Deniable-Based Privacy-Preserving Authentication Against Location Leakage in Edge Computing

Shengke Zeng, Hongjie Zhang, Fei Hao, and Hongwei Li, *Senior Member, IEEE*

***Abstract*—Edge computing provides cloud services at the edge of the network for Internet of Things (IoT) devices. It aims to address low latency of the network and alleviates data processing of the cloud. This "cloud-edge-device" paradigm brings convenience as well as challenges for location-privacy protection of the IoT. In the edge computing environment, the fixed edge equipment supplies computing services for adjacent IoT devices. Therefore, edge computing suffers location leakage as the connection and authentication records imply the location of IoT devices. This article focuses on the location awareness in the edge computing environment. We adopt the "deniability" of authentication to prevent location leakage when IoT devices connect to the edge nodes. In our solution, an efficient deniable authentication based on a two-user ring signature is constructed. The robustness of authentication makes the fixed edge equipment accept the legal end devices. Besides, the deniability of authentication cannot convince any third party that the fact of this authentication occurred as communication transcript is no longer an evidence for this connection. Therefore, it handles the inherent location risk in edge computing. Compared to efficient deniable authentications, our protocol saves 10.728% and 14.696% computational cost, respectively.**

***Index Terms*—Deniability, edge computing, location privacy, privacy-preserving authentication.**

I. Introduction

EDGE computing is a distributed computing paradigm that brings cloud resources closer to Internet of Things (IoT) devices or local edge servers. Compared to the traditional cloud computing, edge computing improves response time and gains better bandwidth availability [1]. In edge computing, the edge equipment location is known and fixed as the beacon node. In order to reduce communication costs, IoT devices usually select the nearest edge equipment to conduct the tasks. Obviously, the edge computing paradigm discloses the locations of IoT devices to the public.

On the other hand, authentication is necessary for IoT devices to connect and communicate with edge equipment for the access control and data query [2]. When communication occurs, it ensures that IoT devices are the legal counterparties and the messages delivered from the source are intact. Digital signature seems to be an alternative to realizing identity authentication and message authentication. However, the public verifiability of digital signature convinces anyone that this authentication is made by the source. Therefore, the locations of IoT devices are revealed naturally from the communication with the edge equipment.

Let us consider this scenario. The user travels with some wearable devices. These devices collect and process data for a better experience in this travel. Therefore, the devices have to make authentication with the edge equipment in order to enjoy the computing service. The authentication records reveal the location of user devices as edge equipment is fixed and the communication distance is short. Obviously, the continuous communication records reflect the user's traveling routine [3].

Location is a kind of very important privacy information for clients as same as the identity of users. Some research indicates that the location information is closely related to the individual habits, activities, and relationships [4]. Therefore, the location privacy receives great concerns [5]–[7]. Many solutions for protecting user's location privacy are proposed. The straight approach regarding to location privacy is to use pseudonyms to make the user identity and location information irrelevant [8]. It requires to carry a great number of certificates for the user to achieve the strong privacy; thus, it is inefficient in terms of storage. The second one is to enlarge the user's location into a region, in which the accurate location information is replaced by a coarse-grained position to prevent the attacker from learning the exact location. In the spatial cloaking technique [9], the user's location is hidden in a large cloaked area such that it cannot be pinpointed by the attacker. This kind of approach always degrades the quality of location-based services (LBSs). The mix-zone technique is also widely employed for location privacy [10], [11], which allows the users to exchange their pseudonyms in a dedicated area. Therefore, dummy users have to be created for privacy if there is short of sufficient neighboring users in the area (mix zone). K-anonymity, as another kind of

Manuscript received August 29, 2020; revised October 11, 2020 and November 20, 2020; accepted December 28, 2020. This work was supported in part by the Ministry of Education "chunhui plan" under Grant Z2016150, in part by the Sichuan Science and Technology Program under Grants 2018GZDZX0008, 2019YFG0508, 2019YFG0509 and 2020JDTD0007, in part by the National Natural Science Foundation of China under Grant 61702317, and in part by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Sklodowska-Curie Grant 840922. *(Corresponding author: Fei Hao.)*

Shengke Zeng is with the School of Computer and Software Engineering, Xihua University, Chengdu 610039, China, and also with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: zengshengke@gmail.com).

Hongjie Zhang is with the School of Computer and Software Engineering, Xihua University, Chengdu 610039, China (e-mail: 18280418253@163.com).

Fei Hao is with the School of Computer Science, Shaanxi Normal University, Xi'an 710119, China, and also with the Department of Computer Science, College of Engineering, Mathematics, and Physical Sciences,University of Exeter, Exeter EX4 4QF, U.K. (e-mail: feehao@gmail.com).

Hongwei Li is with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: hongweili@uestc.edu.cn).

Digital Object Identifier 10.1109/JSYST.2021.3049629

approach to handle privacy [12], [13], is to utilize other $k-1$ positions to cover user location. Obviously, it requires a mass of location information to be involved in the privacy preservation. Since the location information is confidential in location-aware applications, the cryptographic algorithms are employed to encrypt the location data. Homomorphic encryptions are used to protect the location privacy during localization [14]–[17]. Undoubtedly, cryptographic primitives provide high-level privacy but also lead to heavy computation and storage. In addition, differential privacy is also an important tool to prevent disclosing sensitive information [18], [19]. Recently, differential privacy technology is used to protect user's location privacy by a geoindistinguishable task allocation [20].

In summary, the existing location privacy studies mainly focus on preventing the location leakage to the attacker or the server, which provides the LBS; therefore, encryptions or obfuscated location is necessary. Thus, both efficiency and service quality are always the victims of privacy protection. On the other hand, encrypting position or coarse position does not take effect in the edge computing environment. Since authentication is necessary for access control in edge computing, the authentication records reveal the location naturally. Although the identity anonymity technique enables IoT devices locations irrelevant to their identities, it cannot defend against the attackers with prior knowledge. Obviously, the solution is to make the communication between IoT devices and the fixed edge equipment "off the record." In other words, we make the conversation peer has no evidence, to convince any third party, of the fact that this connection has occurred. The location privacy is preserved although the communication peer captures the accurate location. Therefore, the service quality is not reduced. This off-the-record communication can be viewed as the *deniability* capability to the protocol participants.

Indeed, deniability is an important privacy-preserving feature of cryptographic protocols. On the other hand, the authentications during the connections between IoT devices and edge equipment are necessary. If the location privacy preservation is also required, the authentication protocol with deniability should be considered without degrading the service quality. With deniable authentication (DA), the edge equipment guarantees the legality of IoT devices. And the edge equipment cannot prove to any third party that this IoT device was ever involved in this connection. In other words, this connection is "off the record," which is a critical clue to provide the client privacy. Obviously, there is no evidence of revealing the connection to the edge equipment.

A. Contributions

In this article, we aim to present a location privacy-preserved scheme in edge computing based on DA. We focus on the communication round, strong privacy, and practicability. Latency is the critical evaluation metric in edge computing; therefore, low communication capacity should be concerned for practicality [21]. However, noninteractive DAs reach the *partial* deniability only. It implies that only the receiver (not anyone) makes simulation. Therefore, the sender can deny its involvement as the receiver may produce the indistinguishable communication transcript. Unfortunately, *partial* deniability is not enough for the edge computing scenario since the receiver is an edge equipment, which might be a trusted party by the public. Therefore, the communication transcript points to the client (the IoT device). Thus, we focus on the optimal communication round with *full* deniability. In order to make the authentication protocol applicable to the Internet-based service practically, we should consider the concurrent environment. However, rewinding steps are indispensable in the traditional approaches of *full deniability* in the case of malicious verifiers. It causes that the concurrent deniability does not hold and the heavy communication cost also degrades the quality of service in edge computing. In addition, the encryption algorithm is a common primitive to construct DA protocols [22], [23]. The underlying cost is that the encryption must be against adaptive chosen ciphertext attack (CCA2), which is inefficient for practice. In order to suit for practicable and strong-privacy-required applications, we construct a two-round authentication protocol with full and concurrent deniability. We adopt different primitives to avoid a chosen ciphertext attack (CCA) paradigm and any strong number-theoretic assumptions. The major contributions of this article are summarized as follows.

