This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3252051

LCDMA: Lightweight Cross-domain Mutual Identity Authentication Scheme for Internet of Things

Bei Gong, Guiping Zheng, Muhammad Waqas, *Senior Member, IEEE,* Shanshan Tu, *Member, IEEE,* and Sheng Chen, *Fellow, IEEE*

Abstract—With the widespread popularity of mobile terminals in the Internet of things (IoT), the demand for cross-domain access of mobile terminals between different regions has also increased significantly. The nature of wireless communication media makes mobile terminals vulnerable to security threats in cross-domain access. Identity authentication is a prerequisite for secure data transmission in cross-domain, and it is also the first step to guarantee the credibility of data sources. Most existing authentication schemes are based on bilinear pairing or public key encryption and decryption with high computation overhead, which are not suitable for the resource-limited mobile IoT terminals. Moreover, these schemes have some security drawbacks and cannot meet the security requirements of cross-domain access. In this paper, we propose a lightweight cross-domain mutual identity authentication (LCDMA) for mobile IoT environment. LCDMA uses symmetric polynomial instead of high-complexity bilinear pairing in the traditional schemes. We theoretically analyze the security performance under the random oracle model. Our results show that LCDMA not only resists common attacks, but also preserves secure traceability while guaranteeing anonymity. Performance evaluation further demonstrates that our scheme has better performance in terms of computation and communication overhead, compared with other existing representative schemes.

Index Terms—Internet of things, cross-domain authentication, mutual identity authentication, key agreement, random oracle model.

1 Introduction

The Internet of things (IoT) consists of wireless interrelated and connected devices that can collect, send, process and store data over the Internet or other communication networks. IoT does not require human-to-human or human-to-computer interaction [1], and it has found wide applications in smart home, intelligent manufacturing, intelligent transportation, smart city, smart medical care, smart ocean, etc. [2]. In the IoT environment, mobile IoT terminals, such as smart wearable devices, cars in the Internet of vehicles, etc., need to access resources in other systems or domains [3], [4]. These mobile IoT terminals, referred to as cross-domain access mobile nodes, collect raw data and communicate with others using wireless communication technologies, such as WiFi, Bluetooth, GPS, etc., to upload raw data, which may contain user's sensitive information, and process data for upper-layer applications or other smart terminals. Since cross-domain access mobile nodes mainly rely on vulnerable public communication media such as radio for data transmission, attackers can launch interception, modification, impersonation and other attacks, resulting in the disclosure of sensitive information. Therefore, it is essential to ensure the legitimacy, anonymity and privacy of cross-domain access mobile nodes.

Mobile IoT has the features of massive heterogeneous devices, complex and variable communication carriers, significant differences in the resource requirements between terminals, and dynamic changes in network topology [5], [6]. In the complex and changeable IoT environment, mutual identity authentication, which ensures that both sender and receiver are legitimate, and key agreement, which ensures that the communication parties are exchanging messages in a pre-negotiated session, are the prerequisite for ensuring the trust of data sources and achieving secure and reliable operation of mobile IoT [7]. Therefore, how to design an identity authentication scheme suitable for cross-domain access is the first crucial step to ensure the security of mobile IoT.

Most existing identity authentication schemes in IoT environment are based the operations such as bilinear pairing, public key encryption and decryption, and symmetric encryption [8], [9], [10], [11], [12], [13], [14]. Although these schemes are flexible, they impose high overhead and require high resources for the running entity. Therefore, they are unsuitable for resource-constrained mobile IoT terminals. By contrast, symmetric polynomial is not only flexible but also has a low computational cost, which is better suited for resource-limited mobile IoT terminals. The emergence of identity authentication schemes based on symmetric polynomial represent a breakthrough in the field of IoT authentication. However, the cross-domain access process of the existing symmetric polynomial-based authentication

- *B. Gong, G. Zheng and S. Tu are with Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China (E-mails: gongbei@bjut.edu.cn, zhenggp@emails.bjut.edu.cn, sstu@bjut.edu.cn).*
- *M. Waqas is with Department of Computer Engineering, Faculty of Information Technology, University of Bahrain, Bahrain, and also with the School of Engineering, Edith Cowan University, WA 6027, Australia (E-mail: engr.waqas2079@gmail.com).*
- *S. Chen is with School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K and Faculty of Information Science and Engineering, Ocean University of China, Qingdao 266100 China (E-mail: sqc@ecs.soton.ac.uk).*

schemes [15], [16], [17], [18] is complicated. The trusted center also cannot provide trusted traceability services to locate illegal acts, and may not be able to eliminating malicious users. In addition, there exist other schemes based on lightweight cryptographic primitives for identity authentication [20], [21], [22], [23], [24]. However, these schemes have some drawbacks, including lack of intra- or cross-domain authentication capability as well as inability to resist replay attacks, insider attacks, and session key leak attacks.

In this paper, we propose a lightweight cross-domain mutual identity authentication scheme based on symmetric polynomial for mobile IoT environment, referred to as LCDMA, to solve the problems of mutual authentication and session key confidentiality for cross-domain access mobile nodes. We theoretically show that LCDMA not only minimizes the computation and communication overhead of the participating entities but also preserves security and traceability while satisfying anonymity. The main contributions of this paper are summarized as follows.

1) By introducing a binary symmetric polynomial as the authentication key, LCDMA utilizes the symmetric polynomial to achieve not only the intra-domain mutual authentication between mobile nodes and local domain servers, but also cross-domain mutual authentication between mobile nodes and other domain servers. Furthermore, it is cable of completing the secure key agreement for the cross-domain access mobile nodes.
2) LCDMA is proven to be secure under the random oracle model (ROM). Specifically, it not only meets the security requirements by resisting various attacks, but also preserves security traceability while guaranteeing anonymity.
3) LCDMA requires only two rounds of interaction during cross-domain authentication. As demonstrated in the performance comparison with the existing state-of-the-art schemes, LCDMA can better utilize the limited resources of mobile nodes and authentication servers and imposes low computation and communication overhead, making it more suitable for mobile IoT environment.

The rest of this paper is organized as follows. Section 2 discusses the existing related research work, and Section 3 introduces the preliminaries used by LCDMA. Section 4 presents the network model applicable to LCDMA and details the proposed LCDMA scheme. A theoretical security proof and analysis of LCDMA is provided in Section 5, while Section 6 evaluates its performance in comparison with other existing schemes. Our work is concluded in Section 7.

2 Related Work

Existing authentication schemes to solve the identity authentication problem in IoT can be divided into two categories: intra-domain and cross-domain identity authentication.

2.1 Intra-domain Identity Authentication

Lin *et al.* [15] proposed a user authentication and key agreement scheme for fog computing environment, which can establish a secure session between different entities, allow users to access other fog servers, and satisfy the perfect forward security and anonymity. Shuai *et al.* [8] provided an anonymous authentication protocol for smart home environment and use ECC for smart home security. Xiang and Zheng [9] proposed a context-aware protocol for device authentication for smart home environment, using hash functions and synchronous encryption for authentication. However, the above schemes have complex calculation process.

The Physical Unclonable Function (PUF) is a hardware-secure technique that exploits inherent device variations to produce a non-clonable unique device response for a given input [19]. Due to the characteristics of PUF that cannot be Cannot be cloned, predicted, simulated or replicated, it can be applied to the identity authentication of IoT terminals with limited resources. Liang *et al.* [20] proposed a bidirectional RFID authentication protocol based on double PUF, which effectively saves the cost of RFID system and avoids storing a large number of excitation response pairs. The protocol uses XOR for processing strings and random fill for encrypting PUF responses. There are many similar protocols [25], [26], [27] that are also based on PUF-designed authentication protocols for IoT. While these protocols are effective against many of the current mainstream attacks and reduce computing and storage overhead, the PUF is weak in stability and aging resistance. For the same challenge information, PUF will output different results under the influence of the environment, which reduces the PUF security. Furthermore, the hardware age and the output of PUF will change as time passes. Unfortunately, such changes will make the legal owner of the PUF unable to pass the verification of the verifier.

In addition, some of the existing schemes have drawbacks in terms of performance. Sharma and Kalra [28] proposed a remote user authentication scheme in the cloud environment, but the scheme fails to realize clock synchronization and time error detection [29].Wang *et al.* [30] analyzed the two-factor authentication schemes of [31], [32] for multi-server environment, and proved that these schemes have some security defects, which would make them invalid in practical applications without further improvement. It can be seen that the aforementioned schemes all have security vulnerabilities. Gope *et al.* [16] proposed an authentication scheme based on symmetric keys. However, Roy and Bhattacharya [21] found various defects in the scheme of [16], including the vulnerabilities to insider attacks, offline password guessing attacks, session key leak, unauthenticated login stage, imperfect forward secrecy and inappropriate mutual authentication as well as having high database maintenance costs and synchronization problem.

2.2 Cross-domain Identity Authentication

Lee *et al.* [22] introduced a new privacy-preserving authentication scheme for mobile networks, and the authors claimed that the scheme can resist various attacks in the cross-domain process of mobile terminals. However, this authentication scheme was found to be not only vulnerable to impersonation attacks, denial of service attacks and replay attacks, but also lacked a native password mechanism to

detect bad passwords [33], [34]. Sarabi *et al.* [23] proposed a lightweight protocol for mutual authentication between nodes and servers in IoT. Divide nodes into three priority groups, and each group node performs static authentication and generates a token at the beginning of the interval. Use this token to perform continuous authentication until the end of the interval. Combine grouped nodes with static and continuous authentication, and implement lightweight authentication between nodes and servers using simple computational operations of hashing and XOR. However, in the authentication process, the number of continuous authentication increases rapidly with the increase of nodes, which makes the calculation and transmission tasks of the server heavier.

