IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON DATA MINING FOR INTERNET OF THINGS

Received September 5, 2019, accepted September 23, 2019, date of publication September 30, 2019,
date of current version October 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2944515

Anti-Synchronization and Robust Authentication for Noisy PUF-Based Smart Card

YULING CHEN[1], WEI KONG[2,3], AND XINZHAO JIANG[2,3]
[1]Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
[2]Peng Cheng Laboratory, Cyberspace Security Research Center, Shenzhen 518000, China
[3]Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing 210044, China

Corresponding author: Wei Kong (wei_kongnuist@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61962009, in part by the Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2018BDKFJJ005 and Grant 2018BDKFJJ013, in part by the Major Scientific and Technological Special Project of Guizhou Province under Grant 20183001, in part by the Talent Project of Guizhou Big Data Academy and Guizhou Provincial Key Laboratory of Public Big Data under Grant [2018]01, in part by the Peng Cheng Laboratory Project of Guangdong Province under Grant PCL2018KP004, in part by the National Natural Science Foundation of China under Grant 61922045, Grant U1836115, and Grant 61672295, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20181408, and in part by the Foundation of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2018BDKFJJ003.

ABSTRACT Smart card is indispensable part in our daily life, which brings us many conveniences including e-commerce and m-commerce service. However, because of the limited computation resource, the remote authentication between smart card and server is vulnerable to be attacked over insecure communication channel. Until now, many authentication schemes are proposed with their own pros and cons. Note that most of them are based on Elliptic curve cryptography, which are vulnerable to the card lose attack and desynchronization attack, where some schemes add a random number in verifier-value to resist the card lose attack and store both the old and new pseudo-identities between authenticator and the corresponding authenticated party to withstand desynchronization attack. However, the random number stored in card memory can be extracted and the new conversation may be blindly blocked by adversary. Hence, in this paper, we propose a novel authentication protocol that can utilize physical unclonable function (PUF) and elliptic curve cryptography (ECC) to protect the random number and support offline updating if online updating is blocked, which can be proven safe in formal security analysis. Meanwhile, we also introduce the robust PUF to prevent the modification of help data. Finally, our scheme is efficient by comparing with other related schemes in computation and communication overhead.

INDEX TERMS Anti-synchronization, authentication, PUF, smart card.

I. INTRODUCTION

With the rapid development of Internet, smart card becomes an integral part in various representative scenarios, like e-commerce and m-commerce. Hence, data mining in smart card data is increasingly used to investigate consumer behavior and the demand characteristics. It is non-neglectable fact that remote authentication is indispensable part between terminal user and server to ensure the security and integrity of data, and to provide solid and secure foundation for data mining. In other words, one communication party should evince authenticity by corroborative evidence to corresponding communication party [1], [2]. The core component of mutual authentication is user authentication, because authorized entity and unauthorized entity should be distinguished for ensuring the confidentiality and integrity of data. As we known, the user side is resource-constrained device, like smart card, which is vulnerable to various attack including card loss attack, password guessing attack, denial of service attack so on and so forth. Hence, it is an open problem to design secure and efficient authentication protocol in public channel for smart card.

In the remote authentication, the universal conventional mechanism is the combination of password and ID [3], which user can login the server only if both password and ID are correct. Nevertheless, the mechanism faces two serious security issues: first, password table leakage problem. Second, impersonation attack problem. Generally, maintaining the confidential password table in back-end server is the central of two problems. Hereafter, Yang and Shieh [4]

The associate editor coordinating the review of this manuscript and approving it for publication was Chun-Wei Tsai.

firstly introduced smart card authentication scheme without storing password verification table so that the system can be stay stable, because the user accounts cannot be leaked. Hence, before Wang *et al.* [5] proposed refined criteria set, so many protocols [6], [7] were proposed to achieve no password-related verification storing in server. However, it is not difficult to see that, if no user sensitive-related information storing in the server, server cannot distinguish the revoked user from valid user, which is inherent conflict in aforesaid protocols. The next important issue is that the static of user identity, which may lead to the leakage of user's partial login information or sensitive information such as shopping, location or preference. To resolve the static user ID issue, user anonymous mechanism [43], [44] and dynamic user ID technology are employed in many related researches. However, as to anonymous mechanism, how to achieve the limited anonymity without trusted third party is remaining under research.

Hence, no card-related data storing in the server at all should not emphasized in our proposed scheme, and we prefer to achieve trade-off between on-card related information stored in table and distinguishing valid user from invalid user. Then, in our proposed scheme, dynamic user ID technology [45] is utilized to prevent the leakage of user privacy. In the part of literature reviewing, three mainly types of authentication schemes are investigated to present the advantages of ECC-based scheme and the loopholes in current ECC-based scheme.

A. RELATED WORK

Recently, researchers have proposed many kinds of identity authentication schemes in smart card, which mainly are hash-based, state-based and ECC-based identity authentication protocols and each has their own merits and demerits. In 1981, Lamport [3] proposed the first hash-based scheme which is vulnerable to stolen-verifier attack and inefficient in managing password table. Then many authentication schemes (e.g., [28], [29], [33]) try to achieve no sensitive password table on the server. However, Wang *et al.* [5] pointed out that there is an inherent deficiency between no-verifier table and smart card revocation. In addition, although many attempts are continuing to be done. For example, in 2014, Ramesh and Bhaskaran [8] proposed a hash-based remote authentication scheme which can resist denial-of-service attack and temper attack, but the fatal deficiency is that user cannot change the password freely. In 2016, Rafidha *et al.* [9] resolved aforementioned issue and introduced zero knowledge during authentication phase. Only little progress has been made, because almost every hash-based scheme cannot resist physical attack and has no resilient solution like PUF-based protocols. As to status-based authentication, these status-based remote authentication schemes [10], [30], [42] can resist spoofing attack and only require less computation overhead. However, in these cases, adversary can easily break synchronization between device and server.