1) We present a privacy-preserving authentication scheme with *full* deniability to avoid the location leakage of IoT devices in edge computing. The fact on deniability of communication is favorable for IoT devices as it does not have any evidence to show that IoT devices have ever been involved in some connection to the edge equipment. It preserves the location privacy of the IoT devices naturally.
2) We focus on both latency and concurrency of the edge computing environment. Most fully DAs are built on the zero-knowledge argument against the malicious verifier; thus, they require at least four rounds. This security is strong but not practical in communication applications. We observe that the communication round can be reduced to 2 if the verifier follows the protocol honestly. This assumption is feasible as the receiver in edge computing is the edge equipment, which is accepted by the public, and its behavior would be honest for its reputation. Therefore, this simplified two-round authentication protocol with full deniability is optimal for the IoT devices' connection to the edge equipment. In addition, our protocol does not require an extra challenge–response mechanism to extract the witness. Therefore, the deniability does not fail in concurrent settings, such as Internet environment.
3) We avoid the need for encryption algorithms in our construction to realize authentication; otherwise, the underlying encryption must be CCA2-secure, which is inefficient. Moreover, we are not dependent on strong and inefficient assumptions. The existed works to achieve the fully concurrent deniability by the timing constraints, plaintext awareness (PA) of the underlying encryption, knowledge of exponent assumption (KEA) or the public random oracles are inefficient or impracticable. Instead, we adopt the two-user ring signature to simulate the deniability. The

full deniability is met by the unconditional anonymity of the ring signature. Therefore, we avoid the underlying CCA2-secure primitive, strong number-theoretic assumptions, and public random oracles.

B. Organization

The rest of this article is organized as follows. Section II introduces the related work of DAs. Section III provides some preliminaries that are the building blocks in our protocol. Section IV describes the system model of edge computing and its security requirements. In Section V, we propose a privacy-preserving authentication scheme with full deniability and apply it to the edge computing environment to protect the location privacy for IoT devices. The security of our scheme is proven and the performance is analyzed in Section VI. Finally, Section VII concludes this article.

II. Related Work

DA was first introduced by Dolev *et al.* [24] and formally studied by Dwork *et al.* [22]. It follows the "simulation paradigm" to realize deniability. The authentication is deniable if the conversation transcript can be simulated without any secret. Therefore, participants can deny as someone else would produce this indistinguishable communication transcript. We call it *fully* deniable if this simulation can be run by anyone not only the verifier. The generic technique to realize the DA is to revoke the secret, which is used to authenticate in an appropriate phase. Thus, early works [22], [25] require more rounds to reveal the witness upon the receipt of the committed secret against malicious verifiers. In this way, the simulation is perfect as anyone with the revoked secret can simulate the statistically indistinguishable communication transcript.

However, this kind of approach leads to heavy communication rounds inevitably. It is not suitable for the Internet-based applications. In addition, the Internet is a fully concurrent environment. However, the simulation in constructions relying on revoked witness requires rewinding steps. Obviously, this deniability cannot hold in the concurrent scenario.

Some related works have been proposed to overcome this barrier. There exist some approaches to reveal the witness without rewinding steps. Di Raimondo and Gennaro [25] demonstrated that the assumption of PA [26] can be used to extract the witness. Inspired by Di Raimondo and Gennaro's idea, Zeng *et al.* [23] presented a DA with source hiding based on PA-secure multireceiver encryption. However, the underlying assumption is strong. Stinson and Wu [27] proposed a two-round deniable identification protocol. Its deniability against a dishonest verifier is based on the KEA and random oracles. Their scheme does not rely on any signatures or encryptions; thus, it can be used in identity authentication only. Jiang and Safavi-Naini [28] used the public random oracle to extract the witness to avoid the rewinding steps. Yao and Zhao [29] utilized the KEA to extract the witness to ensure the deniability in the concurrent interactive setting. Tian *et al.* [30] made use of the selectively unforgeable but existentially forgeable signature to simulate the transcript. Jiang [31] proposed a moderate encryption to realize deniability without rewinding by virtue of timed commitment. However, these works suffer the limitations such as the strong number-theoretic assumptions, inefficiency, or public random oracles.

The direct application of DA is to design the deniable key exchange protocols [28], [29], [32]. As Yao and Zhao [29] claimed, if the key exchange is deniable, then all the transactions using the session key generated by the key exchange can be deniable for both the participants. There are some other applications for DA. Some research works concern E-mail privacy [33], [34]. Li *et al.* [35] applied the DA to pervasive computing, and Zeng *et al.* [36] utilized the deniability to construct the privacy-preserving LBS.

III. Preliminaries

We present building blocks, including the DA and ring signature of our scheme, in this section.

A. Deniable Authentication

Generally, DA protocols enable a sender to speak to the receiver privately. In other words, the receiver can guarantee the legality of the sender but cannot convince others that the sender has participated in the authentication. It is realized without leaving the "paper trail" of the conversation. Formally, the communication record can be simulated by someone else. Therefore, there is no evidence to show the sender's involvement. In other words, the participates (not only the sender even the receiver) can deny the fact of an authentication conversation.

1) Security Properties of the DA Protocol: There are two roles in the authentication protocol, namely, the sender (prover, denoted as $\mathtt{P}$) and the receiver (verifier, denoted as $\mathtt{V}$). $\mathtt{P}$ authenticates a message $\mathtt{m}$ to $\mathtt{V}$. The fundamental security requirements of the DA protocol are *Completeness*, *Authentication (Unforgeability)*, and *Deniability*.

a) *Completeness:* $\mathtt{V}$ accepts the authentication for the message $\mathtt{m}$ with overwhelming probability if $\mathtt{P}$ and $\mathtt{V}$ follow the authentication protocol honestly.

b) *Authentication (unforgeability):* This property states that an attacker $\mathcal{A}$ cannot pretend to be the sender $\mathtt{P}$ to complete authentication. Consider the probabilistic polynomial time attacker $\mathcal{A}$ trying to forge a message. It adaptively chooses a sequence of arbitrary messages $\mathtt{m}_1, \mathtt{m}_2, \ldots$ and asks some good participant $\mathtt{P}_\mathtt{i}$ to authenticate $\mathtt{m}_\mathtt{i}$. We say that $\mathcal{A}$ succeeds if $\mathtt{V}$ accepts $\mathcal{A}$'s authentication to message $\mathtt{m} \notin \{\mathtt{m}_\mathtt{i}\}_{i=1,2,\ldots}$ as $\mathtt{P}_\mathtt{i}$ and $\mathcal{A}$ does not have $\mathtt{P}_\mathtt{i}$'s secret. The authentication (unforgeability) requirement is that the probability of success of $\mathcal{A}$ is negligible.

c) *Deniability:* This property states that $\mathtt{P}$ and $\mathtt{V}$ can deny the involvement of authentication. Formally, the deniability can be captured by the *simulation* paradigm. The adversary $\mathcal{A}$'s view of this conversation can be simulated by a simulator $\mathcal{M}$ without the secret of the sender $\mathtt{P}$, and the two transcripts (the real one and the simulated one) have the same distribution. Therefore, the real authentication transcript cannot be convinced by others as it can be performed by running $\mathcal{M}$. In addition, the concurrent

Round 1. $\mathtt{V} \rightarrow \mathtt{P}$: $\mathtt{V}$ randomly chooses value r and computes $c = E_{v_\mathtt{P}}(\mathtt{m} \parallel r)$.
Round 2. $\mathtt{P} \rightarrow \mathtt{V}$: Upon receiving message c, $\mathtt{P}$ decrypts c by its private key $s_\mathtt{P}$ and obtains the suffix of plaintext, namely r. Technically, $\mathtt{P}$ returns $d = E_{v_\mathtt{P}}(r)$ instead of r. d can be viewed as the commitment of r as $E(\cdot)$ is non-malleable.
Round 3. $\mathtt{V} \rightarrow \mathtt{P}$: Upon receiving message d, $\mathtt{V}$ opens c using the random encryption coin ρ used in the encryption in Round 1 and returns (r, ρ) to $\mathtt{P}$.
Round 4. $\mathtt{P} \rightarrow \mathtt{V}$: Upon receiving message (r, ρ), $\mathtt{P}$ checks the correct r and opens d by revoking the random encryption coin σ used in the encryption in Round 2.
Finally, $\mathtt{V}$ accepts $\mathtt{P}$'s authentication if d is opened correctly.