Zhou and Yang [10] proposed a provably secure cross-domain authentication scheme for IoT. The mobile nodes and the remote domain authentication server can complete the identity legality verification of the mobile nodes through only one round of interaction. He *et al.* [11] proposed a cross-domain authentication mechanism for mobile medical social networks, which enables two patients registered in different medical centers to achieve mutual authentication and generate session key for future secure communication. Shashidhara *et al.* [12] proposed a lightweight authentication scheme for cross-domain access services in mobile environment, which combats mobile network transmission delay and uses a sequence of events to prevent replay attacks. Although the aforementioned schemes can ensure user anonymity, privacy and security, they use bilinear pairing, public key encryption and decryption, and symmetric encryption, which require a large amount of computation. Kumar and Chouhan [14] proposed an authentication scheme for medical IoT networks that is resistant to impersonation, password guessing, man-in-the-middle and replay attacks. Since these schemes have complicated cross-domain process and impose high computation costs, they are not suitable for the cross-domain authentication mechanism in mobile IoT.

Additionally, Roy and Bhattacharya *et al.* [21] designed a certificateless anonymous two-factor authentication scheme based on ECC. Kang *et al.* [24] proposed a lightweight user authentication scheme, which only uses hash and XOR operations without symmetric or asymmetric key encryption to achieve high computational efficiency. This scheme ensures the privacy, anonymity and even non-traceability of user identity and password. However, the above two schemes assume that the mobile node and the local domain management node are mutually trusted, and therefore they lack intra-domain mutual authentication mechanism.

To sum up, most of the existing authentication schemes cannot be directly applied to cross-domain access in the mobile IoT. First, they have various security vulnerabilities and are vulnerable to attacks. Moreover, the cost of computation and communication is high, and they are not suitable for cross-domain access terminals with limited resources. Therefore, in this work, we propose a secure and efficient cross-domain mutual identity authentication scheme to enhance the security of mobile IoT environment.

3 PRELIMINARIES

In this section, we introduce the cryptography used in LCDMA and the security requirements that a cross-domain access authentication scheme for mobile IoT needs to meet.

3.1 Computational Problems

An elliptic curve over the finite field $F_p = Z_p = \{0, 1, \cdots, p-1\}$ is a collection of points that satisfy a particular equation. The formula for an elliptic curve $E(F_p)$ over F_p can be expressed as $y^2 = \left(x^3 + ax + b\right) \mod p$, where p is a prime greater than 3, $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0$.

Diffie-Hellman problem for elliptic curve calculation (ECCDHP). Let q be a large prime, where $q > 2^\lambda$ and λ is the security parameter, the order of cyclic addition group G on elliptic curve $E(F_p)$ be q, and g be a generator of G. Given $g, ag, bg \in G$, for any unknown $a, b \in Z_q^* = \{1, 2, \cdots, q-1\}$, computing abg is negligible in probabilistic polynomial time [35].

Elliptic curve DLP (ECDLP). Let q be a large prime, where $q > 2^\lambda$ and λ is the security parameter, the order of cyclic addition group G on elliptic curve $E(F_p)$ be q, and g be a generator of G. Given $g, ag \in G$, for any unknown $a \in Z_q^*$, calculating a is negligible in probabilistic polynomial time [36].

3.2 Anti-collision One-way Hash Function

A one-way hash function h represents a deterministic function where the input is a binary string of arbitrary length and the output is an m-bit fixed-length string. Let the advantage of adversary $\mathcal{A}$ in detecting a hash conflict within execution time rt be $Adv_{\mathcal{A}}^h(rt) = \Pr\left[\mathcal{A} \rightarrow_r (x_1, x_2) : x_1 \neq x_2, h(x_1) = h(x_2)\right]$, where $\mathcal{A} \rightarrow_r (x_1, x_2)$ denotes the two strings x_1, x_2 randomly selected by adversary $\mathcal{A}$. If $Adv_{\mathcal{A}}^h(rt)$ is negligible, the one-way hash function h is anti-collision.

3.3 Binary t-degree Symmetric Polynomial

A binary t-degree symmetric polynomial over the finite field F_p is denoted as $F(x, y) = \left(\sum_{m,n=0}^{t} a_{m,n} x^m y^n\right) \mod p$, where the coefficients $a_{m,n}$, $0 \leq m, n \leq t$, are random numbers from the finite field F_p with $a_{m,n} = a_{n,m}$, and $F(x, y)$ is symmetric, namely, for any $x, y \in F_p$, $F(x, y) = F(y, x)$.

The security of binary t-degree symmetric polynomial is based on the property that $t + 1$ values are required to reconstruct a t-degree polynomial. We utilize binary t-degree symmetric polynomial to generate authentication keys for mobile IoT devices.

3.4 Security Goals

In the process of cross-domain authentication and key agreement for mobile IoT, it is not only necessary to verify the identity information of entities, but also to protect the privacy of the entities during the authentication process. Therefore, the design of a mobile IoT cross-domain authentication scheme should satisfy the following security goals [37], [38]:

1) Mutual identity authentication. A mobile node must complete mutual identity authentication between itself and

the local authentication server to ensure that it is a legitimate node in the local domain. Furthermore, when the mobile node reaches the remote domain, it needs to complete the mutual identity authentication between itself and the remote domain authentication server to ensure that it is legitimate in the remote domain before it can access resources.

2) Session key agreement. In order to protect the confidentiality and security of the interactive data during cross-domain access, the interacting entities need to agreement the session key in advance to ensure that the communication parties are in a secure communication session.

3) Anonymity. In the authentication process, it is necessary to protect the identity information of cross-domain visitors from being leaked. Therefore, it is required to ensure the identity anonymity of cross-domain visitors when designing the authentication scheme. This means that even if an attacker intercepts the packets during message transmission, the real identity of cross-domain visitor cannot be obtained, or even if an attacker knows the pseudonym of the cross-domain visitor, it cannot use other information, such as connected devices, use time, active area, etc., to obtain the real identity.

4) Forward/backward security. To protect the confidentiality of the messages transmitted during the interaction, the scheme must be designed to guarantee the forward/backward security so that an attacker cannot guess the previous/future session key even if it obtains the current session key.

5) Anti-man-in-the-middle attack. The identity authentication scheme should be designed to resist attacks that impersonate legitimate entities and deceive other participating entities.

6) Anti-replay attack. The authentication scheme for mobile IoT should be designed to enable the participating entities to identify whether the packet to be received is a duplicate packet that has already been received.

TABLE 1
Symbols Used in LCDMA

Symbol	Description
$IoT\text{-}TC$	IoT trust center
$DA\text{-}Server_i$	Domain authentication server for $Domain_i$
$CDA\text{-}MNode$	Movable node for cross-domain access
PID_{DAS_i}	Pseudo-identity of $DA\text{-}Server_i$
PID_{MN}	Pseudo-identity of $CDA\text{-}MNode$
λ	Security parameter
p, q	Big primes
F_p	Finite field
$E(F_p)$	Elliptic curve over finite field F_p, expressed as $y^2 = (x^3 + ax + b) \mod p$
G	Cyclic additive group on $E(F_p)$ of order q
g	A generator of G
sk	Private key of $IoT\text{-}TC$
pk	Public key of $IoT\text{-}TC$, $pk = sk \cdot g$
sk_{DAS_i}	Private key of $DA\text{-}Server_i$
pk_{DAS_i}	Public key of $DA\text{-}Server_i$
sk_{MN}	Private key of $CDA\text{-}MNode$
pk_{MN}	Public key of $CDA\text{-}MNode$
$SEnc()$	Symmetric encryption algorithm
$F(x, y)$	Binary t-degree symmetric polynomial
$h_i(\cdot)$	Collision-resistant one-way hash function
$\oplus$	XOR operation in bit operation

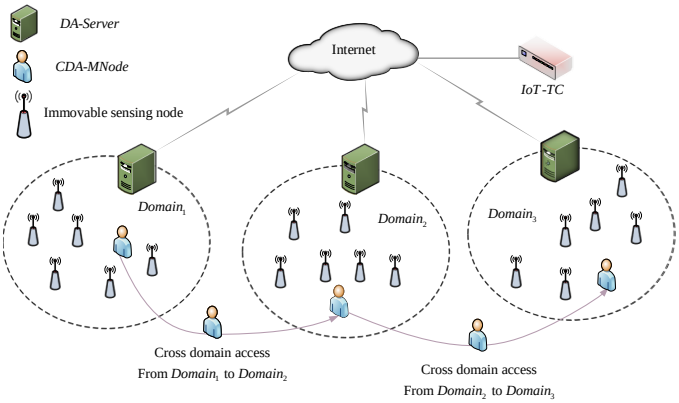

Fig. 1. Cross-domain access network model for mobile nodes for mobile IoT

4 Proposed Lightweight Cross-domain Mutual Identity Authentication Scheme for Mobile IoT

In this section, we first discuss the network model for the LCDMA and then give the architecture of LCDMA, followed by the detailed description of the LCDMA scheme. The symbols used in our LCDMA scheme are listed in Table 1.

4.1 Network Model

Our cross-domain identity authentication system for mobile IoT is illustrated in Fig. 1, which mainly contains three types of entities: IoT trust center ($IoT\text{-}TC$), domain authentication server ($DA\text{-}Server$), and movable node for cross-domain access ($CDA\text{-}MNode$). The features and functions of these three types of entities are summarized below.

4.1.1 $CDA\text{-}MNode$

The difference between these nodes and common sensing nodes in sensing network is that they have mobility. Because such nodes generally need to run on entities with mobile characteristics (e.g. smart phones, cars, drones), they are integrated with mobile entities and collectively referred to as $CDA\text{-}MNode$ in this paper. $CDA\text{-}MNode$ requires data exchange in different domains to provide services for its upper-layer applications. In the initialization phase of the cross-domain authentication system, $CDA\text{-}MNode$ will be assigned to the corresponding domain $Domain_i$ and managed by $DA\text{-}Server_i$.