Moreover, public key cryptography has been proved to be more confidential and secure in remote authentication but with higher computational cost and memory overhead than aforementioned types. However, because of the characteristic of elliptic curve cryptography(ECC), it can maintain lower computational cost while supporting high security performance, which meets all requirements of security authentication. In 2012, Islam and Biswas [11] proposed an improved ECC-based password authentication scheme which can remedy the security weakness of Lin and Hwang [12] such that impersonation attack and stolen-verifier attack. However, in that year, Li [13] claimed that [11] cannot resist the inside attack, password guessing attack and stolen verifier attack, and fulfilled these pitfalls by proposing an improved anonymity authentication scheme in smart card. Nevertheless, Wang *et al.* [5] investigated and revealed some loopholes in that scheme, which is prone to card loss attack and desynchronization attack. Li's [13] detailed protocol and attacks on this protocol was elaborated in Wan *et al.* [5] paper, and it is not difficult to see that, adversary can offline guess the password in a polynomial time because the secret parameter stored in card memory. Moreover, if only adversary changes the single transcript of the updated data, it will completely destroy the synchronization between user and server. Furthermore, many recent works [31], [32], [37] are proposed to address the drawbacks of the multi-server authentication, but the card loss attack is still a threat to authentication of smart card whatever in single server or multi-server.

B. MOTIVATION

As aforesaid schemes shown, we ought to design an improved protocol that can efficiently address offline password guessing attack under side channel attack and desynchronization attack. Our protocol seeks ways to address these issues: for that we investigate various latest protocols and inspired by the physical characteristics of PUF, which are unduplicatable because of the deviation of manufacturing process and unpredictability of one-way function.

1) If user lose the control of smart card, adversary can extract password-related verifier by side-channel attack and then execute off-line password guessing attack to acquire the correct password. Hence, password-related verifier should not be stored in card memory.

2) The synchronization between communication parties are easy to be blocked and it is vulnerable to be blindly blocked again by adversary if storing both old and new pseudo-identities in communication parties.

3) Under noisy PUF environment, our proposed scheme should ensure the integrity and correctness of response. Moreover, if adversary can modify the help data in fuzzy extractor, our proposed scheme should have ability to detect fault rather than output wrong value.

C. OUTLINE

The reminding parts are depicted as follows: Preliminary knowledge and our contributions are presented in

Section 2 and 3, respectively. In Section 4, we detailed defined the system model and adversary model. Our authentication protocol is elaborated in next section. In Section 6, we give the system security analysis in terms of card loss attack, desynchronization attack, robustness, anonymity and weak-PUF attack. Computational cost and communication cost are presented in Section 7. Finally, the conclusion and future work are given in Section 8. It is worth noting that, the notations described our proposed scheme are listed in Table 1.

TABLE 1. Notations used in this paper.

Notations	Description
G	base point of elliptic curve $E(\mathbb{F}_p)$
P_s, d_s	public key and private key of server
$h(*)$	one-way hash function $\{0,1\}^* \rightarrow \{0,1\}^K$
$H(*)$	one-way hash function $\{0,1\}^* \rightarrow Z_p^*$
ID, TID_i	user ID and temporary ID
C_i, R_i, hd_i	challenge, response and help data
k_i	key of fuzzy extractor
N_s	random number generated by server
P_c, PW_c	verifer value and password of card
SK, sk	symmetric key and session key
$\|\|$	Concatenation operation
XOR	Exclusive-OR operation

II. PRELIMINARY KNOWLEDGE

A. PHYSICAL UNCLONABLE FUNCTION (PUF)

Microelectronic chip attached to PUF [34]is the core of smart card, which can significantly improve the security against reverse engineering attacks on chip. With PUF, the digital device need not store the long-term key and can resist any tamper attack to chip.

PUF: $\mathcal{K} \times \mathcal{C} \rightarrow \mathcal{R}$, is actually a challenge-response pair(CRP) which can be represented as $R = PUF_T(C)$, where $\mathcal{K}$ is the physical parameters of chip, $\mathcal{C}$ is the challenge message, and $\mathcal{R}$ is the response of PUF function. However, in noisy PUF environment, the response may have little different in different session which can be represented as $R' = PUF_T(C)$.

B. FUZZY EXTRACTOR (FE)

Fuzzy Extractor [18] $FE(x, y)$ mainly consists of key generate algorithm $FE.Gen()$ and reconstruction algorithm $FE.Rec()$. We take the R as input and key generate algorithm will output key k and help data hd as follows, where R is the response of PUF.

$$FE.Gen(R) = (k, hd)$$

Hereafter, if we take help data hd and response with noisy R' as input, reconstruction algorithm will recover the key k as follows if the hamming distance between R and R' is less than d.

$$FE.Rec(hd, R') = (k)$$

C. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

We assume that $\mathbb{F}_p$ is a finite filed with order p and a elliptic curve $E : Y^2 = X^3 + AX + B$ on $\mathbb{F}_p$, where A, B satisfy $4A^3 + 27B^2 \neq 0$ and p is an odd prime, which can be represented as:

$$E(\mathbb{F}_p) = \left\{(x, y) : x, y \in \mathbb{F}_p \text{ satisfy } Y^2 = X^3 + AX + B\right\} \cup \{\mathcal{O}\}.$$

Then G is the basic point of $E(\mathbb{F}_p)$ over $\mathbb{F}_p$ together with an infinity point $\mathcal{O}$.

ECC mainly includes three well-known schemes which are 1) Elliptic Curve Integrated Encryption Scheme (ECIES), 2) Elliptic Curve Diffie-Hellman key agreement scheme (ECDH), 3) Elliptic Curve Digital Signature Algorithm (ECDSA) [39], [40]. First of all, each scheme will agree on some domain parameters $T = (p, a, b, G, n, h)$ at the desired security level. Then entity will establish an elliptic curve key pair $(d, Q = dG)$ associated with T. Note that, each scheme is operating on the elliptic curve and they have the same security level with short key size compared with original encryption, key agreement and signature schemes.

Definition 1 (Elliptic Curve Discrete Logarithm Problem (ECDLP)):

We assume that a elliptic curve E on finite field F, where P, Q is on $E(\mathbb{F}_p)$. For $n \in Z_p^*$, it is easy to calculate $Q = nP$. However, for given P and Q, it is infeasible to find n in polynomial time. Let $Adv_{\mathcal{A}}^{ECDLP}$ represents the advantage of $\mathcal{A}$ get $n \in Z_p^*$ from $Q = nP$. Then under ECDLP hard problem, the possibility of A can solve the ECDLP is negligible [35], which can be represented as follows:

$$Pr[Adv_{\mathcal{A}}^{ECDLP}] = Pr[n \in Z_p^* | Q = nP] \leq \xi,$$

where ξ is a negligible possibility.