Fig. 1. Dwork *et al.*'s DA protocol.

deniability should be considered in the interactive fashion. In the Internet-based environment, the attacker $\mathcal{A}$ may launch a concurrent interaction with $\mathtt{P}$ by arbitrary interleaved steps. The concurrent deniability should hold even in such a setting. We denote the interaction between $\mathcal{A}$ and the real sender $\mathtt{P}$ by $\Gamma^{\mathtt{rea}}$, and the interaction between $\mathcal{A}$ and the simulator $\mathcal{M}$ by $\Gamma^{\mathtt{sim}}$. The authentication is deniable if a distinguisher $\mathcal{D}$'s views in $\Gamma^{\mathtt{rea}}$ and $\Gamma^{\mathtt{sim}}$ are indistinguishable. Formally, $|\Pr[\mathcal{D}(\mathtt{view}(\mathcal{A}, \Gamma^{\mathtt{rea}})) = 1] - \Pr[\mathcal{D}(\mathtt{view}(\mathcal{A}, \Gamma^{\mathtt{sim}})) = 1]| \approx \mathtt{negl}(\kappa)$, where $\mathtt{negl}(\kappa)$ is a negligible function for the security parameter κ.

2) Review of the DA Protocol: Let us review the traditional DA protocol proposed by Dwork *et al.* [22] to explain the *Authentication (Unforgeability)* and the *Deniability*. In this protocol, $\mathtt{P}$ has a public–private keypair $(v_\mathtt{P}, s_\mathtt{P})$ of a nonmalleable encryption algorithm $E(\cdot)$. $\mathtt{P}$ and $\mathtt{V}$ perform the interactive DA protocol, as shown in Fig. 1.

Only the legal sender $\mathtt{P}$ can get the right r with the decryption key $s_\mathtt{P}$. Therefore, the correct r implies $\mathtt{P}$'s authentication. On the other hand, the exposure of r in *Round 3* is the vital step to realize the deniability. With r, anyone can produce d even without the secret $s_\mathtt{P}$. We can see that this simulation is perfect after seeing r. Therefore, we say that this perfect simulation run by anyone is realized by rewinding steps. Note that this kind of deniability does not hold in a concurrent environment due to its rewinding steps. Dwork *et al.* [22] handled this problem by timing assumption.

3) Full Deniability Versus Partial Deniability: The advantage of noninteractivity is reflected in the communication overhead. Noninteractivity handles the concurrency problem naturally as it requires one round. However, the noninteractive DA achieves partial deniability only. Obviously, the transcripts in the noninteractive DA protocol cannot be simulated by anyone; otherwise, it conflicts the unforgeability. The generic construction of noninteractive DA is to calculate the authentication tag with the sender's secret and the receiver's public key [35]. In this way, the receiver is assured that a message originated from the sender but cannot prove this to any third party, just like the designated-verifier signature. However, the transcript can only be simulated by using receiver's secret. In other words, it only realizes the partial deniability.

The full deniability states that the conversation transcript can be simulated by anyone, not only the receiver. It is proven to be simulatable with the challenge–response subprotocol. Therefore, it must be realized by the interactive steps. The full deniability is more practical in terms of strong privacy compared to partial deniability. Since only the receiver can simulate the transcript in the partially DA, it results that either the sender or the receiver is bound to this authentication. If the receiver (i.e., service provider) is accepted by the public, it is unfair for the sender (i.e., client). Therefore, we focus on the full deniability in our application.

B. Ring Signature

The ring signature scheme is used to sign a message anonymously. Given a valid ring signature σ w.r.t. a message $\mathtt{m}$ and a set of public keys $\mathcal{PK} = \{\mathtt{PK}_1, \ldots, \mathtt{PK}_\mathtt{n}\}$, any verifier cannot decide which user in the ring $\mathcal{PK}$ is the actual signer even if the secret keys of all the users in $\mathcal{PK}$ are exposed.

The syntax of the ring signature is as follows.

Definition 1 (Ring Signature): A ring signature scheme is a triple of algorithms $(\mathtt{KGen}, \mathtt{RSig}, \mathtt{RVer})$.

1) A probabilistic key generation algorithm $\mathtt{KGen}(1^\kappa)$: Given the security parameter κ, output the keypair $(\mathtt{PK}_\mathtt{i}, \mathtt{SK}_\mathtt{i})$ for user $\mathtt{i}$, that is, $(\mathtt{PK}_\mathtt{i}, \mathtt{SK}_\mathtt{i}) \leftarrow \mathtt{KGen}(1^\kappa)$.
2) A probabilistic ring signing algorithm $\mathtt{RSig}(\mathtt{m}, \mathcal{PK}; \mathtt{SK}_\mathtt{s})$: Given a message $\mathtt{m}$, a ring $\mathcal{PK}$, and the private (signing) key $\mathtt{SK}_\mathtt{s}$ of the signer $\mathtt{s}$ ($\mathtt{PK}_\mathtt{s} \in \mathcal{PK}$), output the ring signature σ, that is, $\sigma \leftarrow \mathtt{RSig}(\mathtt{m}, \mathcal{PK}; \mathtt{SK}_\mathtt{s})$.
3) A deterministic verification algorithm $\mathtt{RVer}(\mathtt{m}, \sigma, \mathcal{PK})$: Given the ring signature σ and the message $\mathtt{m}$ with respect to the ring of public keys $\mathcal{PK}$, determine whether σ is valid w.r.t. $(\mathtt{m}, \mathcal{PK})$. That is to check $\mathtt{RVer}(\mathtt{m}, \sigma, \mathcal{PK}) \stackrel{?}{=} 1$.

The properties of a secure ring signature contain *Completeness*, *Unconditional Anonymity*, and *Unforgeability*.

Completeness: For any $\{\mathtt{PK}_\mathtt{i}, \mathtt{SK}_\mathtt{i}\}_{i=1}^n$ output by $\mathtt{KGen}(1^\kappa)$, any $\mathtt{s} \in \{1, 2, \ldots, n\}$, and any message $\mathtt{m}$, we have $\mathtt{RVer}(\mathtt{m}, \mathtt{RSig}(\mathtt{m}, \mathcal{PK}; \mathtt{SK}_\mathtt{s}), \mathcal{PK}) = 1$, where $\mathcal{PK} = \{\mathtt{PK}_1, \ldots, \mathtt{PK}_\mathtt{n}\}$.

Unconditional anonymity: This property states that an attacker is not able to tell which user in a ring $\mathcal{PK}$ produced the signature σ, although it obtains the signing keys of all the users in $\mathcal{PK}$. Formally, we consider the anonymity game as follows.

Given a ring signature scheme $(\mathtt{KGen}, \mathtt{RSig}, \mathtt{RVer})$ and an adversary $\mathcal{A}$, the *anonymity game* is as follows.

1) For $\mathtt{i} = 1, 2, \ldots$, generate $(\mathtt{PK}_\mathtt{i}, \mathtt{SK}_\mathtt{i}) \leftarrow \mathtt{KGen}(1^\kappa)$, $\mathcal{A}$ is given $\mathcal{R} = \{\mathtt{PK}_1, \mathtt{PK}_2, \ldots\}$.
2) $\mathcal{A}$ is given access to an oracle $\mathtt{Osign}(s, \mathtt{m}, \mathcal{PK})$, which returns $\mathtt{RSig}(\mathtt{m}, \mathcal{PK}; \mathtt{SK}_\mathtt{s})$. We require $\mathcal{PK} \subseteq \mathcal{R}$ and $\mathtt{PK}_\mathtt{s} \in \mathcal{PK}$.