4.1.2 $DA\text{-}Server$

It is a semi-trusted participant in the cross-domain access system for mobile IoT and has a stronger computation and storage capacity than common sensing nodes. $DA\text{-}Server$ is responsible for verifying the cross-domain access registration information of mobile nodes in the local domain and generating cross-domain authentication packets for legitimate requests. It is also responsible for the authentication of cross-domain mobile nodes in foreign domains and generating session keys for legitimate cross-domain mobile nodes. There are multiple $DA\text{-}Server_i$ distributed in different domains in the cross-domain access authentication system for mobile IoT.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3252051

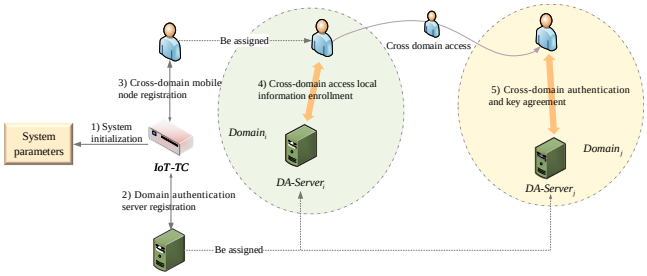

Fig. 2. Framework of LCDMA

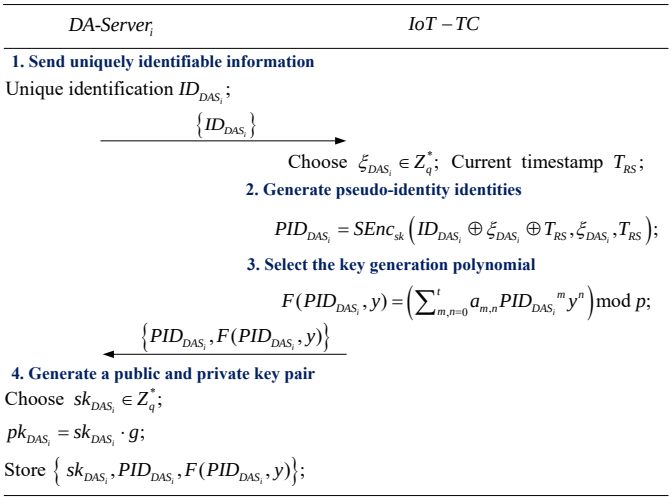

Fig. 3. Flowchart of domain authentication server registration phase

4.1.3 IoT-TC

It represents a trusted third party responsible for the system parameter generation and registration of other entities (mobile devices and domain authentication servers) in the cross-domain access authentication system. IoT-TC is trusted, and its private/secret key is not compromised. When events need to be traced to obtain the true identity of an entity, IoT-TC can use its secret key to perform the tracing. In Fig. 1, CDA-$MNode$ cross-domain accesses from $Domain_1$ to $Domain_2$, and then cross-domain accesses from $Domain_2$ to $Domain_3$. Our scheme mainly addresses the identity authentication issues involved in such a cross-domain access process. During the system registration phase, CDA-$MNode$ is assigned to the corresponding $Domain_i$, and DA-$Server_i$ will manage it locally.

4.2 Framework of LCDMA

Fig. 2 depicts the framework of LCDMA, which consists of five parts: 1) system initialization, 2) domain authentication server registration, 3) cross-domain mobile node registration, 4) cross-domain access local information enrollment, and 5) cross-domain authentication and key agreement.

In the preparatory stage of cross-domain access, IoT-TC initializes the system and generates the system parameters for the system. When some entities, such as mobile nodes and domain authentication servers, participate in the system, they first need to be registered. After the registration, IoT-TC will assign them to the corresponding domain.

In the process of cross-domain access authentication for IoT, mobile nodes need to enroll the cross-domain access information with the local authentication server to complete the intra-domain mutual identity authentication. Only the nodes that are successfully enrolled can enter the remote domain. The remote domain authentication server implements cross-domain identity authentication and key agreement for IoT.

4.3 Lightweight Cross-domain Mutual Identity Authentication

We now detail the proposed LCDMA scheme for IoT. Specifically, we describe the detailed procedures for the five parts of the LCDMA framework depicted in Fig. 2, to complete the cross-domain access identity authentication of mobile nodes in IoT environment.

4.3.1 Initialization

Initialization is mainly accomplished by IoT-TC to generate the system parameters for the IoT authentication system. Specifically, IoT-TC selects the security parameter λ as input and generates the system parameters through the following operations.

1) IoT-TC selects a cyclic additive group G of order q, where $q > 2^\lambda$ is a large prime, on an elliptic curve $E(F_p)$, and a generator g of G.

2) IoT-TC selects a random number $sk \in Z_q^*$ as the private key and keeps it secret.

3) IoT-TC selects anti-collision one-way hash functions h_i, $1 \le i \le 7$, where $h_1 : \{0,1\}^* \times \{0,1\}^* \to Z_q^*$, $h_2 : \{0,1\}^* \times G \times G \to Z_q^*$, $h_3 : \{0,1\}^* \to Z_q^*$, $h_4 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G \to Z_q^*$, $h_5 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G \times G \to Z_q^*$, $h_6 : \{0,1\}^* \times G \to Z_q^*$, and $h_7 : \{0,1\}^* \times G \times G \times G \to Z_q^*$.

4) IoT-TC randomly selects a binary t-order symmetric polynomial $F(x,y) = \left(\sum_{m,n=0}^{t} a_{m,n} x^m y^n\right) \bmod p$ over the finite field F_p.

5) IoT-TC selects symmetric encryption algorithm $SEnc()$.

6) IoT-TC publishes system parameters $param = \{p, q, g, G, h_i\}$, but keeps sk and $F(x,y)$ secret.

4.3.2 Domain Authentication Server Registration

The domain authentication server in IoT environment is not immutable. When DA-$Server_i$ joins the authentication system, it needs to register with IoT-TC. As shown in Fig. 3, DA-$Server_i$ and IoT-TC perform the following process to complete the domain authentication server registration.

1) DA-$Server_i$ sends its unique identity ID_{DAS_i} to IoT-TC through a secure channel.

2) IoT-TC selects a random number $\xi_{DAS_i} \in Z_q^*$, and calculates the pseudo-identity $PID_{DAS_i} = SEnc_{sk}(ID_{DAS_i} \oplus \xi_{DAS_i} \oplus T_{RS}, \xi_{DAS_i}, T_{RS})$ corresponding to ID_{DAS_i}, where T_{RS} is the registration timestamp of DA-$Server_i$.

3) Based on the pseudo-identity PID_{DAS_i} of DA-$Server_i$, IoT-TC calculates the unique binary symmetric polynomial of DA-$Server_i$ according to $F(PID_{DAS_i}, y) = \left(\sum_{m,n=0}^{t} a_{m,n} PID_{DAS_i}^m y^n\right) \bmod p$.

4) IoT-TC sends $\{PID_{DAS_i}, F(PID_{DAS_i}, y)\}$ to DA-$Server_i$ through a secure channel.

5) DA-$Server_i$ selects a random number $sk_{DAS_i} \in Z_q^*$ as its private key, calculates and publishes the public key $pk_{DAS_i} = sk_{DAS_i} \cdot g$.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3252051

4.3.3 Mobile Node Cross-domain Access Registration

The cross-domain access mobile node $CDA\text{-}MNode$ in IoT environment first requires the identity registration with $IoT\text{-}TC$, and $IoT\text{-}TC$ assigns an initial domain and generates intra-domain authentication information for $CDA\text{-}MNode$. As shown in Fig. 4, $CDA\text{-}MNode$ and $IoT\text{-}TC$ perform the following procedures to complete the cross-domain access registration of mobile node.

1) $CDA\text{-}MNode$ sends its unique identity ID_{MN} and password PW to $IoT\text{-}TC$ through the secure channel.

2) $IoT\text{-}TC$ selects a random number $\xi_{MN} \in Z_q^*$, calculates the pseudo-identity $PID_{MN} = SEnc_{sk}(ID_{MN} \oplus PW \oplus \xi_{MN} \oplus T_{RMN}, \xi_{MN}, T_{RMN})$ corresponding to $CDA\text{-}MNode$, where T_{RMN} is the current timestamp, and then stores the identity ID_{MN}, password PW, and the current password setting timestamp T_{RMN} of $CDA\text{-}MNode$. When the user changes password of $CDA\text{-}MNode$, the pseudo-identity corresponding to $CDA\text{-}MNode$ will also be updated.

3) $IoT\text{-}TC$ assigns $CDA\text{-}MNode$ to $Domain_i$. The corresponding domain authentication server to this domain is $DA\text{-}Server_i$ and the pseudo identity is PID_{DAS_i}. The pseudo identity PID_{MN} and password PW of $CDA\text{-}MNode$ are stored in $DA\text{-}Server_i$, to be used for preliminary authentication of $CDA\text{-}MNode$.

4) Based on the pseudo-identity PID_{MN} of $CDA\text{-}MNode$ and the pseudo-identity PID_{DAS_i} of $DA\text{-}Server_i$, $IoT\text{-}TC$ calculates the authentication key $AK_{MN\text{-}i} = F(PID_{DAS_i}, PID_{MN})$ between $CDA\text{-}MNode$ and $DA\text{-}Server_i$.

5) $IoT\text{-}TC$ sends $\{PID_{MN}, PID_{DAS_i}, AK_{MN\text{-}i}\}$ to $CDA\text{-}MNode$ through the secure channel.

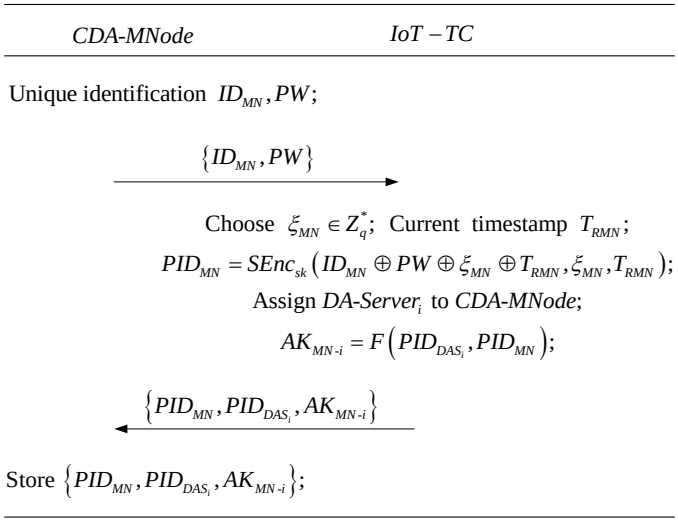

Fig. 4. Flowchart of mobile node cross-domain access registration stage

4.3.4 Cross-domain Access Local Information Enrollment

Before $CDA\text{-}MNode$ can make cross-domain access, the identity authentication for IoT terminals needs to be completed with the local domain $Domain_i$. The process of mutual authentication and the cross-domain access to local information registration is illustrated in Fig. 5. $CDA\text{-}MNode$ inputs its pseudo-identity PID_{MN} and its password PW, and the local domain server $DA\text{-}Server_i$ compares the data in the database for the preliminary identity determination. If the determination fails, the verification is terminated. Otherwise, $CDA\text{-}MNode$ and $DA\text{-}Server_i$ perform the following operations to enable $CDA\text{-}MNode$ obtaining the cross-domain authentication information generated by the local domain server.