D. DESYNCHRONIZATION ATTACK

Desynchronization attack [36] is existing in these schemes that need to synchronously update the shared secret key. If adversary blocks partial sessions of protocol, so that the key of one party of the protocol is updated and the other party is unable to update the key. Hence, the shared key cannot be synchronized, and then the next round of authentication cannot work successfully. Desynchronization attack is a great threat in IoT, because tags are permanently unable to pass the authentication if tags lose synchronization with the back-end database.

III. OUR CONTRIBUTIONS

Generally, our scheme employs physical unclonable function to generate key k_i to XOR random number, which must store in the card memory [13]. Hence, even if the adversary executes side-channel attack to extract the data in card memory and offline password attack to try all possibilities of password, it is infeasible to guess all possible of the password because which is hidden in multiplying with random number and basic point G. In addition, because of the noise of PUFs, Fuzzy Extractor(FE) is used to enhance the soundness and robust of system. Finally, desynchronization attack can be resisted in our protocol, because updated information is

shared in card and server. The contributions are summarized as follows:

1. Innovatively addressing the smart card loss and desynchronization attack in [13] by introducing noisy PUFs and Fuzzy Extractor in smart card authentication. In this paper, to address the attack pointed by [5] in [13], we proposed to use PUF and FE to generate key to *XOR* random number and hide password in the multiplication with random number and basic point *G*. Hence, adversary cannot guess all possibility of password based on ECDLP assumption and Definition 1.

2. Desynchronization attack can be resisted in our protocol. In the authentication phase, updated information is known by both parties. Server will get the âĂIJsynchronization informationâĂİ in the last authentication phase only card side is verified successfully by server. Hence, our proposed scheme supports offline updating if online synchronization is blocked.

3. The robust of card authentication can be achieved by utilizing robust fuzzy extractor. Our proposed scheme firstly introduces the robust fuzzy extractor in the authentication scheme. When considering the possibility that help data may modified or altered by adversary, robust fuzzy extractor can inform user that the help data is tampered rather that outputting wrong key.

IV. SYSTEM MODEL AND SECURITY MODEL

A. SYSTEM MODEL

This research is focused on the smart card authentication model like [5] and [14] and as shown in FIGURE 1. There are two entities including smart card and server. The first entity is registered with the second via secure channel while authenticate using insecure channel (public channel) which is vulnerable to several attacks like eavesdropping, replay, and desynchronization. The proposed security model consists of five phases i.e. system initialization, registration, authentication, password updating, and card revocation. The initialization and registration phases are performed once in which the security parameters are generated and other necessary computations are performed while in the authentication phase the legitimate user can login the remote server using the already given identity and password. This phase is subject to the provision of valid password and identity.

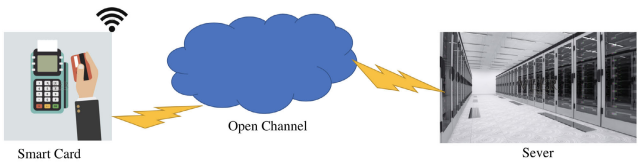


FIGURE 1. System model.

B. SECURITY MODEL

In the conventional smart card remote authentication protocols [37], [38], the security models often defined that the adversary can control the public channel which they can execute the eavesdrop attack, replay attack and desynchronization attack to destroy the authentication between smart card and server. In other words, these assumptions only consider that smart card is always under control by user. However, in the practical threats, there is a great possibility that the user will lose the smart card whatever theft by adversary or lose accidently. Hence, in the recent works [5], [11], [13], the smart card loss attack is taken into consideration. However, it is worth noting that, the adversary cannot extract the stored secret data in smart card even if they can somehow obtain the card in aforesaid assumptions. Hence, in our paper, we assume that a determined adversary can execute up-to-data side channel attack to extract the stored data in the smart card.

Before defining our security model, we firstly propose our assumption:

Assumption 1 (Card Unclonability Assumption): Under this standard assumption, it is impossible for adversary to predict the behavior of the PUF without holding the physical devices. In other word, adversary cannot acquire or guess the correct response in a non-negligible possibility.

Definition 2: For formalizing the card loss attack, we introduce a query-response Game 1 *between challenger C and adversary A to present how our scheme can against card loss attack. The server and the card memory are taken as challenger C, who will give the correct response to adversary queries expected PW and random number N_s. Because N_s is deleted by both card and server, and PW is only known by user. The game steps are as follows:*

1) System initialization phase: The challenger C runs the system initialization algorithm to obtain following parameters including server's private key d_s, public key P_s, temporary ID TID and verifier value P_s. And then challenger C sends public parameters P_s, TID to A.

2) Query phase: The adversary A will query the challenger C as following:

a. Extract query: In this query, it means that the adversary A can get confidential data by side-channel attack, which stored in card memory. Hence, adversary A queries temporary ID, C from challenger and then challenger runs Extract algorithm to generate TID and C and sends them to A.

b. PUF and Fuzzy Extractor query: After receiving the C from challenger, adversary A queries the response, and random number from challenger. Meanwhile, challenger will respond R_R and R_T to adversary.

3) Challenge phase: As to this phase, adversary A pretends the prover to interact with challenger C who becomes verifier. Firstly, adversary A sends the challenge $\{ID, TID_i\}$ to verifier. Next, verifier requests A to send response.

4) Authentication phase: After receiving the challenge from challenger C, adversary A will generate encrypted proof in form of $E_{sk_x^*}(TID_i, K_c, C_{i+1}, R_{i+1})$.

Adversary A succeeds in this game in a non-negligible possibility if $sk_x^* = sk_x$, which can be denoted as $Adv_A^{card-lost} = [sk_x^* = sk_x]$.