3) $\mathcal{A}$ is given $\mathtt{SK}_1, \mathtt{SK}_2, \ldots$; $\mathcal{A}$ outputs a message $\mathtt{m}$, distinct indices $\mathtt{s}_o, \mathtt{s}_1$, and a ring $\mathcal{P}K$ for $\mathtt{PK}_{\mathtt{s}_0}, \mathtt{PK}_{\mathtt{s}_1} \in \mathcal{P}K$. Furthermore, $\mathcal{A}$ is given $\sigma \leftarrow \mathtt{RSig}(\mathtt{m}, \mathcal{P}K; \mathtt{SK}_{\mathtt{s}_b})$.
4) $\mathcal{A}$ outputs a bit b' and succeeds if $b' = b$.

Definition 2 (Anonymity Against Full Key Exposure): A ring signature scheme is unconditionally anonymous if the success probability of $\mathcal{A}$ in the above *anonymity game* is negligibly close to 1/2.

Remark 1: This is a weak definition for anonymity except that full key exposure is required. Indeed, this model does not consider such attack that the adversary would generate public keys in arbitrary manner (i.e., possibly depending on the public keys of the honest users). Therefore, Bender *et al.* [37] defined a stronger model, and they considered the adversarially chosen key attack, in which the adversary must know the actual signer. However, our scheme does not need to depend on such a stronger model since we require that the adversary should be unable to prove to a third party about the actual signer even though it knows someone. On the other hand, we require the unconditional anonymity w.r.t. full key exposure such that the transcript can be simulated by anyone to reach the full deniability.

Unforgeability: The intuitive notion of unforgeability is that a forger should be unable to output $(\mathcal{P}K, \mathtt{m}, \sigma)$ such that $\mathtt{RVer}(\sigma, \mathtt{m}, \mathcal{P}K) = 1$, where the corresponding signing keys in $\mathcal{P}K$ are unknown to the forger. Formally, we consider the unforgeability game as follows.

Given a ring signature scheme $(\mathtt{KGen}, \mathtt{RSig}, \mathtt{RVer})$ and a forger $\mathcal{F}$, the *unforgeability game* is working as follows.

1) Generate $(\mathtt{PK}_\mathtt{i}, \mathtt{SK}_\mathtt{i}) \leftarrow \mathtt{KGen}(1^\kappa)$ for $\mathtt{i} = 1, 2, \ldots$, $\mathcal{F}$ is given $\mathcal{R} = \{\mathtt{PK}_1, \mathtt{PK}_2, \ldots\}$.
2) $\mathcal{F}$ is given access to a signing oracle $\mathtt{Osign}(s, \mathtt{m}, \mathcal{P}K)$, which returns $\mathtt{RSig}(\mathtt{m}, \mathcal{P}K; \mathtt{SK}_\mathtt{s})$. We require $\mathcal{P}K \subseteq \mathcal{R}$ and $\mathtt{PK}_s \in \mathcal{P}K$.
3) $\mathcal{F}$ outputs $(\mathcal{P}K^*, \mathtt{m}^*, \sigma^*)$ and succeeds if $\mathcal{P}K^* \subseteq \mathcal{R}$, $\mathtt{RVer}(\sigma^*, \mathtt{m}^*, \mathcal{P}K^*) = 1$, and $\mathcal{F}$ never queried $\mathtt{Osign}(\cdot, \mathtt{m}^*, \mathcal{P}K^*)$.

Definition 3 (Unforgeability): A ring signature scheme is unforgeable if the success probability of $\mathcal{F}$ in the above *unforgeability game* is negligible.

IV. Edge Computing Model and Its Security Goals

A. Edge Computing System Overview

The centralization of resources in cloud computing increases the average network latency and jitter. In contrast, the edge computing immigrates the tasks from the central cloud to the distributed edge equipment to provide convenience for the local IoT devices [38]. As shown in Fig. 2, the edge equipment is deployed close to IoT devices. The location of the edge equipment is public and fixed; the communication record between the IoT device and the edge equipment implies the IoT device location. Therefore, the location privacy of IoT devices should be considered in edge computing.

B. Security Requirement

During the access procedure, there are two aspects that should be concerned.

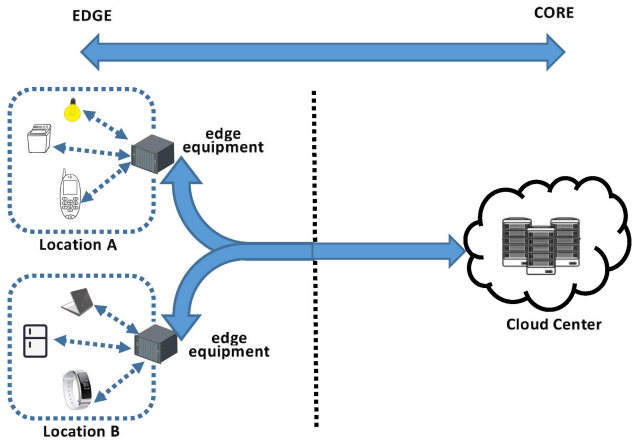

Fig. 2. Illustration of edge computing system.

1) Authentication: Authentication is necessary during the communication between IoT devices and the edge equipment, which includes identity authentication and message authentication. When the IoT devices connect to the edge equipment, the identities of IoT devices must be confirmed. When the communication occurs between the two entities, the message integrity should also be considered. Clearly, password-based authentication suffers insecurity even though it is efficient and practical, and key-based authentication avoids nonrandomness of the passwords and provides stronger security. In such kind of authentication, the user should prove its knowledge about the public key or the shared secret.

2) Location Privacy Leakage: As shown in Fig. 2, the edge equipment is close to IoT devices. In addition, the edge equipment is fixed and public; its location implies the location of end devices. Therefore, it leaks the client location inherently since the authentication transcript and the connection record are the evidence to validate the fact of IoT device involvement.

Therefore, a secure communication scheme in edge computing with location awareness should meet the following security requirements.

a) *Authentication:* The edge equipment authenticates the IoT device to identify the client and to ensure the message integrity. Formally, a forger $\mathcal{F}$ can query the authentication transcripts for its adaptive chosen messages $\mathtt{m}_1, \mathtt{m}_2, \ldots$ from its challenger. Finally, $\mathcal{F}$ forges an accepted authentication on $(\mathtt{m}^*, \mathtt{PK}_\mathtt{i})$ without knowing the secret of $\mathtt{PK}_\mathtt{i}$. The success probability of $\mathcal{F}$ in the authentication game is denoted by $\Pr[\mathtt{Succ}_{\mathcal{F}}^{\mathtt{auth}}]$. We require that *authentication* is satisfied if $\Pr[\mathtt{Succ}_{\mathcal{F}}^{\mathtt{auth}}]$ is negligible.
b) *Location privacy:* The client location privacy is preserved in the authentication when it accesses to the fixed edge equipment. It seems paradoxical and challenging. A feasible way is to make the authentication transcript simulatable. In other words, we require that a distinguisher $\mathcal{D}$'s views in a real conversation transcript $\Gamma^{\mathtt{rea}}$ and a simulated $\Gamma^{\mathtt{sim}}$ are indistinguishable. Therefore, the real client can deny that it communicated with the edge equipment before as the conversation transcript may be simulated by others. Thus, there is no evidence to show IoT device location.

The sender denoted as $\mathtt{P}$ authenticates a message $\mathtt{m}$ to the receiver denoted as $\mathtt{V}$. Let $(\mathtt{SK_P}, \mathtt{PK_P})$ denote the private/public key pair for $\mathtt{P}$ and $(\mathtt{RSig}(\cdot), \mathtt{RVer}(\cdot))$ denote the ring signature scheme.

Round 1. $\mathtt{V} \rightarrow \mathtt{P}$: $\mathtt{V}$ randomly chooses a value $\mathtt{PK}$ and sends $\mathtt{PK}$ to $\mathtt{P}$.