1) $CDA\text{-}MNode$ selects random numbers $r_{MN}, r_a \in Z_q^*$, and records the current timestamp T_1. It then calculates $PK_{DAS_i}^* = pk_{DAS_i} \cdot r_{MN}$, $PK_{DAS_i}^{**} = PK_{DAS_i}^* \oplus h_1(AK_{MN\text{-}i}, T_1)$, $R_{MN} = r_{MN} \cdot g$, $R_a = r_a \cdot g$, $H_1 = h_2(R_{MN}, R_a, T_1)$, and sends the message $\{PID_{MN}, PID_{DAS_j}, H_1, PK_{DAS_i}^{**}, R_a, T_1\}$ to $DA\text{-}Server_i$ through the public channel.

2) After receiving the message $\{PID_{MN}, PID_{DAS_j}, H_1, PK_{DAS_i}^{**}, R_a, T_1\}$, $DA\text{-}Server_i$ verifies the freshness of the timestamp T_1 by judging whether $|T_1 - T_1'| \le \Delta T$ is true, where T_1' is the timestamp of receiving the message, and then calculates $AK_{i\text{-}MN} = F(PID_{DAS_i}, PID_{MN})$, $PK_{DAS_i}^{*\prime} = PK_{DAS_i}^{**} \oplus h_1(AK_{i\text{-}MN}, T_1)$, $R_{MN}' = PK_{DAS_i}^{*\prime} \cdot sk_{DAS_i}^{-1}$, $H_1' = h_2(R_{MN}', R_a, T_1)$. If $H_1' == H_1$ holds, the one-way authentication of $DA\text{-}Server_i$ to $CDA\text{-}MNode$ is passed.

3) After the one-way authentication is passed, $DA\text{-}Server_i$ generates the authentication information and sends it to $CDA\text{-}MNode$. Specifically, $DA\text{-}Server_i$ selects random numbers $r_b, r_x \in Z_q^*$, sets T_2 as the current timestamp, and calculates $AK_{i\text{-}j} = F(PID_{DAS_i}, PID_{DAS_j})$, $R_x = r_x \cdot g$, $PK_{DAS_j}^* = pk_{DAS_j} \cdot r_x$, $PK_{DAS_j}^{**} = PK_{DAS_j}^* \oplus h_3(AK_{i\text{-}j})$, $M_0 = h_4(PID_{DAS_i}, PID_{MN}, AK_{i\text{-}j}, R_x)$ (M_0 is mainly for $DA\text{-}Server_j$ to verify that $CDA\text{-}MNode$ is a legitimate node in $Domain_i$), $R_b = r_b \cdot g$, $R_c = R_a \cdot r_b$, $R_b^* = R_b \oplus h_1(AK_{i\text{-}MN}, T_2)$, $H_2 = h_4(AK_{i\text{-}MN}, R_c, T_2, M_0)$. Then $DA\text{-}Server_i$ sends $\{H_2, R_b^*, T_2, M_0, PK_{DAS_j}^{**}\}$ to $CDA\text{-}MNode$ through the public channel.

4) After $CDA\text{-}MNode$ receives the message $\{H_2, R_b^*, T_2, M_0, PK_{DAS_j}^{**}\}$, the freshness of the timestamp T_2 is verified by judging whether $|T_2 - T_2'| \le \Delta T$ is true, where T_2' is the timestamp when the message was received. Then $CDA\text{-}MNode$ calculates $R_b' = R_b^* \oplus h_1(AK_{MN\text{-}i}, T_2)$, $R_c' = R_b' \cdot r_a$, $H_2' = h_4(AK_{MN\text{-}i}, R_c', T_2, M_0)$, and determines whether $H_2 == H_2'$ is true. If it holds, the mutual identity authentication for IoT environment between $CDA\text{-}MNode$ and $DA\text{-}Server_i$ is passed and the packet is correct, and cross-domain access authentication can be performed.

4.3.5 Cross-domain Authentication and Key Agreement

$CDA\text{-}MNode$ can enter $Domain_j$ for cross-domain access authentication after completing the cross-domain access local information enrollment in IoT. As illustrated in Fig. 6, $CDA\text{-}MNode$ cooperates with the domain authentication server $DA\text{-}Server_j$ in $Domain_j$ to complete the following steps to realize cross-domain mutual authentication for IoT environment.

1) $CDA\text{-}MNode$ randomly selects $r_u \in Z_q^*$, records the current timestamp T_3, calculates $R_u = r_u \cdot g$, $PK_u = pk_{DAS_j} \cdot r_u$, $M_1 = h_5(PID_{MN}, PID_{DAS_i}, R_u, M_0, PK_{DAS_j}^{**}, T_3)$, and then sends $\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK_{DAS_j}^{**}, T_3\}$ to $DA\text{-}Server_j$ through the public channel.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3252051

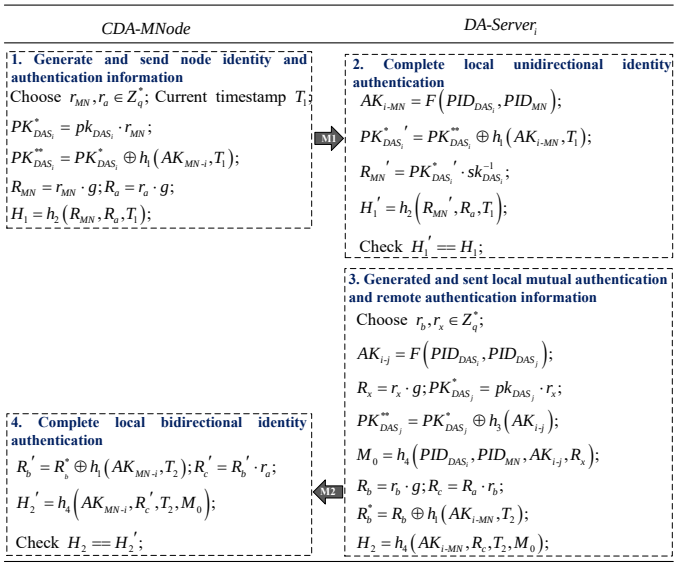

Fig. 5. Flowchart of local information registration phase for cross-domain access

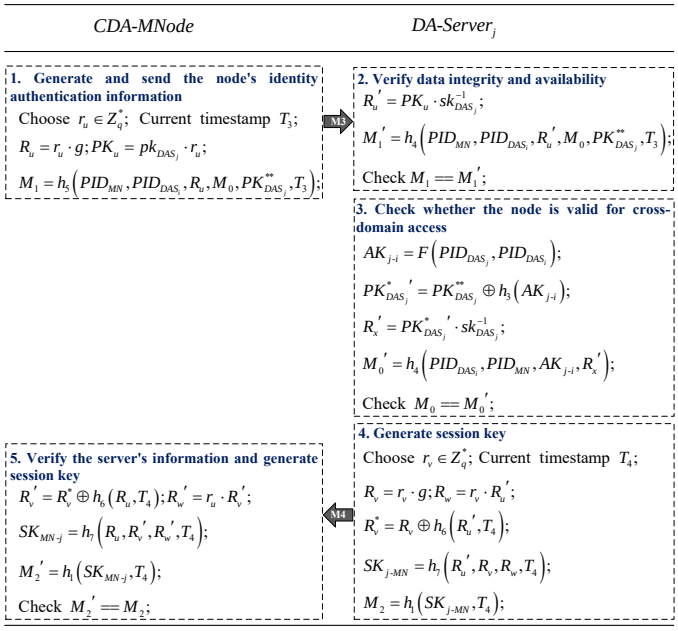

Fig. 6. Flowchart of cross-domain authentication and key agreement phase

2) After $DA\text{-}Server_j$ receives the message $\left\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK_{DAS_j}^{**}, T_3\right\}$, first it verifies the freshness of the timestamp T_3 by checking if $|T_3 - T_3'| \leq \Delta T$ holds, where T_3' is the timestamp of receiving the message. Then it calculates $R_u' = PK_u \cdot sk_{DAS_j}^{-1}$, $M_1' = h_5\left(PID_{MN}, PID_{DAS_i}, R_u', M_0, PK_{DAS_j}^{**}, T_3\right)$, and verifies whether $M_1 == M_1'$ is established. If this is established, it is considered that the message $\left\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK_{DAS_j}^{**}, T_3\right\}$ has not been tampered in the process of public channel transmission.

3) Next, $DA\text{-}Server_j$ calculates $AK_{j\text{-}i} = F\left(PID_{DAS_j}, PID_{DAS_i}\right)$, $PK_{DAS_j}^{*\prime} = PK_{DAS_j}^{**} \oplus h_3\left(AK_{j\text{-}i}\right)$, $R_x' = PK_{DAS_j}^{*\prime} \cdot sk_{DAS_j}^{-1}$, $M_0' = h_4\left(PID_{DAS_i}, PID_{MN}, AK_{j\text{-}i}, R_x'\right)$, and verifies whether $M_0 == M_0'$ is true. If so, $DA\text{-}Server_j$ considers $CDA\text{-}MNode$ as a legitimate registered node on its home domain authentication server $DA\text{-}Server_i$. That is, $DA\text{-}Server_j$ has completed the identity validity verification of $CDA\text{-}MNode$.

