the scheme can resist camouflage attacks on both client and server, thus ensuring the security of mutual authentication.

C11: User anonymity: in order to fully protect users’ privacy, the proposed scheme needs to have strong anonymity which is untraceable. In our scheme, the real identity of the user is encrypted with the user key $K_u$, extracted from the biometric and the randomly generated secret number $N$ in the registration stage. $AID_i$ is obtained from $AID_i = ID_i \oplus h(K_u || N)$, and only the user has the biometric information, and only the user can know the values of the keys $K_u$ and $N$. Therefore, the attacker cannot retrieve $ID_i$ values from $AID_i$. During the login phase, the user sends $\{AID'_i, A_1, A_2\}$ to the server, where $AID'_i = AID_i \oplus N_u$. Because the user’s mobile device randomly generates $N_u$ for each session, the parameters in the message are dynamic, and all values in the login message are different in the session, which greatly reduces the possibility of traceability. Therefore, the proposed scheme can provide intractability and user anonymity, so as to further protect user privacy.

C12: Forward secrecy: our scheme uses different random values $N_u$ and $N_s$ in each session to calculate the session key $SK = h(AID_i || X_{us} || N_u || N_s)$, so the values of $N_u$ and $N_s$ must be known if you want to calculate the session key $SK$. Even if an attacker intercepts all the information passing through the public channels, the value of $X_{us}$ is unknown and thus cannot calculate the key $SK$. Even if the attacker $U_a$ gets a challenge $C_p$, he still needs to compute the response $R_i$ in each session using $PUFi$ installed on the user’s mobile device to obtain the $X_{us}$. Due to the confidentiality of $PUFi$, the attack cannot be carried out and the attacker cannot rebuild the established session key. Therefore, our scheme has perfect forward confidentiality.

### 3.2 BAN Logic Proof

In this section, BAN logic is used to prove the correctness of this scheme. The symbols and meanings in BAN logic are shown in Table 2.

BAN logic rules are as follows:

(i) Message meaning rule 1: the meaning of $P |\equiv P \xrightarrow{K} Q, P \oplus \langle X \rangle_i |P|=Q \sim X$ is that if principal $P$ believes that the key $K$ is Shared between $P$ and $Q$, and $P$ sees the message $X$ encrypted by the key $K$, then $P$ believes that $Q$ has said the message $X$.

(ii) Message meaning rule 2: the meaning of $P |\equiv P \xrightarrow{Y} Q, P \oplus \langle X \rangle_i |P|=Q \sim X$ is that if subject $P$ believes that only $P$ and $Q$ know the secret $Y$, and $P$ sees the message that $X$ combines with $Y$, then $P$ believes that $Q$ has said the message $X$.

(iii) Nonce verification rule: the meaning of $P |\equiv \#(X), P |\equiv Q \sim X |P|=Q |\equiv X$ is that if subject $P$ believes that $X$ was sent at the current moment, and $P$ believes that $Q$ has said $X$, then $P$ believes that $Q$ believes that $X$ is true.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Roy et al. (2018)</td>
<td>[27]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Islam et al. (2018)</td>
<td>[31]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Jia et al. (2019)</td>
<td>[21]</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Patonico et al. (2019)</td>
<td>[22]</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Gupta et al. (2019)</td>
<td>[8]</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Gope et al. (2019)</td>
<td>[40]</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Li et al. (2020)</td>
<td>[9]</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Shabisha et al. (2020)</td>
<td>[23]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ali et al. (2020)</td>
<td>[12]</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Chen-Chen (2021)</td>
<td>[39]</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Masud et al. (2022)</td>
<td>[34]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ours</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
(iv) Jurisdiction rule: the meaning of \( P \equiv Q \iff X, P \equiv Q \iff X/P \equiv X \) is that if subject \( P \) believes that \( Q \) has jurisdiction over \( X \), and \( P \) believes that \( Q \) believes \( X \), then \( P \) believes \( X \).

(v) Freshness conjunction rule: the meaning of \( P \equiv Q \iff (X, Y)/P \equiv Q \iff (X, Y) \) is that if subject \( P \) believes that \( X \) is fresh, then \( P \) believes that \( (X, Y) \) is fresh.

(vi) Belief rule: the meaning of \( P \equiv Q \iff (X, Y) \) is that if \( P \) believes \( Q \) believes \( (X, Y) \), then \( P \) believes \( Q \) believes \( X \).