Round 2. $\mathtt{P} \rightarrow \mathtt{V}$: Upon receiving $\mathtt{PK}$, $\mathtt{P}$ generates a 2-user ring signature σ on $\mathtt{m}$, that is $\sigma = \mathtt{RSig}(\mathtt{m}, (\mathtt{PK_P}, \mathtt{PK}); \mathtt{SK_P})$ and sends σ to $\mathtt{V}$.

Finally, $\mathtt{V}$ accepts $\mathtt{P}$'s authentication if σ is a valid ring signature w.r.t. $(\mathtt{m}, \mathtt{PK_P}, \mathtt{PK})$. That is $\mathtt{RVer}(\sigma, \mathtt{m}, \mathtt{PK_P}, \mathtt{PK}) = 1$.

Fig. 3. Our DA protocol.

V. Privacy-Preserving Authentication Protocol Against Location Leakage

We present a privacy-preserving authentication protocol with full deniability against location leakage for edge computing environment in this section. The authentication transcript leaks the IoT device location, while it is connecting to the fixed edge equipment. Therefore, we adopt the *full deniability* to make it confident for IoT devices to deny the fact of communication records. This kind of authentication does not expose the locations of IoT devices even if the edge equipment accepts IoT devices. We observe that the verifier in this scenario can be assumed honest, and thus, we can simplify and optimize this fully DA protocol with two rounds to adapt to the IoT. Besides, the concurrent communication must be considered for Internet-based applications. Under this setting, the interaction executions in the fully DA protocol can be arbitrarily interleaved by the attacker. Thus, the deniability may fail with rewinding steps. Therefore, our construction is without rewinding steps to reach concurrent deniability. Moreover, we avoid the CCA paradigm for constructing authentication. Therefore, it is practical and suitable for the Internet environment. In this section, we first introduce our generic construction of the underlying DA protocol, and then, we instantiate this DA with a concrete two-member ring signature scheme to implement a privacy-preserving authentication protocol for edge computing against client location leakage.

A. DA Protocol

Most DAs are constructed by CCA2-secure encryptions, as shown in Fig. 1. The underlying building block is impractical. It is more significant to construct efficient protocols based on primitives with looser requirements. Moreover, the deniability in CCA-paradigm DAs is proven to be black-box simulatable and, hence, has to add the challenge–response subprotocol with the secret revocation. It incurs rewinding steps in the simulation. Therefore, the deniability property in CCA-paradigm DA holds only if copies of the protocol are performed sequentially. It is impractical in the Internet-based service, which is under the concurrent environment. The Stinson–Wu scheme [27] does not rely on any signatures or encryptions but only to realize identity authentication. Recently, Zeng *et al.* [39] have made use of projective hash functions to construct an authentication protocol with deniability. In this section, we adopt another building block to avoid CCA-paradigm encryption.

We propose an authentication with full deniability. Different with the traditional approaches (i.e., CCA paradigm) to reach fully DA, as shown in Fig. 1, we construct it by employing the ring signature with two members. Our communication round is only 2, which is the optimal round in the fully DA, and it reaches the concurrent deniability. Indeed, the simulation in our protocol does not require the rewinding steps and is, therefore, perfect, although there exist adversaries who may schedule the executions or delay messages in arbitrary ways. While most interactive DAs involve rewinding steps to be black-box simulatable, the timing assumption is necessary to handle the concurrency problem. Our two-round DA is shown in Fig. 3.

Remark 2: It would be noticed that the underlying ring signature is not used directly to provide privacy. Instead, we adopt the "challenge–response" paradigm to construct the authentication protocol with full deniability based on a ring signature algorithm. As we know, ring signature provides signer anonymity noninteractively. However, it reaches partial deniability since the transcript of the signature can be simulated by the group of members only. In order to realize full deniability, our inspiration is that one is the sender $\mathtt{P}$'s real public key $\mathtt{PK_P}$, and the other is a logic "public key" $\mathtt{PK}$, which is a random value challenged by the receiver. The sender responses it by generating a ring signature σ with $\mathtt{m}$ and the two-size ring $\mathcal{PK} = \{\mathtt{PK_P}, \mathtt{PK}\}$. That is, $\sigma \leftarrow \mathtt{RSig}(\mathtt{m}, \mathcal{PK}; \mathtt{SK_P})$. The corresponding private key of the logic public key $\mathtt{PK}$ is only known to the receiver. Thus, a valid ring signature implies that the receiver is assured that $\mathtt{m}$ originated from the sender $\mathtt{P}$. The authentication is achieved. On the other hand, the *full* deniability is realized since the authentication tag σ can be simulated by anyone. Indeed, the simulator (without secret) randomly chooses a value r to simulate the logic public key R, which has the same distribution with $\mathtt{PK}$. Note that $\mathtt{PK}$ is just a random value chosen by the receiver $\mathtt{V}$ (not its pubic key) if $\mathtt{V}$ performs the protocol honestly. Therefore, the simulated ring signature $\sigma_{\mathtt{sim}} = \mathtt{RSig}(\mathtt{m}, (\mathtt{PK_P}, R); r)$ produced by the "private key" r is indistinguishable from σ due to the unconditional anonymity property of ring signature (see Section III-B). Therefore, the full deniability is achieved without rewinding steps, and it can hold in concurrent setting also.

We briefly analyze the authentication and full deniability of our generic two-round DA, as shown in Fig. 3. The formal proof will be elaborated in the next section.

Our generic two-round DA shown in Fig. 3 satisfies the authentication property of the DA protocol. Actually, an adversary $\mathcal{A}$ violates this property if it forges a ring signature σ, which passes the verification algorithm $\mathtt{RVer}(\cdot)$. Note that the ring signature σ is generated by $\mathtt{SK_P}$ or the secret of $\mathtt{PK}$ if the ring signature algorithm is sound. Obviously, $\mathtt{SK_P}$ and the secret of $\mathtt{PK}$ are not known to $\mathcal{A}$. Therefore, our DA protocol meets authentication if the underlying ring signature algorithm is unforgeable.

Our generic two-round DA shown in Fig. 3 satisfies the full deniability property of the DA protocol. This property follows the unconditional anonymity of the underlying ring signature algorithm. Due to the unconditional anonymity of the ring signature scheme $(\mathtt{RSig}(\cdot), \mathtt{RVer}(\cdot))$, the ring signature σ generated by $\mathtt{SK_P}$ has the indistinguishable distribution to that generated by the secret of $\mathtt{PK}$. Since $\mathtt{PK}$ is a random value chosen by the honest verifier $\mathtt{V}$, anyone can pick a random value to generate the same distributed $\mathtt{PK}'$. Obviously, this ring signature σ' produced by the secret of $\mathtt{PK}'$ is valid and has the same distribution as σ. In other words, anyone can simulate an indistinguishable conversation transcript. The full deniability follows.

B. Application to Edge Computing Against Location Leakage

We instantiate our DA described above with a concrete two-user ring signature scheme and implement it on the edge computing environment to preserve client location privacy.

1) Setup: The edge computing system runs this algorithm to publish the parameters $\mathtt{Para}$ as follows. Choose a safe prime q; let $\mathbb{G}$ and $\mathbb{G}_1$ be two multiplicative cyclic groups of order q that are associated with an efficiently computable bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$. g is the generator of $\mathbb{G}$. Choose a collision-free hash function $\mathtt{H} : \{0,1\}^* \to \mathbb{G}$. $\mathtt{Para} = (q, \mathbb{G}, \mathbb{G}_1, \hat{e}, g, \mathtt{H})$.

2) KeyGen: The client $\mathtt{U_i}$ (e.g., IoT device) runs this algorithm to generate its keypair $(\mathtt{PK_i}, \mathtt{SK_i})$ as follows: Choose $x_i \leftarrow \mathbb{Z}_q$ and compute $y_i = g^{x_i}$. Set $\mathtt{SK_i} = x_i$ and $\mathtt{PK_i} = y_i$. The public key $\mathtt{PK_i}$ of $\mathtt{U_i}$ is authenticated by the certificate system.