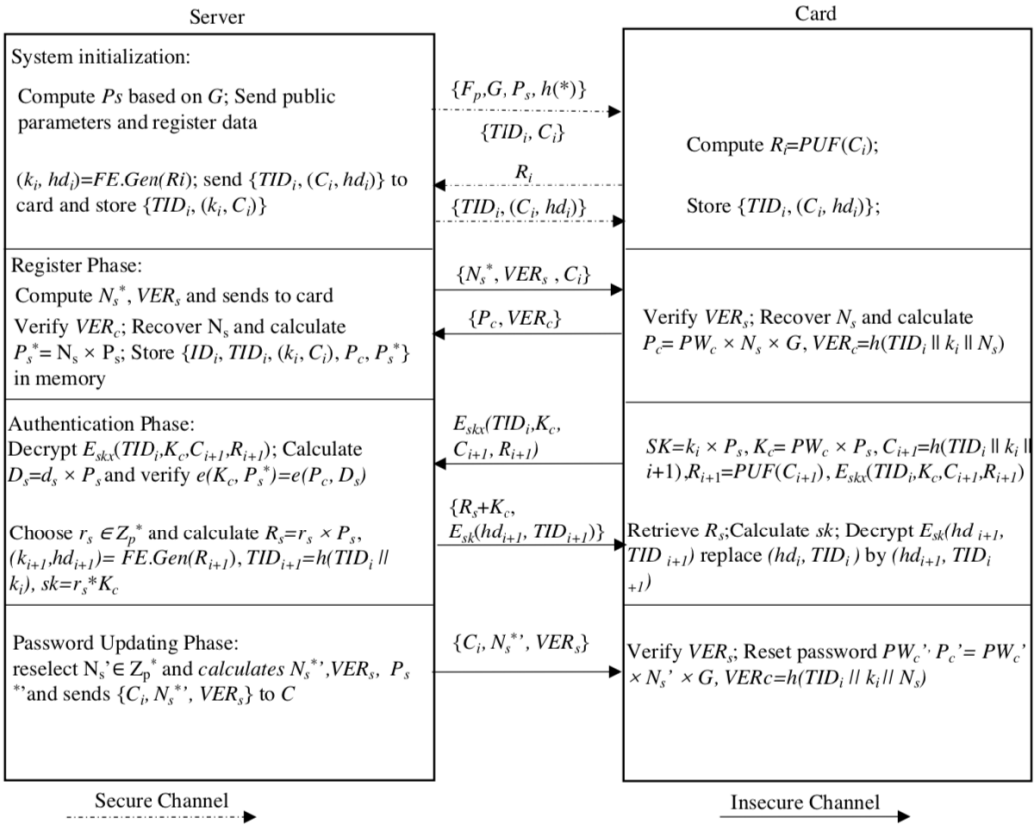


FIGURE 2. Proposed scheme.

In aforementioned games, we simulate that, adversary A executes card loss attack and offline password guessing attack to acquire the correct PW. However, we must admit that the security of our protocol is based on the unclonability and unpredictability of PUF, so that our scheme can resist the card loss attack.

Definition 3: Even if the adversary A has a non-negligible possibility to win the Game 1, our scheme can resist desynchronization attack. Because server also stores a confidential information to reconstruct the updated information.

Definition 4: In this definition, adversary A has ability to enter the Fuzzy Extractor to alter or tamper the help data. However, there exists a robust Fuzzy Extractor [15] outputting invalid if the help data is modified by adversary other than wrong key.

V. PROPOSED SCHEME

In this section, our proposed authentication scheme is explicated in five phases including system initialization, register, authentication, password change and user eviction. Elliptic curve cryptography and physical unclonable function are employed into our scheme. FIGURE 2 presents whole structure of our proposed authentication protocol. The details of proposed scheme is explicated in subsequent sections.

Phase-1: System initialization

In Phase-1, smart card and back-end server are initialized to generator and release system public parameters before they participant in the interactive process, which consists of public parameter generation, smart card initialization and back-end server initialization.

1) System parameter generation: Firstly, server S selects elliptic curve E over a finite group F_p and defines the cyclic subgroup of $E(\mathbb{F}_p)$ which is generated by basic point G with prime order n. Next, sever selects d_s as private key and calculates $P_s = d_s \times G$ as public key. Thereafter, sever chooses an anti-collision hash functions $h(*) : \{0,1\}^* \rightarrow \{0,1\}^K$. Finally, sever releases public parameters $\{p, F_p, G, P_s, h(*)\}$.

2) Smart card initialization: Before handed over to users, smart card SC should be interactive with sever to stored confidential data in memory. First of all, sever will randomly generate unique temporary TID_i and a challenge C_i to smart card. After that, card SC will produce response R_i by using embedded PUF. Note that TID_i will continually update with different authentication. Hereafter, Sever S will compute $\{k_i, hd_i\} = FE.Gen(R_i)$ and transmit $\{TID_i, (C_i, hd_i)\}$ to card SC. Finally, smart card SC will store $\{TID_i, (C_i, hd_i)\}$ and server S will save $\{TID_i, (k_i, C_i)\}$ in database.

Phase-2: Register

Upon receiving register application, user will get the smart card SC and perform as follows:

1) The smart card SC will be activated by entering user identity ID_i and sends ID_i to server S. Next, S saves ID_i as $\{ID_i, TID_i, (k_i, C_i)\}$ and randomly generates number

$N_s \in Z_p^*$. Hereafter, S calculates $N_s^* = N_s \ XOR \ k_i$, $VER_s = h(TID_i||k_i||N_s^*)$ and sends $\{C_i, N_s^*, VER_s\}$ to SC.

2) SC verifies the correctness of the VER_s by using TID_i, k_i in its memory and N_s^* which sent by S. If verifying successfully, SC calculates $R_i' = PUF(C_i)$ which the hamming distance between R_i' and R_i is at most and $FE.REC(R_i', hd_i) = k_i, N_s = N_s^* \ XOR \ k_i$. Finally, SC informs user to set password PW_c, $Pc = PW_c \times N_s \times G$, $VER_c = h(TID_i||k_i||N_s)$ and transmits to server S.

3) Server S firstly verifies the correctness of VER_c by using TID_i, k_i, N_s in memory and calculates verifier value $P_s^* = N_s \times P_s = N_s \times d_s \times G$. If validation passes, Server S will store P_c, P_s^* to database as $\{ID_i, TID_i, (k_i, C_i), P_c, P_s^*\}$. It is noteworthy that both SC and S will delete N_s in memory and SC will store $\{ID_i, TID_i, (C_i, hd_i), P_c\}$ when register successfully.

Phase-3: Authentication

1) When user inserts SC to card reader and inputs ID_i and PW_c^*, S will search the database and send C_i to SC. After receiving C_i, SC retrieves k_i using PUF and Fuzzy Extractor as phase-2. Meanwhile, SC calculates $SK = H(k_i) \times P_s = H(k_i) \times d_s \times G$, $K_c = PW_c^* \times P_s = PW_c^* \times d_s \times G$, $C_{i+1} = h(TID_i||k_i||i+1)$, $R_{i+1} = PUF(C_{i+1})$. Hereafter, SC encrypts $E_{SK_x}(TID_i, K_c, C_{i+1}, R_{i+1})$ by the x coordinate of SK and transmits to S.