Server \( S \) and user \( U_i \) achieve the security goal of mutual authentication:

\[
\text{Goal 1: } U_i \equiv S \iff U_i \xrightarrow{SK} S.
\]

\[
\text{Goal 2: } U_i \equiv U_i \xleftarrow{SK} S.
\]

\[
\text{Goal 3: } S \equiv U_i \iff U_i \xrightarrow{SK} S.
\]

\[
\text{Goal 4: } S \equiv U_i \xrightarrow{SK} S.
\]

Safety assumption

\[
\text{H1: } U_i \equiv \#N_i,
\]

\[
\text{H2: } S \equiv \#N_i,
\]

\[
\text{H3: } U_i \equiv U_i \iff S \equiv h(K_i[e]),
\]

\[
\text{H4: } S \equiv U_i \iff S \equiv h(K_i[e]),
\]

\[
\text{H5: } U_i \equiv U_i \iff S \equiv X_{u_i},
\]

\[
\text{H6: } S \equiv U_i \iff S \equiv X_{u_i},
\]

\[
\text{H7: } U_i \equiv S \iff U_i \xrightarrow{SK} S,
\]

\[
\text{H8: } S \equiv U_i \iff U_i \xrightarrow{SK} S
\]

Proof Process

\[
V1: U_i \equiv (AID_i, N_u_i, N_i) \iff (AID_i, N_u_i, N_i)
\]

According to security hypothesis H3, message meaning rule 1 and V1 can be obtained as follows:

\[
V2: U_i \equiv S \iff (AID_i, N_u_i, N_i)
\]

According to the safety hypothesis H1 and the fresh series rule can be obtained as follows:

\[
V3: U_i \equiv \#(AID_i, N_u_i, N_i)
\]

According to V2, V3 and random number verification rules, it can be obtained as follows:

\[
V4: U_i \equiv S \iff (AID_i, N_u_i, N_i)
\]

According to V4, H1, H2, H5, SK = \( h(AID) \| X_{u_i} \| N_u_i \| N_i \), fresh series rule and random number verification gauge, we can get:

\[
V5: U_i \equiv S \iff U_i \xrightarrow{SK} S \text{(Goal 1)}
\]

According to V5, H7 and the jurisdiction rules:

\[
V6: U_i \equiv U_i \xrightarrow{SK} S \text{(Goal 2)}
\]

\[
V7: S \equiv (U_i \xrightarrow{SK} S \equiv N_i)
\]

According to H6, V7 and message meaning rule 2:

\[
V8: S \equiv U_i \iff (U_i \xrightarrow{SK} S \equiv N_i)
\]

According to H2 and fresh series rule, it can be obtained as follows:

\[
V9: S \equiv \#(U_i \xrightarrow{SK} S \equiv N_i)
\]

According to V8, V9 and random number verification rules:

\[
V10: S \equiv U_i \equiv (U_i \xrightarrow{SK} S \equiv N_i)
\]

According to the trust rule and V10, we can get:

\[
V11: S \equiv U_i \equiv U_i \xrightarrow{SK} S \text{(Goal 3)}
\]

According to V11, H8 and the jurisdiction rules:

\[
V12: S \equiv U_i \xrightarrow{SK} S \text{(Goal 4)}
\]

Goals 1–4 above clearly show that our solution achieves mutual authentication with the user and the server.

3.3. Performance Analysis and Comparison. We compared our proposed scheme with 12 representative schemes for the 12 evaluation metrics and use a table with reference to the literature [47, 48] to visually reflect the comparison results. As shown in Table 3, “√” means that the attack can be resisted and “×” means that the attack cannot be resisted.

As can be seen from Table 3, our scheme can satisfy the 12 evaluation metrics.

For decades, protocol designers have been working to break old protocols and propose new ones, and the proposed protocols will be broken within a few years, so provable security has become an indispensable tool for analyzing and evaluating new cryptographic protocols [49]. However, provable security has its limitations, and hundreds of schemes claiming to be “provably secure” have failed. In general, the process of providing “provably security” for a protocol requires making some cryptographic assumptions under which any provably secure protocol satisfies its goals within some security model, rather than achieving provable security in a particular protocol. Most two-factor schemes with formal proofs have been found to have serious problems soon after they were proposed [50, 51]. This indicates that having a formal (but inadequate) security model does not ensure actual security. Therefore, we employ a multifaceted evaluation and provide some heuristic analyses in order to strive for proposed protocols that can guarantee their security under existing conditions.

4. Conclusion and Future Work

Aiming at the security defects of existing identity authentication and key agreement schemes, a two-factor authentication and key agreement scheme based on fingerprint biometrics and PUF is proposed, and fuzzy extraction technology is used to improve the stability of the scheme. The BAN logic is used to prove the protocol, and the security analysis proves that our solution can resist various known security attacks. Finally, a comparative analysis of the proposed scheme with other related schemes shows that the scheme in this paper is safe and effective for actual user authentication applications.

In the next step, we consider applying mobile-edge technology to the smart home environment to solve the problem of limited computing capacity of smart home terminal devices and combine the two-factor authentication and key scheme mentioned in this paper with mobile-edge computing technology to ensure the security of a smart home environment.

Data Availability

The data used to support the findings of this study are included within the article.
Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the Natural Science Foundation of Hebei Province, China under Grant No. F2019201427 and Fund for Integration of Cloud Computing and Big Data, Innovation of Science and Education of China under Grant No. 2017A20004.

References


[27] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. H. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for Mobile Information Systems