3) Access Authentication: $\mathtt{U_P}$ submits the connection request to the nearest edge equipment, say EE, with its certificate $\mathtt{Cert_P}$, which includes $\mathtt{PK_P}$. If $\mathtt{Cert_P}$ is valid, EE starts this authentication as follows.

1) EE $\to \mathtt{U_P}$: EE randomly chooses a value $h \leftarrow \mathbb{G}$ and sends h to $\mathtt{U_P}$.
2) $\mathtt{U_P} \to$ EE: Upon receiving h, $\mathtt{U_P}$ generates a two-user ring signature σ as follows.
   a) Choose $r \leftarrow \mathbb{Z}_q$.
   b) Compute $\mathtt{H}(\mathtt{m})$.
      i) If this is an identity authentication, $\mathtt{m} = \mathtt{ID_P} \| \mathtt{PK_P}$, where $\mathtt{ID_P}$ is the identity of $\mathtt{U_P}$.
      ii) If this is a message authentication, $\mathtt{m}$ is the message delivered from $\mathtt{U_P}$ to EE.
      iii) Output $\sigma = \left(h^{x_\mathtt{P}} \cdot \mathtt{H}(\mathtt{m})^r, g^r\right)$. σ is the ring signature w.r.t. $(\mathtt{m}, \{\mathtt{PK_P}, h\})$. $\mathtt{U_P}$ sends σ to EE to complete its authentication.

Finally, EE accepts $\mathtt{U_P}$'s authentication if $\sigma = (A, B)$ is a valid ring signature w.r.t. $(\mathtt{m}, \{\mathtt{PK_P}, h\})$. That is to check whether $\hat{e}(y_\mathtt{P}, h) \cdot \hat{e}(B, \mathtt{H}(\mathtt{m})) \stackrel{?}{=} \hat{e}(A, g)$.

VI. Security Analysis and Performance Evaluation

In this section, we analyze the security and performance of our protocol. Since the verification of *Correctness* of our protocol is straightforward, in what follows, we will prove that our protocol meets other two properties, i.e., *Authentication* and *Location Privacy*, which have been presented in security model. Then, we provide the performance evaluation for our instantiation and the comparisons of the underlying DA to the related constructions regarding to computational cost.

A. Security Analysis

We focus on the security of the instantiation for our DA protocol. As presented in the security model in Section IV, this privacy-preserving authentication protocol should concern *Authentication* and *Full Deniability* if it is applied to be against location leakage in the edge computing environment.

1) Authentication: The communication between the clients (IoT devices) and the server (edge equipment) should concern the identity authentication and message authentication. This authentication is provided by the soundness (unforgeability) of the underlying DA protocol. We apply the two-user ring signature scheme to preserve the authentication. Indeed, the generated ring signature σ is bounded to two public keys $\mathtt{PK_P}$ and h. Due to the unforgeability of the ring signature, only the member who knows the secret of $\mathtt{PK_P}$ or h can generate a valid signature. The receiver (i.e., EE) is assured that σ originated from the sender $\mathtt{U_P}$ (who knows the secret of $\mathtt{PK_P}$) since h's secret is unknown to anyone. Intuitively, our protocol meets authentication due to the unforgeability of the underlying ring signature scheme. Theorem 1 formally proves this property.

Theorem 1: Our protocol described in Section V-B satisfies authentication if the computational Diffie–Hellman (CDH) assumption holds and the hash function $\mathtt{H}$ is a random oracle.

Proof: Suppose $\mathcal{A}$ is the adversary against the soundness of our protocol presented in Section V-B. We construct $\mathcal{A}'$ to break the unforgeability of the underlying two-user ring signature scheme. $\mathcal{C}$ is the challenger of $\mathcal{A}'$ whose goal is to solve the CDH problem. $\mathcal{C}$ controls the random oracle. Given a CDH problem instance (g, g^a, g^b) over the pairing group $(\mathbb{G}, \mathbb{G}_1, g, q, \hat{e})$, $\mathcal{C}$ runs $\mathcal{A}$ and $\mathcal{A}'$ as follows.

$\mathcal{C}$ sets the sender public key as $\mathtt{PK_P} = g^a$. When $\mathcal{A}$ queries authentication to arbitrary messages $\mathtt{m}_1, \mathtt{m}_2, \ldots$ adaptively, $\mathcal{A}'$ acts as sender $\mathtt{P}$ and $\mathcal{A}$ acts as receiver $\mathtt{V}$ by given g^b. $\mathcal{A}'$ performs the authentication to $\mathcal{A}$ as follows.

When $\mathtt{m_i}$ is queried by $\mathcal{A}$ by sending $h = g^b$ to $\mathcal{A}'$, according to our protocol, $\mathcal{A}'$ makes hash query $\mathtt{H}$-query $\mathtt{H}(\mathtt{m_i})$ to $\mathcal{C}$. Note that, before any hash queries are made, $\mathcal{C}$ chooses $i^* \in [1, q_H]$, where q_H is the number of hash queries. If $\mathtt{m_i}$ is already in $\mathcal{C}$'s hash list (which is empty at the beginning), $\mathcal{C}$ responds following its hash list. Otherwise, $\mathcal{C}$ chooses $w_i \leftarrow \mathbb{Z}_q$ randomly and sets $\mathtt{H}(\mathtt{m_i}) = g^{w_i}$ if $i = i^*$ and sets $\mathtt{H}(\mathtt{m_i}) = g^{b+w_i}$ if $i \neq i^*$. Then, $\mathcal{A}'$ makes ring signature queries to $\mathcal{C}$ on $\mathtt{m_i}$. If $i = i^*$, $\mathcal{C}$ aborts this query. Otherwise, $\mathcal{C}$ chooses $r'_i \leftarrow \mathbb{Z}_q$ randomly and returns $\sigma = \left((g^a)^{-w_i}\mathtt{H}(\mathtt{m_i})^{r'_i}, (g^a)^{-1} g^{r'_i}\right)$ to $\mathcal{A}'$. Finally, $\mathcal{A}'$ responds σ to $\mathcal{A}$ to complete its authentication to $\mathtt{m_i}$. Obviously, the simulation of $\mathcal{A}'$ is perfect and $\mathcal{A}$ accepts $\mathcal{A}'$'s authentication since the returned $\sigma = (A, B)$ satisfies the verification $\hat{e}(y_\mathtt{P}, h) \cdot \hat{e}(B, \mathtt{H}(\mathtt{m})) = \hat{e}(A, g)$, where $\mathtt{H}(\mathtt{m}) = g^{b+w_i}$.

$\mathcal{A}$ pretends to $\mathtt{P}$ to make fake authentication to $\mathtt{m}^*$ after its authentication queries to $\mathtt{m}_1, \mathtt{m}_2, \ldots$. Obviously, $\mathcal{A}$ succeeds if and only if its production $\sigma_{\mathtt{m}^*} = (A^*, B^*)$ satisfies the verification equation $\hat{e}(y_\mathtt{P}, h) \cdot \hat{e}(B^*, \mathtt{H}(\mathtt{m}^*)) = \hat{e}(A^*, g)$. It helps $\mathcal{A}'$ to break the unforgeability of the underlying ring signature undoubtedly.

If m^* is the i^*th queried message in the hash list, it helps $\mathcal{C}$ to solve the CDH problem indeed. In this case, $\mathtt{H}(\mathtt{m}^*) = g^{w_{i^*}}$ and $(A^*, B^*) = \left(g^{ab}(g^{w_{i^*}})^r, g^r\right)$. Therefore, $\mathcal{C}$ obtains g^{ab} by $A^*/(B^*)^{w_{i^*}}$.

Therefore, we have that if $\mathcal{A}$ breaks the authentication property of our protocol with probability ε after making q_H queries to the random oracle, $\mathcal{C}$ solves the CDH problem with ε/q_H. ■

2) Location Privacy: In the edge computing environment, the location of edge equipment reveals client location during the connection and communication. Our protocol makes use of "deniability" to handle this problem. If the IoT devices can deny their involvement in this authentication, there is no evidence for its connection. The location privacy is preserved naturally. Thus, the deniability of our protocol indicates location privacy of IoT devices.