4) After the authentication of $CDA\text{-}MNode$ is passed, $DA\text{-}Server_j$ generates a session key $SK_{j\text{-}MN}$ for $CDA\text{-}MNode$. Specifically, $DA\text{-}Server_j$ randomly selects a number $r_v \in Z_q^*$, sets T_4 as the current timestamp, calculates $R_v = r_v \cdot g$, $R_w = r_v \cdot R_u'$, $R_v^* = R_v \oplus h_6\left(R_u', T_4\right)$, $SK_{j\text{-}MN} = h_7\left(R_u', R_v, R_w, T_4\right)$, $M_2 = h_1\left(SK_{j\text{-}MN}, T_4\right)$, and sends $\{M_2, R_v^*, T_4\}$ to $CDA\text{-}MNode$ through the public channel.

5) After receiving the message $\{M_2, R_v^*, T_4\}$, $CDA\text{-}MNode$ first verifies the freshness of timestamp T_4 by checking if $|T_4 - T_4'| \leq \Delta T$ is true, where T_4' is the timestamp when the message was received. It then calculates $R_v' = R_v^* \oplus h_6\left(R_u, T_4\right)$, $R_w' = r_u \cdot R_v'$, $SK_{MN\text{-}j} = h_7\left(R_u, R_v', R_w', T_4\right)$, $M_2' = h_1\left(SK_{MN\text{-}j}, T_4\right)$, and verifies whether $M_2' == M_2$ is holds. If so, the cross-domain mutual identity authentication and key agreement between $CDA\text{-}MNode$ and $DA\text{-}Server_j$ is completed, and the session key between $CDA\text{-}MNode$ and $DA\text{-}Server_j$ is $SK_{MN\text{-}j}$.

5 Security Proof and Analysis

In this section, the security threats faced by the authentication scheme are introduced, and the security proof and analysis of the proposed LCDMA scheme are performed.

5.1 Threat Model

To verify the security of LCDMA, we adopt a threat model based on the widely used DY adversarial model [39], CK adversarial model [40] and eCK adversarial model [41]. The communication network has the following properties.

1) If two entities communicate over a common channel, neither of the communicating entities can be trusted.
2) $IoT\text{-}TC$ is trusted, and its private/secret key will not be compromised.

Let $\mathcal{A}$ be an adversary against LCDMA running in polynomial time rt in ROM. Adversary $\mathcal{A}$ has the following capabilities.

1) Adversary $\mathcal{A}$ can control the public channel, that is, it can read, change, discard or forge messages transmitted over the public channel.
2) Adversary $\mathcal{A}$ can obtain secret information stored in smart device through power analysis attack [42]. The obtained data can be used for some unauthorized tasks, such as session key calculation, smart device impersonation attack, replay attack, privileged insider attack, and man-in-the-middle attack.
3) Adversary $\mathcal{A}$ has excellent analytical and guessing abilities.

Assume that all the entities, including adversary $\mathcal{A}$, can access the anti-collision one-way hash function $h(\cdot)$. We

define a random oracle query, called $H\vartheta$. In this query, adversary $\mathcal{A}$ sends a message m, and challenger $\mathcal{C}$ returns a random value r to $\mathcal{A}$ and records the entry (m, r) into the list.

5.2 AKA Security

We demonstrate the session key security of our proposed LCDMA during node registration, cross-domain access local authentication, and cross-domain authentication and key agreement (AKA) phases.

Theorem 1. In ROM, LCDMA faces adversary $\mathcal{A}$ with AKA security, that is, any polynomial adversary $\mathcal{A}$ cannot break LCDMA with a non-negligible advantage $Adv_{\mathcal{A}}^{LCDMA}(rt)$.

Proof 1. The advantage of adversary $\mathcal{A}$ breaking the session key security in LCDMA can be estimated as:

$$Adv_{\mathcal{A}}^{LCDMA}(rt) \leq \frac{q_{hash}^2 + \left(q_{exe} + q_{send}\right)^2}{2\left|Hash\right|} + 2Adv_{\mathcal{A}}^{ECCDHP}(rt) + 2\varepsilon, \quad (1)$$

where q_{exe}, q_{send} and q_{hash} are the numbers of *Execute* queries, *Send* queries and $H\vartheta$ queries, respectively, $|Hash|$ denotes the range space of $h(\cdot)$, $Adv_{\mathcal{A}}^{ECCDHP}(rt)$ is the advantage of adversary $\mathcal{A}$ breaking ECCDHP in polynomial time rt, and ε is a negligible minimum.

To prove (1), we define four games, denoted as $Game_r$, $r = 0, 1, 2, 3$, and execute them in sequence. The advantage of adversary $\mathcal{A}$ winning $Game_r$ is $Adv_{\mathcal{A}}^{Game_r} = \Pr\left[Succ_r\right]$, where $Succ_r$ represents the event that adversary $\mathcal{A}$ can guess bit c in $Game_r$. The details of each $Game_r$ are as follows.

$Game_0$. The game represents an initial attack on LCDMA in ROM. In this game, adversary $\mathcal{A}$ executes *Test* query, and when $c = 1$, adversary $\mathcal{A}$ can obtain the session key SK. Hence, the semantic security of the session key is defined as:

$$Adv_{\mathcal{A}}^{LCDMA}(rt) = \left|2Adv_{\mathcal{A}}^{Game_0} - 1\right|. \quad (2)$$

$Game_1$. This game simulates eavesdropping attack of adversary $\mathcal{A}$ through *Execute* query. Adversary $\mathcal{A}$ executes *Test* query, which determines whether the output of *Test* is the real session key SK between $CDA\text{-}MNode$ and $DA\text{-}Server_j$ or a random number. In LCDMA, the session key SK is calculated by $CDA\text{-}MNode$ and $DA\text{-}Server_j$ as $SK_{j\text{-}MN} = h_7(R'_u, R_v, R_w, T_4) = SK_{MN\text{-}j}$, where $R'_u = PK_u \cdot sk_{DAS_j}^{-1}$, $R_v = r_v \cdot g$, and $R_w = r_v \cdot R'_u$. Suppose that adversary $\mathcal{A}$ can intercept all the messages $\left\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK_{DAS_j}^{**}, T_3\right\}$ and $\{M_2, R_v^*, T_4\}$ transmitted by $CDA\text{-}MNode$ and $DA\text{-}Server_j$ over the common channel. But relying on these messages, it cannot derive the key secret values sk_{DAS_j}, r_v, r_u in the session key SK. Therefore, the probability of $\mathcal{A}$ winning by eavesdropping attack in $Game_1$ will not increase. That is, adversary $\mathcal{A}$ has the same probability of winning $Game_0$ and $Game_1$, and hence

$$Adv_{\mathcal{A}}^{Game_1} = Adv_{\mathcal{A}}^{Game_0}. \quad (3)$$

$Game_2$. In this game, adversary $\mathcal{A}$ can perform *Send* query and $H\vartheta$ query. The game simulates an active attack in which adversary $\mathcal{A}$ tries to trick the participant into accepting its fabricated information. After intercepting $\left\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK_{DAS_j}^{**}, T_3\right\}$ and $\{M_2, R_v^*, T_4\}$, adversary $\mathcal{A}$ attempts to modify either of them, forging a legitimate message to pass the verification. But in order for the forged message to be authenticated by the participant, adversary $\mathcal{A}$ must know the authentication key $AK_{i\text{-}MN}$ or $AK_{MN\text{-}i}$ protected by the anti-collision one-way hash function between $CDA\text{-}MNode$ and $DA\text{-}Server_j$. Assume that adversary $\mathcal{A}$ has obtained the timestamp in the message through *Execute* query and embedded it in the forged message package. Then, adversary $\mathcal{A}$ repeats $H\vartheta$ query to find the conflict. Since each message is associated with the participant's identity and timestamp, etc., according to the birthday paradox [43], we have:

$$\left|Adv_{\mathcal{A}}^{Game_2} - Adv_{\mathcal{A}}^{Game_1}\right| \leq \frac{q_{hash}^2 + \left(q_{exe} + q_{send}\right)^2}{2\left|Hash\right|}. \quad (4)$$

$Game_3$. In this game, adversary $\mathcal{A}$ tries to calculate the session key SK between $CDA\text{-}MNode$ and $DA\text{-}Server_j$ based on $\left\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK_{DAS_j}^{**}, T_3\right\}$ and $\{M_2, R_v^*, T_4\}$ intercepted in the common channel. In order to calculate $SK_{j\text{-}MN} = h_7(R'_u, R_v, R_w, T_4)$, adversary $\mathcal{A}$ needs to calculate $R_w = r_u r_v g$ through $R_u = r_u \cdot g$ and $R_v = r_v \cdot g$. This is equivalent to requiring adversary $\mathcal{A}$ to solve ECCDHP in polynomial time, and therefore

$$\left|Adv_{\mathcal{A}}^{Game_3} - Adv_{\mathcal{A}}^{Game_2}\right| \leq Adv_{\mathcal{A}}^{ECCDHP}(rt). \quad (5)$$

Finally, the probability of adversary $\mathcal{A}$ guessing $c = 1$ is:

$$Adv_{\mathcal{A}}^{Game_3} = \frac{1}{2} + \varepsilon. \quad (6)$$

From (2), (3) and (6), we have

$$\begin{aligned}\frac{1}{2}Adv_{\mathcal{A}}^{LCDMA}(rt) &= \left|Adv_{\mathcal{A}}^{Game_0} - \frac{1}{2}\right| = \left|Adv_{\mathcal{A}}^{Game_1} - \frac{1}{2}\right| \\ &= \left|Adv_{\mathcal{A}}^{Game_1} - Adv_{\mathcal{A}}^{Game_3} + \varepsilon\right|. \quad (7)\end{aligned}$$

Based on (4) and (5), we can get:

$$\begin{aligned}Adv_{\mathcal{A}}^{Game_1} - Adv_{\mathcal{A}}^{Game_3} &= \left|Adv_{\mathcal{A}}^{Game_1} - Adv_{\mathcal{A}}^{Game_2}\right| + \left|Adv_{\mathcal{A}}^{Game_2} - Adv_{\mathcal{A}}^{Game_3}\right| \\ &\leq \frac{q_{hash}^2 + \left(q_{exe} + q_{send}\right)^2}{2\left|Hash\right|} + Adv_{\mathcal{A}}^{ECCDHP}(rt). \quad (8)\end{aligned}$$

Combining (7) and (8) leads to (1), and this completes the proof.