2) S decrypts $E_{SK_x}(TID_i, K_c, C_{i+1}, R_{i+1})$ by calculating $SK = H(k_i) \times P_s$ and verifies the correctness of C_{i+1}. Next, S calculates $D_s = d_s \times P_s = d_s \times d_s \times G$. If S verifies successfully, S will check that the equation $e(K_c, P_s^*) = e(P_c, D_s)$ is established. If the equation holds, S considers SC has correct PW_c and grants the access permission.

3) S then chooses random number $r_s \in Z_p^*$, calculates $R_s = r_s \times P_s$, $(k_{i+1}, hd_{i+1}) = FE.Gen(R_{i+1})$, $TID_{i+1} = h(TID_i||k_i)$ and session key $sk = r_s \times K_c$. S transmits $\{R_s + K_c, E_{sk}(hd_{i+1}, TID_{i+1})\}$.

4) SC retrieves $R_s = R_s + K_c - K_c$ and calculates $sk = R_s \times PW_c^*$. Only if $PW_c^* = PW_c$, SC can decrypt $E_{sk}(hd_{i+1}, TID_{i+1})$ and replace (hd_i, TID_i) by (hd_{i+1}, TID_{i+1}) in memory such that $\{ID_i, TID_{i+1}, (C_{i+1}, hd_{i+1}), P_c\}$.

Phase-4: Password Updating

If user wants to change the password, it is necessary to authenticate with server as steps(1)(2) in phase-3. User can send the request of changing password if he acquires the permission to access the server.

1) If server receives the request, S will reselect random number $N_s' \in Z_p^*$. Next, S calculates $Ns'^* = N_s' \ XOR \ k_i$, $VER_s = h(TID_i||k_i||N_s'^*)$, $P_s' = N_s' \times P_s = N_s' \times d_s \times G$ and sends $\{Ci, N_s'^*, VER_s\}$ to SC and saves $P_s'^*$ in memory.

2) SC calculates $R_i' = PUF(C_i)$, $FE.REC(R_i', hd_i) = k_i$, $N_s' = N_s'^* \ XOR \ k_i$ after VER_s is correct. Finally, user resets password PW_c', $Pc' = PW_c' \times N_s' \times G$, $VER_c = h(TID_i||k_i||N_s')$ and transmits to server S.

3) After finishing password updating, the system will update (TID_i, k_i, hd_i, C_i) as above phase-3 steps(3)(4).

TABLE 2. Security comparisons with other different schemes.

	[13]	[16]	[11]	[17]	Ours
Desynchronization attack	×	×	×	✓	✓
Resistance to password disclosure attack	✓	✓	×	×	✓
Dos attack	×	✓	✓	✓	✓
Lost Smart Card Problem	×	×	×	✓	✓
Server Spoofing Attack	✓	✓	✓	×	✓
Impersonation attack	✓	✓	✓	×	✓
Insider privileged attack	×	✓	×	×	✓

e. phase-5: Card Revocation

If user wants to revoke the account, it is important to login the server successfully and send the revocation request just like Phase-3. After server S takes SC as valid user, S will delete $\{ID_i, TID_i, (k_i, C_i), P_c\}$ in the database so that SC cannot login the server by his ID.

VI. SECURITY PROOF

In Section 6.1, through the formal security analysis, our proposed scheme is proofed secure against the aforementioned security model in Section 4. Meanwhile, user anonymity proof and server spoofing attack are presented through informal security proof in Section 6.2. In the following, our proposed scheme is elaborated to withstand above attacks and the security comparison is shown in Table 2.

A. FORMAL SECURITY ANALYSIS

Theorem 1 (The Correctness of Authentication): When smart card and server properly follow our protocol, they can pass the mutual verification between two parties.

Proof:

$$\begin{aligned} e(K_c, P_s^*) &= e(PW_c^* \times d_s \times G, N_s \times d_s \times G) \\ &= e(G, G)^{PW_c^* \times d_s \times N_s \times d_s} \\ e(P_c, D_s) &= e(PW_c \times N_s \times G, d_s \times d_s \times G) \\ &= e(G, G)^{PW_c \times N_s \times d_s \times d_s}. \end{aligned}$$

Before verifying correctness of the equation, only server S has the private key d_s, so if S can decrypt the $E_{SK_x}(TID_i, K_c, C_{i+1}, R_{i+1})$ by $SK = H(k_i) \times P_s$, it proves that SC is a valid card. Hereafter, only PW_c^* equals PW_c, where PW_c^* is the input by user and PW_c is correct password, card can pass the verification. It is worth noting that N_s is no possible revealed by adversary because N_s is deleted after register. □

Theorem 2 (Resistance to Card Loss Attack): Suppose that ECDLP problem is infeasible to resolve in polynomial time and smart card with PUF is unclonable. It is difficult for adversary to execute card loss attack if stored information is revealed by adversary.

Proof: As aforesaid in Section 4, if challenger and adversary can follow steps as Game 1. That is, system initialization phase and query phase are executed by challenger, resulting in user ID_i, temporary ID of card TID_i, a pair of challenge C_i and help data hd_i and card public key P_c are acquired by adversary. This simulates that adversary A

TABLE 3. Functionality comparisons with other different schemes.