Following the security model of the DA protocol described in Section III, we use *simulation* fashion to prove the deniability of our protocol. If a simulator (run by anyone) can simulate the authentication transcript without participant's secret, the full deniability is satisfied. The formal proof is presented as follows.

Theorem 2: Our protocol described in Section V-B satisfies the *full deniability* if the receiver follows our protocol honestly.

Proof: For the underlying ring signature algorithm, we argue that it is unconditionally anonymous against full key exposure. Indeed, the underlying ring signature algorithm outputs the signature $\sigma = (A, B) = (h^{x_{\mathtt{P}}}\mathtt{H}(\mathtt{m})^r, g^r)$, which can be rewritten as $(y_{\mathtt{P}}^{\omega}\mathtt{H}(\mathtt{m})^r, g^r)$ where $\omega = \log_g h$.

Note that the value $h \in \mathbb{G}$ is randomly chosen by verifier $\mathtt{V}$ (EE) in our protocol. Therefore, we require $\mathtt{V}$ honestly to return a random value from $\mathbb{G}$ in the first flow. In the simulation, the simulator $\mathcal{S}$ chooses $\bar{\omega} \leftarrow \mathbb{Z}_q$ randomly to simulate h, i.e., $\bar{h} = g^{\bar{\omega}}$. Obviously, $\bar{h}$ has the same distribution as h and the simulated h is perfect. With the secret $\bar{\omega}$, the simulator $\mathcal{S}$ generates $\bar{\sigma} = (\bar{A}, \bar{B}) = (y_{\mathtt{P}}^{\bar{\omega}}\mathtt{H}(\mathtt{m})^{\bar{r}}, g^{\bar{r}})$. Obviously, $\bar{\sigma}$ is "identical" to σ as $\hat{e}(y_{\mathtt{P}}, \bar{h}) \cdot \hat{e}(\bar{B}, \mathtt{H}(\mathtt{m})) = \hat{e}(\bar{A}, g)$ holds.

Clearly, this simulated transcript $(\bar{h}, \bar{\sigma})$ (produced by anyone) is indistinguishable from the real one. Therefore, the actual sender $\mathtt{U}_{\mathtt{P}}$ can fully deny its involvement as this authentication transcript for connection to EE may be "fabricated" by anyone and the location privacy is preserved. ■

B. Performance Evaluation

We make use of the DA protocol to preserve authentication and privacy while IoT devices accessing and communicating with the edge equipment. The performance of the underlying DA protocol mainly affects the efficiency of our protocol in Section V-B. Therefore, we analyze the performance of this article from two sides. We first analyze our underlying DA protocol theoretically and give the performance comparisons among related constructions; then, we implement our protocol on the specific edge computing environment to show its efficiency.

1) Efficiency of Underlying DA Protocol: Our underlying DA protocol, as described in Fig. 3, employs the two-user ring signature algorithm and challenge–response phase to realize authentication and full deniability. With this design and under the assumption of the honest verifier, our DA protocol is only two rounds, which is the optimal communication round in the fully DA protocols. Besides that, our DA protocol realizes concurrent deniability even. Since we do not require "rewinding" steps to simulate the authentication transcript, the copies of the protocol are not necessarily performed sequentially. Therefore, our DA protocol with both optimal round and concurrent deniability can be applied to Internet-based service practically.

There are some other related DA protocols to be compared in this qualitative research. Dwork's scheme [22] is constructed by encryptions, and the underlying encryption algorithm is required to be CCA2-secure. Their work requires four rounds to realize full deniability, and the deniability does not hold in concurrent setting. From the authentication type point of view, this work supports both message authentication and identity authentication. Jiang's scheme [28] relies on public random oracle to realize three-round mutual authentication (and two rounds if one-way authentication). The communication transcript is simulated without rewinding steps; thus, it realizes concurrent deniability. Yao *et al.*'s work [29] depends on nonmalleable zero-knowledge proofs; thus, the underlying communication round is heavy. The communication round of their scheme is 2+ means that the round of one-way authentication is 2, whereas its non-malleable zero-knowledge (NMZK) may incur extra communication round. The Stinson–Wu scheme [27] depends on the KEA to realize a two-round full deniable identification protocol. It does not rely on any underlying signatures or encryptions. However, KEA is not the standard assumption. The above three works reach identity authentication only. Li *et al.*'s protocols [35] are one round, which seems communication optimal. However, it achieves partial deniability only. In order to show these protocols clearly, we conclude their features in Table I, and the communication round is in one-way authentication fashion.

2) Efficiency of Our Instantiation: Qualitatively, Table I reports that our scheme has superior properties in both communication and security. Our communication round is optimal for the full deniability; therefore, we have lower latency undoubtedly. In this subsection, we consider the computation performance quantitatively in the specific edge computing environment. We run the related protocols and compare their computational cost under the uniform environment. Since literature works [27]–[29] are identity authentications only and Dwork's scheme [22] is a generic construction, we choose the efficient noninteractive DA protocols (HDA-1 and HDA-2) from [35] as the comparison objects. Our experiments show the computation performance of these protocols.

The end devices equipped with a processor of Intel(R) Pentium(R) CPU G4500 3.50 GHz and RAM of 4.00 GB are used to simulate the IoT devices. We choose 80-bit level to reimplement their protocols, and we choose Type A pairing from free C library PBC following their implementation. Fig. 4 reports the experimental results.

We run our protocols, HDA-1 and HDA-2, in [35] 20 times to get 60 records totally. The average cost is also calculated, and we make three lines of every 21 records from each protocol. And under the three lines, we compute 42 records of difference cost; difference between HDA-1 and our protocol is yellow bar, and difference between HDA-2 and our protocol is blue

TABLE I
COMPARISONS OF DA PROTOCOLS

Scheme	Deniability	Round	Concurrency	pRO	Assumption	CCA-paradigm	Authentication Type
Dwork's scheme [22]	Full	4	×	-	Standard	Yes	Message & Identity
Jiang's scheme [28]	Full	2	✓	✓	Standard	No	Identity
Yao's scheme [29]	Full	2+	✓	-	Standard	No	Identity
Stinson-Wu scheme [27]	Full	2	✓	-	KEA	No	Identity
Li's scheme [36]	Partial	1	✓	-	Standard	No	Message & Identity
Our scheme	Full	2	✓	-	Standard	No	Message & Identity

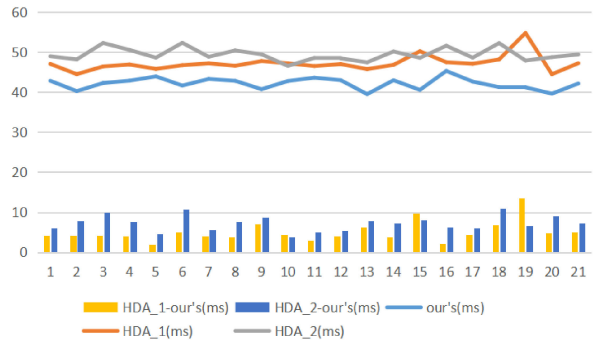

Fig. 4. Experimental time cost.

TABLE II
EXPERIMENTAL RESULT ANALYSIS

Protocol	Level	Cost	Difference	Rate
Ours	80-bit	42.15335ms	-	-
HDA-1	80-bit	47.2193ms	5.06595	10.728%
HDA-2	80-bit	49.41545ms	7.2621	14.696%

bar. These bars graphically illustrate the cost saving between different protocols.

Table II shows our experimental result with the average cost. We find that our protocol saves 10.728% cost compared with HDA-1 and 14.696% cost compared to HDA-2.

VII. CONCLUSION

Authentication in the edge computing environment incurs location leakage; we propose a privacy-preserving authentication scheme with full deniability to protect the locations of IoT devices. Our underlying protocol, including only two communication rounds, achieves the optimal communication latency for the full deniability. Our scheme does not rely on CCA-paradigm encryptions, rewinding steps, and any strong number-theoretic assumptions; thus, it is practical in the concurrent Internet-based environment. Compared to the existing efficient DAs, our scheme has better performance for end devices in terms of computational cost. Therefore, it adapts to the resource-constrained IoT devices. Besides, we note that our approach can be extended to mobile edge computing. It is our future work to investigate this topic.