5.3 Mutual Identity Authentication

During the cross-domain access local information enrollment stage, $CDA\text{-}MNode$'s local domain server $DA\text{-}Server_i$ completes $CDA\text{-}MNode$'s intra-domain identity authentication before cross-domain access. In particular,

$DA\text{-}Server_i$ generates a cross-domain identity authentication message $M_0 = h_4\left(PID_{DAS_i}, PID_{MN}, AK_{i\text{-}j}, R_x\right)$ between $CDA\text{-}MNode$ and $DA\text{-}Server_j$ for $CDA\text{-}MNode$. When $CDA\text{-}MNode$ receives the message $\left\{H_2, R_b^*, T_2, M_0, PK_{DAS_j}^{**}\right\}$ sent from $DA\text{-}Server_i$, it verifies the validity of $DA\text{-}Server_i$'s identity. This process not only realizes the mutual authentication between $CDA\text{-}MNode$ and its local authentication server $DA\text{-}Server_i$, but also generates important credentials M_0 for $CDA\text{-}MNode$'s cross-domain access.

In cross-domain authentication and key agreement, $CDA\text{-}MNode$ puts its own identity information and M_0 into $M_1 = h_5\left(PID_{MN}, PID_{DAS_i}, R_u, M_0, PK_{DAS_j}^{**}, T_3\right)$ together. After $DA\text{-}Server_j$ receives the data packet, it orderly verifies M_1 and M_0 to determine the legitimacy of $CDA\text{-}MNode$, and hence completing $DA\text{-}Server_j$ to $CDA\text{-}MNode$ one-way authentication process. After that, $DA\text{-}Server_j$ sends the generated session key and authentication information to $CDA\text{-}MNode$, and $CDA\text{-}MNode$ verifies the legality of $DA\text{-}Server_j$'s identity after receiving the message, and hence realizing the cross-domain mutual authentication process between $CDA\text{-}MNode$ and $DA\text{-}Server_j$.

In the proposed LCDMA, the authentication keys $AK_{MN\text{-}i} = F\left(PID_{DAS_i}, PID_{MN}\right)$ and $AK_{j\text{-}i} = F\left(PID_{DAS_j}, PID_{DAS_i}\right)$ are the key parts of mutual authentication. The identity authentication key AK uses the binary t-degree symmetric polynomial $F(x,y) = \left(\sum_{m,n=0}^{t} a_{m,n} x^m y^n\right) \bmod p$, and its security is based on the property that the t-degree symmetric polynomial needs $t+1$ values to reconstruct. Even if adversary $\mathcal{A}$ captures all member nodes in a domain, it cannot obtain the t-degree symmetric polynomial in the domain. This is because if an attacker wants to reconstruct the polynomial, it must capture the key values of at least $t+1$ member nodes in the domain during the establishment of the session key to reconstruct the polynomial. However, the number of nodes in each domain is only t at most, and hence the attacker cannot reconstruct the cryptography polynomial. Therefore, LCDMA realizes both the intra-domain mutual authentication and the cross-domain mutual authentication. The use of random numbers in the interaction process also ensures the freshness of the message.

5.4 Session Key Agreement

When $CDA\text{-}MNode$ and $DA\text{-}Server_j$ complete the mutual identity legality authentication for IoT environment, they also complete the session key security agreement. In the session key $SK_{j\text{-}MN} = h_7\left(R'_u, R_v, R_w, T_4\right)$, $R_u = r_u \cdot g$, $R_v = r_v \cdot g$, and $R_w = r_v \cdot R'_u$ are mainly determined by the random secret numbers r_u and r_v selected by the two parties, respectively. Therefore, neither party can forge the legitimate session key. At the same time, the secure storage of the random secret numbers r_u and r_v ensures the security of the session key, and the randomness of the secret number ensures the freshness of the session key. If an attacker wants to crack the session key, it needs to calculate $R_w = r_u \cdot r_v \cdot g$ through $R_u = r_u \cdot g$ and $R_v = r_v \cdot g$. This is equivalent to requiring the attacker to solve ECCDHP in polynomial time, which is impossible to achieve.

5.5 Forward/Backward Security of Session Key

$CDA\text{-}MNode$ and $DA\text{-}Server_j$ use different random secret numbers to agree session key each time, and the session key is generated by the random secret numbers. Specifically, in the process of $CDA\text{-}MNode$'s cross-domain access, the strong freshness of random secret numbers ensures that the disclosure of a key agreement parameter will not pose a threat to the security of existing and upcoming session key. That is, the session key in LCDMA has forward and backward security.

5.6 Anonymity

Adversary $\mathcal{A}$ cannot obtain the real ID from the pseudo-identity information PID, because $PID_{MN} = SEnc_{sk}\left(ID_{MN} \oplus \xi_{MN} \oplus T_{RMN}, xi_{MN}, T_{RMN}\right)$ is realized by $IoT\text{-}TC$ using symmetric encryption algorithm, and it is encrypted with the private key of $IoT\text{-}TC$. Since $IoT\text{-}TC$ is trusted, it is impossible for adversary $\mathcal{A}$ to obtain the real identity of mobile nodes. Therefore, LCDMA guarantees the anonymity of mobile nodes in IoT.

5.7 Traceability

If some security events in IoT application need to be traced , $IoT\text{-}TC$ can use the private key to obtain the real identity information of mobile nodes, that is, decrypt the real identity ID of the mobile nodes from the pseudo-identity information PID. Therefore, LCDMA realizes the traceability of mobile nodes.

5.8 Man-in-the-middle Attack

We now show that LCDMA is effective against man-in-the-middle attack in IoT environment. Suppose that adversary $\mathcal{A}$ tries to pretend to be $CDA\text{-}MNode$ or $DA\text{-}Server$ to send messages to their communication partners. But in LCDMA, all messages are verified after they are received by the receiver, and the verification cannot be done when some key information is unknown. For example, in the cross-domain authentication stage, $CDA\text{-}MNode$ needs to send the message $\left\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK_{DAS_j}^{**}, T_3\right\}$ to $DA\text{-}Server_j$, and adversary $\mathcal{A}$ has to forge a legitimate message to pass the verification. However, for the forged message to pass the verification of the participants, $\mathcal{A}$ must know the authentication key $AK_{i\text{-}MN}$ or $AK_{MN\text{-}i}$ protected by the anti-collision one-way hash function between $CDA\text{-}MNode$ and $DA\text{-}Server_j$, in order to forge the legitimate M_0 and M_1. Since the authentication key $AK_{i\text{-}MN}$ or $AK_{MN\text{-}i}$ is obtained by a binary t-degree symmetric polynomial, LCDMA can effectively resist man-in-the-middle attack.

5.9 Replay Attack

In LCDMA, the participating entities, $CDA\text{-}MNode$, $DA\text{-}Server_i$ and $DA\text{-}Server_j$, are provided with the current timestamp, and the entity can verify whether the transmission delay of the message exceeds the maximum transmission delay ΔT after receiving each message. Armed with the secure negotiation and secret storage of session key as

well as the use of random numbers and message timestamps in the message exchange process, LCDMA has the ability to prevent attacker from laughing replaying attack.

6 Performance Evaluation

In this section, we compare the security features and efficiency of the proposed LCDMA scheme with those of five existing representative schemes for IoT environment. Efficiency comparison will focus on computation and communication overhead.

6.1 Benchmark Schemes

The following five benchmark schemes are used in the performance comparison with our LCDMA.

1) PSAP [10]: is a provable, secure and anonymous direct cross-domain authentication scheme for IoT mobile nodes. The mobile nodes use the cross-domain certificate provided by the local domain server to complete the cross-domain authentication process.
2) FCCDA [15]: is a secure cross-domain key agreement and user authentication scheme for fog computing, which aims to protect user privacy while realizing authentication and secure communication between different entities.
3) SAAR [21]: is a two-factor-based anonymous cross-domain authentication scheme.
4) SPMA [12]: is a mutual authentication scheme designed using lightweight cryptographic primitives.
5) CDHSM [11]: is a provable, secure and symptom-matching authentication scheme for cross-domain authentication in mobile medical social networks.

6.2 Comparison of Security Features

Table 2 compares the security features of our LCDMA scheme and the five existing schemes. It can be seen from Table 2 that LCDMA provides more security attributes than the five benchmarks. Specifically, LCDMA completes both cross-domain mutual authentication and intra-domain mutual authentication, but PSAP, SAAR, SPMA and CDHSM only implement cross-domain mutual authentication. Compared with PSAP, FCCDA, SAAR and SPMA, LCDMA retains the security traceability of $IoT\text{-}TC$ to mobile nodes while meeting the anonymity requirements of mobile nodes. The traceability is important to improve security trace to the source.

6.3 Comparison of Computation Overhead

For convenience, we define the symbols of basic cryptographic operations and refer to [15] for the corresponding execution times as shown in Table 3. The JPBC cryptographic library is used to implement various cryptographic operations, while the hardware environment employs Inter i7-6700 processor with 3.40 GHz CPU and 8 G memory, and the software environment adopts Windows 10 operating system.

TABLE 2
Comparison of Security Features

	PSAP	FCCDA	SAAR	SPMA	CDHSM	LCDMA
F_1	✓	✓	✓	✓	✓	✓
F_2	×	✓	×	×	×	✓
F_3	✓	✓	✓	✓	✓	✓
F_4	✓	✓	✓	✓	✓	✓
F_5	✓	✓	✓	✓	✓	✓
F_6	✓	✓	✓	✓	✓	✓
F_7	✓	✓	×	✓	×	✓
F_8	×	✓	✓	✓	×	✓
F_9	✓	✓	×	×	✓	✓
F_{10}	×	✓	×	×	✓	✓
F_{11}	✓	✓	✓	✓	✓	✓
F_{12}	×	×	×	×	✓	✓

F_1: Cross-domain mutual authentication; F_2: Intra-domain mutual authentication; F_3: Session key security agreement; F_4: Forward/backward security; F_5: Anti-forgery attack; F_6: Anti-man-in-the-middle attack; F_7: Resist replay attack; F_8: Anti-dictionary offline attack; F_9: Suitable for multi-server environment; F_{10}: Resist server simulation attack; F_{11}: Identity anonymity; F_{12}: Security traceability.
Feature exists: ✓; Feature does not exist: ×.