	[21]	[22]	[23]	[24]	Ours
No-password Verifier Table	✓	✓	✓	✓	✓
Robustness of Fuzzy Extractor	×	×	×	×	✓
Mutual Authentication	✓	✓	×	×	✓
Anonymity	✓	✓	×	✓	✓
Friendly Password Change	✓	✓	✓	✓	✓
User Revocation	×	×	×	✓	✓

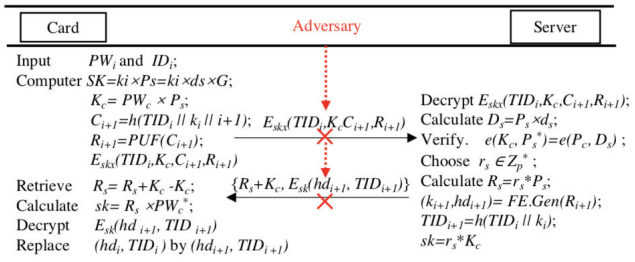


FIGURE 3. Desynchronization attack.

secretly obtains the card from user and extracts stored information $\{ID_i, TID_i, (C_i, hd_i), P_c\}$ using side-channel attack. Hereafter, adversary runs challenge phase to pass the authentication. We assume that adversary can figure out the ECDLP with possibility P. Hence, adversary attempts to plot off-line password guessing attack to guess correct password and guess correct response from PUF between R_R and R_T. Eventually, the possibility of the game is:

$$|Pr[Suc_{card-loss}]| = 1/(2\times 2^k)\times P$$
$$= 1/(2\times 2^k)\times Adv_G^{ECDLP}(TG),$$

where k is the bit length of password and T is the point multiplication in G. While ECDLP is G is computational infeasible, hence p is negligible and $|Pr[Suc_{card-loss}]|$ is also negligible. □

Theorem 3 (Resistance to Desynchronization Attack):For maintaining the anonymity of user, our proposed scheme utilizes the mechanism if dynamic ID to update the pseudo-identity in every new session. Hence, it is essential for both sides to synchronize the pseudo-identity. However, in our proposed scheme, it is impossible for determined adversary to break the synchronization between smart card and server.

Proof: In the authentication phase, the adversary has negligible probability to decrypt $E_{SK_x}(TID_i, K_c, C_{i+1}, R_{i+1})$. Even if we assume adversary A intercepts or block $E_{SK_x}(TID_i, K_c, C_{i+1}, R_{i+1})$ and alters it with random value, it is no way for card to pass the authentication. Moreover, if adversary A blocks $\{R_s + K_c, Esk(hd_{i+1}, TID_{i+1})\}$ and tempers $R_s + K_c$ with wrong value, which will make card cannot decrypt $E_{sk}(hd_{i+1}, TID_{i+1})$. The solution is that card will execute off-line fuzzy extractor generating algorithm to produce help data hd and key k, which will render card synchronization with server. The aforesaid attacks are summarized in FIGURE 3

□

Theorem 4 (Robustness): Assume the help data may be modified by attacker, our proposed scheme is robust for that fuzzy extractor will generate invalid value $\perp$ rather that error valid if hd has been modified. The designation of robust fuzzy extractor is totally refer to [18]–[20], which are proofed to be secure under standard model.

B. INFORMAL SECURITY ANALYSIS

1) Anonymity: In this paper, the true identity of user cannot be traced by adversary over the public channel in the process of mutual authentication. Evidently, for meeting requirements of the anonymity and untraceability, our proposed scheme will login the server in session-variant pseudo-identities ID TID_i. In the process of authentication, SC will send the encrypted block $E_{SK_x}(TID_i, K_c, C_{i+1}, R_{i+1})$ to S, and then if the SC pass the verification, S will updated TID_i by using $TID_{i+1} = h(TID_i||k_i)$. Therefore the ID of SC will change in every round of authentication. Hence, only adversary intrudes into server by side-channel attack, A can destroy the anonymity of user.

2) Resist Replay Attack: The adversary may resend the packet which have been received by host to deceive the system in the process of authentication. However, in our protocol, pseudo-identities ID TID_i, confidential data k_i and help data hd_i will change with the different round of authentication. As said in Phase-3, S computes $(k_{i+1}, hd_{i+1}) = FE.Gen(R_{i+1})$, $TID_{i+1} = h(TID_i||k_i)$ and transmits $\{R_s + K_c, E_{sk}(hd_{i+1}, TID_{i+1})\}$ to SC. Hence, our protocol can successfully resist the replay attack.

3) Server Spoofing Attack: In this attack, adversary A tries to impersonate valid remote server to authentication with A. His intention is informing user to change their password and acquire secret information N_s which will be deleted if server is valid. Upon acquiring the secret information N_s, it is easy for adversary to make smart card useless permanently. However, adversary A is no way to obtain the N_s because the session key SK and sk are only computed by valid server, such that $SK = H(k_i) \times Ps$, $sk = r_s \times K_c$. It is infeasible for adversary to decrypt without session key so that our proposed scheme can withstand server spoofing attack.

VII. PERFORMANCE COMPARISON

In this section, to evaluate the superior functionalities and efficiency property of our proposed scheme, several related schemes are selected to be our comparative objects in terms of no-password verifier table, robustness of fuzzy extractor, mutual authentication, anonymity, friendly password change and user revocation. And then, computation and communication cost are discussed by theoretical analysis and experimental simulation.

A. FUNCTIONALITY COMPARISONS

According to protocol, our scheme can support mutual authentication without maintaining a password table in server. By using different temporary ID in every session, user can maintain anonymity to external user or adversary

TABLE 4. Comparison on computation cost.

	User	Server	Execution time(in milliseconds)
[23]	$t_{hash} + 2t_{exp}$	$7t_{hash} + 6t_{exp}$	$508.6ms$
[26]	$10t_{hash} + t_{pair} + 4t_{exp}$	$5t_{hash} + 3t_{exp} + t_{pair}$	$489.05ms$
[27]	$3t_{sys-e/d} + 12t_{hash} + 3t_{exp}$	$3t_{sys-e/d} + 12t_{hash} + 3t_{exp}$	$885.3ms$
[41]	$4t_{exp} + t_{pair} + 10t_{hash}$	$5t_{sys-e/d} + 2t_{exp}$	$437.8ms$
Ours	$3t_{sys-e/d} + 2t_{exp} + 2t_{hash}t_{FE-gen/rec}$	$t_{sys-e/d} + 2t_{exp} + 2t_{hash}t_{FE-gen/rec} + t_{pair}$	$348.8ms$

TABLE 5. Comparison on communication cost.

	User	Server	Total communication overhead
[23]	$963bits$	$1312bits$	$2275bits$
[26]	$1054bits$	$1184bits$	$2238bits$
[27]	$1240bits$	$1704bits$	$2944bits$
[41]	$864bits$	$768bits$	$1632bits$
Ours	$672bits$	$672bits$	$1344bits$

who can be revoked in our scheme. In addition, password can be changed friendly only if authenticate successfully. Obviously, our proposed scheme can achieve all functionalities compared with other schemes as shown in Table 3, in which $\times$ means corresponding function cannot be satisfied, on the contrary, ✓ means the corresponding function can be satisfied.