ACKNOWLEDGMENT

This article reflects only the authors' view. The European Union Commission is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] J. Ren, D. Zhang, S. He, Y. Zhang, and T. Li, "A survey on end-edge-cloud orchestrated network computing paradigms," *ACM Comput. Surv.*, vol. 52, no. 6, 2019, Art. no. 125.
[2] Y. Ren *et al.*, "Data query mechanism based on hash computing power of blockchain in Internet of Things," *Sensors*, vol. 20, 2020, Art. no. 207.
[3] H. Wu, F. Lyu, C. Zhou, J. Chen, and X. Shen, "Optimal UAV caching and trajectory in aerial-assisted vehicular networks: A learning-based approach," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 12, pp. 2783–2797, Dec. 2020.
[4] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Secur. Privacy*, 2011, pp. 247–262.
[5] X. He, R. Jin, and H. Dai, "Leveraging spatial diversity for privacy-aware location-based services in mobile networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 6, pp. 1524–1534, Jun. 2018.
[6] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 100–114, May 2019.
[7] C. Ma, Z. Yan, and C. W. Chen, "SSPA-LBS: Scalable and social-friendly privacy-aware location-based services," *IEEE Trans. Multimedia*, vol. 21, no. 8, pp. 2146–2156, Aug. 2019.
[8] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.
[9] C.-Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments," *GeoInformatica*, vol. 15, no. 2, pp. 351–380, 2011.
[10] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proc. Annu. Conf. Pervasive Comput. Commun. Workshops*, 2004, pp. 127–131.
[11] B. Palanisamy and L. Liu, "Effective mix-zone anonymization techniques for mobile travelers," *Geoinformatica*, vol. 18, no. 1, pp. 135–164, 2014.
[12] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.
[13] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial k-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Gener. Comput. Syst.*, vol. 94, pp. 40–50, 2019.
[14] T. Shu, Y. Chen, and J. Yang, "Protecting multi-lateral localization privacy in pervasive environments," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1688–1701, Oct. 2015.
[15] S. Li, H. Li, and L. Sun, "Privacy-preserving crowdsourced site survey in WiFi fingerprint-based localization," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, 2016, Art. no. 123.
[16] Z. Yang and K. Järvinen, "The death and rebirth of privacy-preserving WiFi fingerprint localization with Paillier encryption," in *Proc. IEEE Conf. Comput. Commun.*, 2018, pp. 1223–1231.
[17] J. Han, H. Wang, Z. Zheng, and Q. Xu, "Privacy preserved wireless sensor location protocols based on mobile edge computing," *Comput. Secur.*, vol. 84, pp. 393–401, 2019.
[18] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 901–914.
[19] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private naive Bayes learning over multiple data sources," *Inf. Sci.*, vol. 444, pp. 89–104, 2018.
[20] Y. Qian, Y. Jiang, M. S. Hossain, L. Hu, M. Ghulam, and S. U. Amin, "Privacy-preserving based task allocation with mobile edge clouds," *Inf. Sci.*, vol. 507, pp. 288–297, 2020.
[21] P. Yang, F. Lyu, W. Wu, N. Zhang, L. Yu, and X. Shen, "Edge coordinated query configuration for low-latency and accurate video analytics," *IEEE Trans. Ind. Inform.*, vol. 16, no. 7, pp. 4855–4864, Jul. 2020.

[22] C. Dwork, M. Naor, and A. Sahai, "Concurrent zero-knowledge," *J. ACM*, vol. 51, no. 6, pp. 851–898, 2004.
[23] S. Zeng, Y. Chen, S. Tan, and M. He, "Concurrently deniable ring authentication and its application to LBS in VANETs," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 844–856, 2017.
[24] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography," *Soc. Ind. Automobile Manuf. Rev.*, vol. 45, no. 4, pp. 727–784, 2003.
[25] M. D. Raimondo and R. Gennaro, "New approaches for deniable authentication," *J. Cryptol.*, vol. 22, no. 4, pp. 572–615, 2009.
[26] M. Bellare and A. Palacio, "Towards plaintext-aware public-key encryption without random oracles," in *Proc. Int. Conf. Theory. Appl. Cryptol. Inf. Secur.*, 2004, pp. 48–62.
[27] D. R. Stinson and J. Wu, "An efficient and secure two-flow zero-knowledge identification protocol," *J. Math. Cryptol.*, vol. 1, no. 2007, pp. 201–220, 2007.
[28] S. Jiang and R. Safavi-Naini, "An efficient deniable key exchange protocol (extended abstract)," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2008, pp. 47–52.
[29] A. C.-C. Yao and Y. Zhao, "Privacy-preserving authenticated key-exchange over internet," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 1, pp. 125–140, Jan. 2014.
[30] H. Tian, X. Chen, and W. Susilo, "Deniability and forward secrecy of one-round authenticated key exchange," *J. Supercomput.*, vol. 67, no. 3, pp. 671–690, 2014.
[31] S. Jiang, "Timed encryption with application to deniable key exchange," *Theor. Comput. Sci.*, vol. 560, pp. 172–189, 2014.
[32] S. Zeng and Y. Chen, "Concurrently deniable group key agreement and its application to privacy-preserving VANETs," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art. no. 6870742.
[33] L. Harn and J. Ren, "Design of fully deniable authentication service for e-mail applications," *IEEE Commun. Lett.*, vol. 12, no. 3, pp. 219–221, Mar. 2008.
[34] F. Li, D. Zhong, and T. Takagi, "Efficient deniably authenticated encryption and its application to e-mail," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2477–2486, Nov. 2016.
[35] F. Li, J. Hong, and A. A. Omala, "Practical deniable authentication for pervasive computing environments," *Wireless Netw.*, vol. 24, no. 1, pp. 139–149, 2018.
[36] S. Zeng, Y. Mu, M. He, and Y. Chen, "New approach for privacy-aware location-based service communications," *Wireless Pers. Commun.*, vol. 101, no. 2, pp. 1057–1073, 2018.
[37] A. Bender, J. Katz, and R. Morselli, "Ring signatures: Stronger definitions, and constructions without random oracles," *J. Cryptol.*, vol. 22, no. 1, pp. 114–138, 2009.
[38] F. Lyu *et al.*, "LEAD: Large-scale edge cache deployment based on spatio-temporal WiFi traffic statistics," *IEEE Trans. Mobile Comput.,* to be published doi: 10.1109/TMC.2020.2984261,.
[39] S. Zeng, Y. Mu, H. Zhang, and M. He, "A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy," *Inf. Sci.*, vol. 516, pp. 331–345, 2020.

Shengke Zeng received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2013.

She is currently a Professor with the School of Computer and Software Engineering, Xihua University, Chengdu. Her research interests include cryptography and network security.

Hongjie Zhang received the B.E. degree in computer science and technology in 2018 from Xihua University, Chengdu, China, where she is currently working toward the master's degree with the School of Computer and Software Engineering.

Her research interests include data security and searchable encryption.

Fei Hao received the Ph.D. degree in computer science and engineering from Soonchunhyang University, Asan, South Korea, in 2016.

Since 2016, he has been with Shaanxi Normal University, Xi'an, China, where he is currently an Associate Professor. He is currently taking a Marie Sklodowska-Curie Individual Fellowship at the University of Exeter, Exeter, U.K. His research interests include social computing, ubiquitous computing, big data analysis and processing, and mobile cloud computing.

Hongwei Li (Senior Member, IEEE) received the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2008.

He is currently a Professor with the School of Computer Science and Engineering, UESTC. He is the sole author of a book entitled *Enabling Secure and Privacy Preserving Communications in Smart Grids* (Springer, 2014). His research interests include network security and applied cryptography.

Dr. Li is the Distinguished Lecturer of the IEEE Vehicular Technology Society.