TABLE 3
Execution Times of Basic Cryptography Operations

Symbol	Description	Execution time (ms)
T_{ecm}	Execution time for an elliptic curve point multiplication	13
T_{eca}	Execution time for an elliptic curve point addition	5
T_h	Execution time for the hash operation	0.6
T_{pair}	Execution time of a bilinear pairing	25
T_{sed}	Execution time of a symmetric encryption/decryption	6
T_{pkd}	Execution time of public key encryption	43
T_{ske}	Execution time of private key decryption	9
T_{g-sig}	Execution time for identity-based signature generation	57
T_{u-sig}	Execution time for identity-based signature verification	7

For a cross-domain authentication scheme in IoT, the computing entities include mobile nodes, local domain managers, and remote domain managers. In the process of cross-domain authentication and access, the mutual identity authentication process between domains is relatively frequent. We count the numbers of basic cryptographic operations used by the six schemes in the cross-domain authentication process, and the results are listed in Table 4.

In addition, we calculate the computation overhead used by each entity in the authentication process and the total computation overhead of each scheme, in terms of time consumed, and the results obtained for the six schemes are compared in Fig. 7. It can be seen that our LCDMA scheme imposes the lowest computation time.Because only a small amount of elliptic curve point multiplication and hash operations are used in LCDMA, other more complex cryptographic operations, such as bilinear pair and public key encryption and decryption, are not required by LCDMA.

6.4 Comparison of Communication Overhead

We assume that the length of identity information is 160 bits, the length of random number is 160 bits, the length of timestamp is 32 bits, the length of hash digest is 160 bits (we use the SHA-160 hash function), symmetric encryption and

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3252051

TABLE 4
Computation Overheads of Six Schemes in Terms of Numbers of Cryptography Operations Required

Entity / Scheme	Mobile nodes	Local domain managers	Remote domain managers	Total
PSAP	$7T_{ecm}+T_{eca}+2T_h$ $+T_{pkd}+T_{u-sig}$	-	$4T_{ecm}+T_{eca}+2T_h+$ $2T_{pair}+T_{ske}+2T_{g-sig}$	$11T_{ecm}+2T_{eca}+4T_h+2T_{pair}+$ $T_{pkd}+T_{ske}+T_{u-sig}+T_{g-sig}$
FCCDA	$3T_{ecm}+5T_h$	$5T_h$	$4T_{ecm}+8T_h$	$7T_{ecm}+18T_h$
SAAR	$3T_{ecm}+5T_h$	$2T_{ecm}+5T_h$	$3T_{ecm}+4T_h$	$8T_{ecm}+14T_h$
SPMA	$7T_h$	$4T_h+T_{pkd}+T_{ske}$	$T_h+T_{pkd}+T_{ske}$	$12T_h+2T_{pkd}+2T_{ske}$
CDHSM	$6T_{ecm}+2T_{eca}+5T_h$	-	$6T_{ecm}+2T_{eca}+5T_h$	$12T_{ecm}+4T_{eca}+10T_h$
LCDMA	$3T_{ecm}+4T_h$	-	$4T_{ecm}+6T_h$	$7T_{ecm}+10T_h$

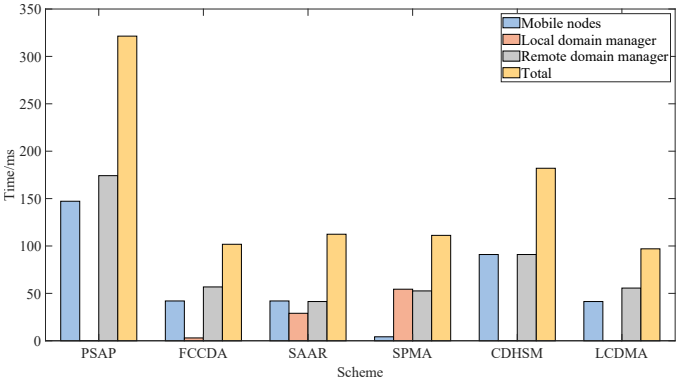

Fig. 7. Comparison of computation overhead (time) for six schemes

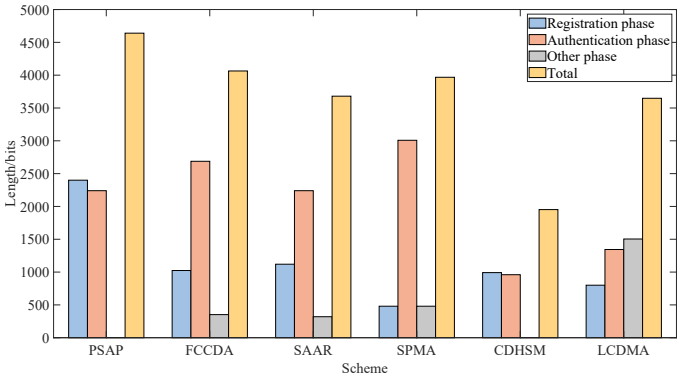

Fig. 8. Comparison of communication overhead (bits) for six schemes

TABLE 5
Communication Overheads of Six schemes in Terms of Bits

Phase / Scheme	Registration phase	Authentication phase	Other phases	Total
PSAP	2400	2240	-	4640
FCCDA	1024	2688	352	4064
SAAR	1120	2240	320	3680
SPMA	480	3008	480	3968
CDHSM	992	960	-	1952
LCDMA	800	1344	1504	3648

decryption algorithm is the advanced encryption standard (AES) [44] (the key length is 256 bits, the highest security), asymmetric encryption and decryption algorithm adopts the 1024-bit Rivest-Shamir-Adleman (RSA) algorithm [45], and the private key signature length is 1024 bits. Further assuming that the security of 160-bit ECC is equivalent to 1024-bit RSA, then the primes in the elliptic curve are 160 bits.

Table 5 lists the communication overheads of the six scheme, in terms of bits. In LCDMA, the data to be transmitted in the mobile node registration stage are $\{ID_{MN}, PW\}$ and $\{PID_{MN}, PID_{DAS_i}, AK_{MN\text{-}i}\}$, and the corresponding data length is $320 + 480 = 800$ bits. During the authentication and key agreement, $\left\{PID_{MN}, PID_{DAS_i}, M_0, M_1, PK_u, PK^{**}_{DAS_j}, T_3\right\}$ and $\{M_2, R^*_v, T_4\}$ need to be transmitted, and the corresponding data length is $992 + 352 = 1344$ bits. There is also an important link in the cross-domain access local information enrollment phase in LCDMA. The data to be transmitted are $\left\{PID_{MN}, PID_{DAS_j}, H_1, PK^{**}_{DAS_i}, R_a, T_1\right\}$ and $\left\{H_2, R^*_b, T_2, M_0, PK^{**}_{DAS_j}\right\}$, and the corresponding data length is $832 + 672 = 1504$ bits. Hence, the amount of the data transmitted in LCDMA totals 3648 bits.

The results of Table 5 are also presented in Fig. 8 for better visualization. It can be seen from Table 5 and Fig. 8 that LCDMA has the second lowest communication overhead, and only CDHSM has a lower communication overhead than LCDMA. However, LCDMA offers more security features than CDHSM. Specifically, unlike the proposed LCDMA scheme, CDHSM does not offer intra-domain mutual authentication and is not secure to resist replay attack and anti-dictionary offline attack.

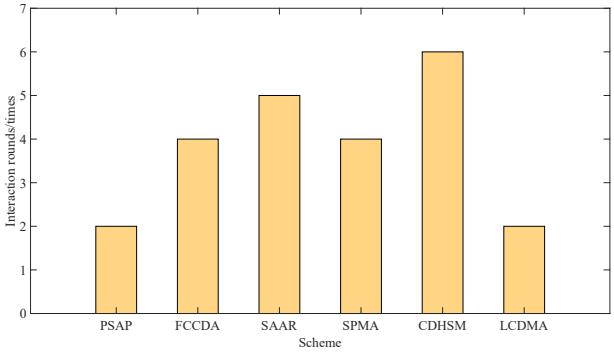

Fig. 9. Comparison of The Numbers of Interactive Rounds Needed By Six Schemes

Furthermore, Fig. 9 compares the numbers of interaction rounds required by the six schemes. Because data interactions between the verification parties are primarily transmitted over a common channel, the more rounds of interaction, the higher the risk of attack as well as higher the transmission delay. From Fig. 9, it can be seen that CDHSM has the highest number of interaction rounds, which is three times higher than LCDMA. It can also be seen that both LCDMA and PSAP has the lowest number of interaction rounds, which is two. However, our LCDMA has a slightly lower communication overhead than PSAP and more importantly, it offers much more security features than PSAP.

7 Conclusion

This paper has proposed a secure and lightweight cross-domain identity authentication scheme, called LCDMA, to

meet the requirements of cross-domain access in mobile IoT environment. LCDMA not only realizes the intra-domain mutual identity authentication between the mobile node and the local domain server, but also realizes the cross-domain mutual identity authentication between the mobile node and other domain servers. The security key negotiation process is completed during cross-domain communication, and the anonymity, privacy and security of the mobile node are guaranteed. The use of symmetric polynomial, rather than bilinear pairing in the traditional scheme, has minimized the computation and communication overhead of participating entities. Our security analysis and performance evaluation have demonstrated that LCDMA provides more security features than existing representative schemes as well as offers better performance in terms of computation and communication overhead.

ACKNOWLEDGMENTS

This work was supported by National Key Research and Development Program of China (Grant No. 2019YFB2102303), and National Natural Science Foundation of China (Grant Nos. 61971014 and 11675199).

REFERENCES

[1] J. T. Kelly, K. L. Campbell, E. Gong, and P. Scuffham, "The Internet of things: Impact and implications for health care delivery," *J. Medical Internet Research*, vol. 22, no. 11, e20135, Nov. 2020.

[2] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, Secondquarter 2020.

[3] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low power networks on Internet of things," *J. Supercomputing*, vol. 77, pp. 4778–4812, 2021.