B. COMPARISON IN COMPUTATION AND COMMUNICATION

As to computation overhead, we only consider login and authentication phase between server and card. Let t_{hash}, t_{exp}, $t_{sys-e/d}$, $t_{FE-gen/rec}$, t_{pair} denote execution time of anti-collision one-way hash, modular exponential under elliptic curve cryptography, symmetric encryption/decryption using AES, fuzzy extractor generation/reconstruction and bilinear pairing. These cryptographic operations are simulated on Intel Pentium4 with 1,024 MB RAM [25], where t_{hash}=0.0005s, t_{exp}=0.063075s, $t_{sys-e/d}$=0.0087s and t_{pair} $=t_{FE-gen/rec}$=0.02001s. Hence, from Table 4, the total computational time of login and authentication are 348.8ms, where user side is 164.4ms and server side is 184.4ms. It is evident to see that execution time of scheme [41] is the closest to our proposed scheme, which is 437.8ms. And then when it comes to communication cost comparison, we amuse that ID is 32$bits$, the challenge C_i is 32$bits$, response R_s and random k_i are 128$bits$, the size of output hash is 128$bits$ and the block size of symmetric encryption/decryption is 128$bits$. In conclusion, in the phase of login and authentication, user sends $\{ID||E_{sk}(TID_i|K_c||C_{i+1}||R_{i+1})||P_c||Ver_c\}$ to server, which needs $32 + \lceil(32 + 128 + 32 + 128)/128\rceil \times 128 + 128 + 128 = 672bits$. In addition, server replies $C_i||R_s + K_c||E_{sk}(hd_{i+1}||Tid_{i+1})||N_s||Ver_s = 32 + 128 + \lceil(128 + 32)/128\rceil \times 128 + 128 + 128 = 672bits$. The comparison with other related schemes is shown in Table 5, which only contains login and authentication phase. The communication overhead in [26] [23] [27] [41] and our proposed

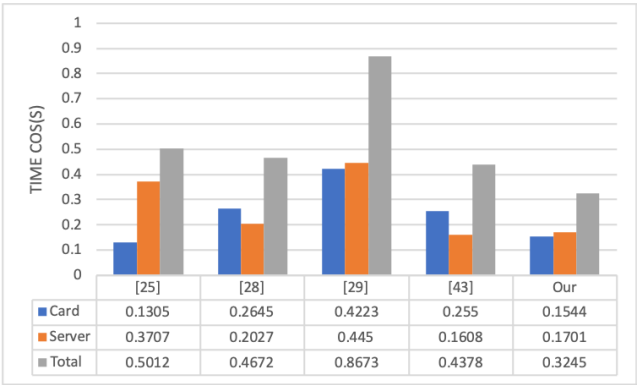


FIGURE 4. Time cost comparison under one smart card.

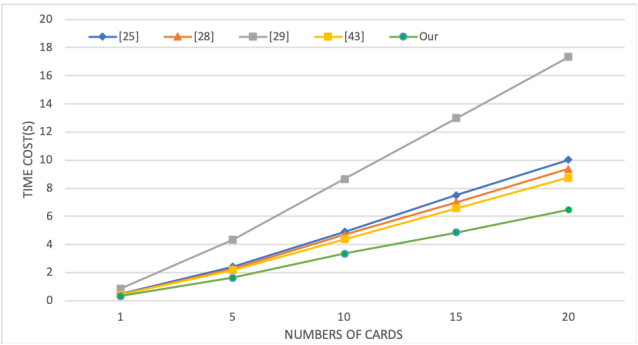


FIGURE 5. Time cost comparison under constant smart cards.

are 2238$bits$, 2275$bits$, 22944$bits$, 1632$bits$ and 1344$bits$, respectively.

Moreover, we simulate the efficient of our protocol in 4, 5 using pairing-based cryptography(PBC), which perform in a desktop with Intel Pentium4 and 1,024 MB RAM. As shown in FIGURE 4, we evaluate our protocol both in smart card side and server side to visual display of experimental result. It is clearly that the total time consumption of authentication is evidently less than all above schemes. Note that the time consumption is little bit higher than [25] on the smart card side, and the time consumption on the server side is also little bit higher than [43]. However, these millisecond advantages are very small that people almost cannot feel the different. While our total time consumption has obvious advantage over 0.1 seconds. Generally speaking, the time consumption increases with the number of smart cards in the FIGURE 5. However, the growth rate of time consumption of our protocol

is significantly less than that of other protocols. Hence, the efficient of our protocol is better than other protocols such as [25], [28], [29], [43] from the experimental results.

VIII. CONCLUSION

In this paper, we propose an anti-desynchronization and robust authentication scheme aiming to resolve the card loss attack and desynchronization attack in Li's paper. The novel scheme incorporated physical unclonable function, which protects the random number stored in card and prevents the off-line password guessing attack under card lose attack. Furthermore, for resisting the desynchronization attack, we innovatively use the off-line updating mechanism to keep the synchronization between two parties of authentication. Moreover, when considering the possibility adversary can change the help data, we introduce the robust fuzzy extractor to prevent to generate wrong key rather than invalid value. In addition, security and functionality comparison are done to show the characteristics of our scheme, which our scheme can satisfy all security requirements in table and functionalities in table. Finally, according to theoretical analysis and experimental results, our scheme can ensure less communication cost and computation cost compare with other password-based schemes, which are 348.8ms and 1344$bits$.