[4] A. Badshah, M. Waqas, F. Muhammad, G. Abbas, Z. H. Abbas, S. A. Chaudhry and S. Chen, "AAKE-BIVT: Anonymous Authenticated Key Exchange Scheme for Blockchain-Enabled Internet of Vehicles in Smart Transportation," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1739-1755, Feb. 2023.

[5] Y. He, X. Guo, X. Zheng, Z. Yu, J. Zhang, H. Jiang, X. Na, and J. Zhang, "Cross-technology communication for the Internet of things: A survey," *ACM Computing Surveys*, Mar. 2022.

[6] A. Badshah, M. Waqas, F. Muhammad, G. Abbas and Z. H. Abbas, "A Novel Framework for Smart Systems Using Blockchain-Enabled Internet of Things," in *IT Professional*, vol. 24, no. 3, pp. 73-80, 1 May 2022.

[7] G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, and G. Spezzano, "IoT platforms and security: An analysis of the leading industrial/commercial solutions," *Sensors*, vol. 22, no. 6, pp. 1–17, 2022.

[8] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Computers & Security*, vol. 86, pp. 132–146, 2019.

[9] A. Xiang and J. Zheng, "A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks," *Electronics*, vol. 9, no. 6, p. 989, 2020.

[10] Y.-W. Zhou and B. Yang, "Provable secure authentication protocol with direct anonymity for mobile nodes roaming service in Internet of things," *J. Software*, vol. 2015, no. 9, pp. 2436–2450, 2015.

[11] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network," *IEEE Trans. Dependable and Secure Computing*, vol. 15, no. 4, pp. 633–645, Jul.-Aug. 2016.

[12] R. Shashidhara, M. Lajuvanthi, and S. Akhila, "A secure and privacy-preserving mutual authentication system for global roaming in mobile networks," *Arabian J. Science and Engineering*, vol. 47, no. 2, pp. 1435–1446, 2022.

[13] G. Abbas, M. Tanveer, Z. H. Abbas, M. Waqas, T. Baker, D. Al-Jumeily OBE, "A secure remote user authentication scheme for 6LoWPAN-based Internet of Things," in *PLoS ONE*, vol. 16, no.11, Nov. 2021.

[14] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical iot networks," *Computer Communications*, vol. 166, pp. 154–164, 2021.

[15] Y. Lin, X. Wang, Q. Gan, and M. Yao, "A secure cross-domain authentication scheme with perfect forward security and complete anonymity in fog computing," *J. Information Security and Applications*, vol. 63, pp. 103022-1–103022-13, Dec. 2021.

[16] P. Gope, S. H. Islam, M. S. Obaidat, R. Amin, and P. Vijayakumar, "Anonymous and expeditious mobile user authentication scheme for GLOMONET environments," *Int. J. Communication Systems*, vol. 31, e3461, pp. 1–18, 2018.

[17] J. Ding, P. Ke, C. Lin, and H. Wang, "Bivariate polynomial-based secret sharing schemes with secure secret reconstruction," *Information Sciences*, vol. 593, pp. 398–414, 2022.

[18] Y. Guo and Y. Guo, "FogHA: An efficient handover authentication for mobile devices in fog computing," *Computers & Security*, vol. 108, pp. 102358-1–102358-14, Sep. 2021.

[19] A. Badshah, M. Waqas, G. Abbas, F. Muhammad, Z. H. Abbas, S. Vimal and M. Bilal, "LAKE-BSG: Lightweight authenticated key exchange scheme for blockchain-enabled smart grids," in *Sustainable Energy Technologies and Assessments*, Vol. 52, pp.102248, Aug. 2022.

[20] W. Liang, S. Xie, J. Long, K.-C. Li, D. Zhang, and K. Li, "A double puf-based rfid identity authentication protocol in service-centric internet of things environments," *Information Sciences*, vol. 503, pp. 129–147, 2019.

[21] P. K. Roy and A. Bhattacharya, "Secure and authentic anonymous roaming service," *Wireless Personal Communications*, vol. 128, pp. 819–839, 2022.

[22] C.-C. Lee, Y.-M. Lai, C.-T. Chen, and S.-D. Chen, "Advanced secure anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1281–1296, 2017.

[23] R. Sarabi Miyanaji, S. Jabbehdari, and N. Modiri, "Continuous lightweight authentication according group priority and key agreement for internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 7, p. e4479, 2022.

[24] D. Kang, H. Lee, Y. Lee, and D. Won, "Lightweight user authentication scheme for roaming service in GLOMONET with privacy preserving," *Plos One*, vol. 16, no. 2, pp. 1-40, 2021.

[25] M. A. Qureshi and A. Munir, "Puf-rake: A puf-based robust and lightweight authentication and key establishment protocol," *IEEE Trans. on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2457-2475, 2022.

[26] L. Zhang, J. Xu, M. S. Obaidat, X. Li, and P. Vijayakumar, "A puf-based lightweight authentication and key agreement protocol for smart uav networks," *IET Communications*, vol. 16, no. 10, pp. 1142-1159, 2022.

[27] P. K. Sadhu, V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Easy-sec: Puf-based rapid and robust authentication framework for the internet of vehicles," *ArXiv*, vol. abs/2204.07709, 2022.

[28] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," *J. Information Security and Applications*, vol. 42, pp. 95–106, Oct. 2018.

[29] K. Hussain, N. Jhanjhi, H. Mati-ur Rahman, J. Hussain, and M. H. Islam, "Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes," *J. King Saud University – Computer and Information Sciences*, vol. 33, no. 4, pp. 417–425, May 2021.

[30] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Computers & Security*, vol. 88, pp. 101619-1–101619-13, Jan. 2020.

[31] S. Zhou, Q. Gan, and X. Wang, "Authentication scheme based on smart card in multi-server environment," *Wireless Networks*, vol. 26, no. 2, pp. 855–863, 2020.

[32] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J.Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Industrial Informatics*, vol. 15, no. 1, pp. 457–468, Jan. 2018.

[33] R. Shashidhara, S. Bojjagani, A. K. Maurya, S. Kumari, and H. Xiong, "A robust user authentication protocol with privacy-

preserving for roaming service in mobility environments," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 1943–1966, 2020.
[34] R. Madhusudhan and R. Shashidhara, "A novel DNA based password authentication system for global roaming in resource-limited mobile environments," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2185–2212, 2020.
[35] D. Boneh and R. J. Lipton, "Algorithms for black-box fields and their application to cryptography," in *Proc. CRYPTO 1996* (Santa Barbara, CA, USA), Aug. 18-22, 1996, pp. 283–297.
[36] V. Shoup, "Lower bounds for discrete logarithms and related problems," in *Proc. EUROCRYPT 1997* (Konstanz, Germany), May 11-15, 1997, pp. 256–266.
[37] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
[38] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, Jul.-Aug. 2018.
[39] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Information Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[40] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. EUROCRYPT 2001* (Innsbruck, Austria), May 6–10, 2001, pp. 453–474.
[41] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proc. ProvSec 2007* (Wollongong, Australia), Nov. 1-2, 2007, pp. 1–16.
[42] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Computers*, vol. 51, no. 5, pp. 541–552, May 2002.
[43] P. Flajolet, D. Gardy, and L. Thimonier, "Birthday paradox, coupon collectors, caching algorithms and self-organizing search," *Discrete Applied Mathematics*, vol. 39, no. 3, pp. 207–229, Nov. 1992.
[44] J. Daemen J and V. Rijmen,"AES proposal: Rijndael," Document version 2, 1999.
[45] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

Bei Gong received his Ph.D. degree from the Beijing University of Technology in 2012. He participates in six National invention patents and one monograph textbook. In the past five years, he has published more than 30 papers in first-class SCI / EI and other famous international journals and top international conferences in relevant research fields. His research interests include trusted computing, Internet of things security, mobile Internet of things, and mobile edge computing. He has presided over 8 national projects, such as the National Natural Science Foundation and 6 provincial and ministerial projects, such as the general science and technology program of the Beijing Municipal Education Commission. Email: gongbei@bjut.edu.cn.

Guiping Zheng pursuing her PhD degree in Beijing University of Technology, Beijing, China. She received her M.S. degree in the Beijing University of Technology, Beijing, China. Her research interests include Internet of things security, trust management, and identity authentication.

MUHAMMAD WAQAS (M'18, SM'22) received his PhD degree (Sept. 2015 – Jun. 2019) with the Department of Electronic Engineering, Tsinghua University, Beijing, China. From Oct. 2019 to Sept. 2021, he was a Postdoctoral researcher at the Faculty of Information Technology, Beijing University of Technology, Beijing, China. Currently, he is an Assistant Professor at the Computer Engineering Department, College of Information Technology, University of Bahrain, Bahrain. He is also an Adjunct Senior Lecturer at the School of Engineering, Edith Cowan University, Australia. He has more than 100 research publications in reputed Journals and Conferences. He is an Associate Editor of International Journal of Computing and Digital Systems. His current research interests are in the areas of Wireless Communication, vehicular networks, Fog/Mobile Edge Computing, Internet of Things and Machine Learning.

SHANSHAN TU received his PhD degree from Computer Science Department at Beijing University of Posts and Telecommunications in 2014. From 2013 to 2014, he visited the University of Essex for National Joint Doctoral Training. He worked in the Department of Electronic Engineering at Tsinghua University as a post-doctoral researcher from 2014 to 2016. He is currently an associate professor in the Faculty of Information Technology, Beijing University of Technology, China. His research interests are in cloud computing, MEC and information security techniques.

Sheng Chen (Fellow, IEEE) received PhD degree in control engineering from City, University of London in 1986, and the Doctor of Sciences (D.Sc.) degree from the University of Southampton, Southampton, U.K., in 2005. Since 1999, he has been with the School of Electronics and Computer Science, the University of Southampton, where he is currently a Professor in intelligent systems and signal processing. He has more than 17 700 Web of Science citations with an H-index 58 and more than 34 900 Google Scholar citations with H-index 80. His research interests include adaptive signal processing, wireless communications, modeling and identification of nonlinear systems, neural network and machine learning, intelligent control system design, and evolutionary computation methods and optimization. He is a fellow of the UK Royal Academy of Engineering, fellow of Asia–Pacific Artificial Intelligence Association, and fellow of IET.