REFERENCES

[1] Y. Wang, R. Chen, C. Liu, B. Wang, and Y. Wang, "Asymmetric subversion attacks on signature and identification schemes," *Pers. Ubiquitous Comput.*, pp. 1–14, Jan. 2019. doi: 10.1007/s00779-018-01193-x.
[2] B. Wang, Y. Wang, and R. Chen, "A practical authentication framework for VANETs," *Secur. Commun. Netw.*, vol. 2019, May 2019, Art. no. 4752612.
[3] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[4] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Comput. Secur.*, vol. 18, no. 8, pp. 727–733, 1999.
[5] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 4, pp. 428–442, Jul./Aug. 2015.
[6] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 57, no. 2, pp. 793–800, Feb. 2010.
[7] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1390–1397, Aug. 2011.
[8] S. Ramesh and V. M. Bhaskaran, "A secured and improved dynamic ID based remote user authentication scheme using smart card and hash function for distributed systems," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 8, p. 305, 2014.
[9] K. R. Rehiman and S. Veni, "A secure authentication infrastructure for IoT enabled smart mobile devices-an initial prototype," *Indian J. Sci. Technol.*, vol. 9, no. 9, pp. 1–6, 2016.
[10] S.-Y. Kang, D.-G. Lee, and I.-Y. Lee, "A study on secure RFID mutual authentication scheme in pervasive computing environment," *Comput. Commun.*, vol. 31, no. 18, pp. 4248–4254, 2008.
[11] S. H. Islam and G. P. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," *Math. Comput. Model.*, vol. 57, nos. 11–12, pp. 2703–2717, 2013.
[12] C.-L. Lin and T. Hwang, "A password authentication scheme with secure password updating," *Comput. Secur.*, vol. 22, no. 1, pp. 68–72, 2003.
[13] C. T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card," *IET Inf. Secur.*, vol. 7, no. 1, pp. 3–10, Mar. 2013.
[14] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1767–1775, Jul. 2014.
[15] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, "Secure remote authentication using biometric data," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2005, pp. 147–163.
[16] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2004–2013, Nov. 2013.
[17] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.
[18] Y. Dodis, J. Katz, L. Reyzin, and A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2006, pp. 232–250.
[19] R. Cramer, Y. Dodis, S. Fehr, and C. Padró, and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2008, pp. 471–488.
[20] B. Kanukurthi and L. Reyzin, "An improved robust fuzzy extractor," in *Proc. Int. Conf. Secur. Cryptogr. Netw.* Berlin, Germany: Springer, 2008, pp. 156–171.
[21] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.
[22] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 1, p. 2946, 2017.
[23] H. Yeh, T. Chen, P. Liu, T. Kim, and H. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, May 2011.
[24] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.
[25] L. Kocarev and S. Lian, *Chaos-based Cryptography: Theory, Algorithms and Applications*. Berlin, Germany: Springer, 2011, p. 354.
[26] X. Li, J. Niu, and K.-K. R. Choo, "A robust authentication protocol with privacy protection for wireless sensor networks," in *Proc. Int. Workshop Radio Freq. Identificat. Secur. Privacy Issues*. Berlin, Germany: Springer, 2016, pp. 30–44.
[27] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multiserver authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.
[28] O. Ruan, Q. Wang, and Z. Wang, "Provably leakage-resilient three-party password-based authenticated key exchange," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 1, pp. 163–173, 2019.
[29] O. Ruan, J. Chen, and M. Zhang, "Provably leakage-resilient password-based authenticated key exchange in the standard model," *IEEE Access*, vol. 5, pp. 26832–26841, 2017.
[30] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Scalable RFID systems: A privacy-preserving protocol with constant-time identification," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 8, pp. 1536–1550, Aug. 2011.
[31] R. Amin and G. Biswas, "A novel user authentication and key agreement protocol for accessing multi-medical server usable in TMIS," *J. Med. Syst.*, vol. 39, no. 3, p. 33, 2015.
[32] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *J. Med. Syst.*, vol. 43, p. 10, Jan. 2019.
[33] E.-J. Yoon and K.-Y. Yoo, "A secure chaotic hash-based biometric remote user authentication scheme using mobile devices," in *Advances in Web and Network Technologies, and Information Management*. Berlin, Germany: Springer, 2007, pp. 612–623.
[34] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov. 2013.

[35] T. Maitra, M. S. Obaidat, S. H. Islam, D. Giri, and R. Amin, "Security analysis and design of an efficient ECC-based two-factor password authentication scheme," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4166–4181, 2016.

[36] M. Deng and W. Zhu, "Desynchronization attacks on RFID security protocols," *TELKOMNIKA Indonesian J. Elect. Eng.*, vol. 11, no. 2, pp. 681–688, 2013.

[37] A. G. Reddy, E.-J. Yoon, A. K. Das, V. Odelu, and K.-Y. Yoo, "Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment," *IEEE Access*, vol. 5, pp. 3622–3639, 2017.

[38] D. Wang and P. Wang, "Offline dictionary attack on password authentication schemes using smart cards," in *Information Security*. Berlin, Germany: Springer, 2015, pp. 221–237.

[39] M. Anoop, "Elliptic curve cryptography," *An Implement. guide*, pp. 51–55, 2007.

[40] D. Hankerson, A. J. Menezes, and S. Vanstone, "Guide to elliptic curve cryptography," *Comput. Rev.*, vol. 46, no. 1, p. 13, 2005.

[41] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," *Future Gener. Comput. Syst.*, vol. 83, pp. 607–618, Jun. 2018.

[42] Q. Yao, J. Ma, R. Li, X. Li, J. Li, and J. Liu, "Energy-aware RFID authentication in Edge computing," *IEEE Access*, vol. 7, pp. 77964–77980, 2019.

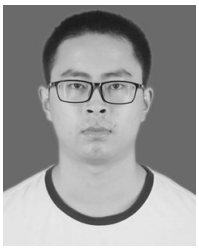
[43] F. Wen, W. Susilo, and G. Yang, "A robust smart card–based anonymous user authentication protocol for wireless communications," *Secur. Commun. Netw.*, vol. 7, no. 6, pp. 987–993, 2014.

[44] X. Wu, J. Qu, and Y. Feng, "Security enhancement on an anonymous authentication scheme for wireless communications using smart cards," *J. Discrete Math. Sci. Cryptogr.*, vol. 21, no. 5, pp. 1139–1155, 2018.

[45] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 629–631, May 2004.

YULING CHEN received the B.S. degree from Taishan University, Tai'an, China, in 2006, and the M.S. degree from Guizhou University, Guiyang, China, in 2009, where she is currently an Associate Professor with the Guizhou Provincial Key Laboratory of Public Big Data. Her recent research interests include cryptography and information safety.

WEI KONG received the B.E. degree from the Nanjing University of Information Science and Technology, Nanjing, China, in 2017, where he is currently pursuing the master's degree. His research interests include computer and network security, privacy-preserving, and cryptography.



XINZHAO JIANG received the B.E. degree from the Binjiang College, Nanjing University of Information Science and Technology, Nanjing, China, in 2017, where he is currently pursuing the M.E. degree. His research interests include security and privacy in cloud as well as attribute-based encryption for cloud storage.