A Lightweight and Privacy-Preserving Answer Collection Scheme for Mobile Crowdsourcing

Yingling Dai[1], Jian Weng[1*], Anjia Yang[1], Shui Yu[2] and Robert H. Deng[3]
[1] College of Information Science and Technology and the College of Cyber Security, Jinan University
Guangzhou 510632, China
[e-mail: daiyingling@foxmail.com, cryptjweng@gmail.com, anjiayang@gmail.com]
[2] University of Technology Sydney, Ultimo, Australia
[e-mail: Shui.Yu@uts.edu.au]
[3] School of Information System, Singapore Management
University, Singapore 178902
[e-mail: robertdeng@smu.edu.sg]
*Corresponding author: Jian Weng

Received August 21, 2020; revised February 9, 2021; accepted July 5, 2021;
published August 31, 2021

Abstract

Mobile Crowdsourcing (MCS) has become an emerging paradigm evolved from crowdsourcing by employing advanced features of mobile devices such as smartphones to perform more complicated, especially spatial tasks. One of the key procedures in MCS is to collect answers from mobile users (workers), which may face several security issues. First, authentication is required to ensure that answers are from authorized workers. In addition, MCS tasks are usually location-dependent, so the collected answers could disclose workers' location privacy, which may discourage workers to participate in the tasks. Finally, the overhead occurred by authentication and privacy protection should be minimized since mobile devices are resource-constrained. Considering all the above concerns, in this paper, we propose a lightweight and privacy-preserving answer collection scheme for MCS. In the proposed scheme, we achieve anonymous authentication based on traceable ring signature, which provides authentication, anonymity, as well as traceability by enabling malicious workers tracing. In order to balance user location privacy and data availability, we propose a new concept named current location privacy, which means the location of the worker cannot be disclosed to anyone until a specified time. Since the leakage of current location will

Jian Weng was partially supported by the National Key Research and Development Plan of China under Grant Nos. 2020YFB1005600, National Natural Science Foundation of China (Grant Nos. 61825203, U1736203, 61732021), Major Program of Guangdong Basic and Applied Research Project under Grant No. 2019B030302008, and Guangdong Provincial Science and Technology Project under Grant No. 2017B010111005. Anjia Yang was partially supported by Key-Area Research and Development Program of Guangdong Province (Grant No. 2020B0101360001), National Natural Science Foundation of China (Grant No. 62072215, 61702222, 61877029).

seriously threaten workers' personal safety, causing such as absence or presence disclosure attacks, it is necessary to pay attention to the current location privacy of workers in MCS. We encrypt the collected answers based on timed-release encryption, ensuring the secure transmission and high availability of data, as well as preserving the current location privacy of workers. Finally, we analyze the security and performance of the proposed scheme. The experimental results show that the computation costs of a worker depend on the number of ring signature members, which indicates the flexibility for a worker to choose an appropriate size of the group under considerations of privacy and efficiency.

Keywords: Mobile crowdsourcing, answer collection, authentication, privacy preserving, timed-release encryption, traceable ring signature

1. Introduction

In recent years, crowdsourcing [1] has emerged as a new paradigm to assign online tasks. It provides a distributed and cost-effective way to complete tasks by employing an undefined set of people, rather than assigning a task to specified employees. With the popularity and widespread use of mobile devices, such as mobile phones, tablets, smart watches and various wearable devices, etc., mobile crowdsourcing (MCS) becomes a new paradigm of crowdsourcing, and has attracted great attention from academia and industry recently [2]. Different from the conventional crowdsourcing, MCS can be utilized to complete spatial tasks due to the portability and wide distribution of mobile devices, such as environment monitoring [3], news reporting [4], traffic information collection [5], etc.

In MCS, there are usually three types of entities: requesters, workers and a mobile crowdsourcing server (MCS server). A requester submits a task with some specific information (e.g., time, location, and requirements) to the MCS server. Then a single or a group of mobile users are employed as workers to complete the task by collecting answers using their mobile devices. Finally, the requester obtains the task result from answers uploaded by the employed workers.

However, several security and privacy concerns that threaten the employed workers arise. With the openness of the network, any mobile user is allowed to participate in the MCS activities and upload data. As a result, malicious mobile users may upload invalid data which is meaningless or even fake, reducing data availability, and as well as the quality of MCS service. Therefore, authentication is necessary to check whether the mobile user is an authorized worker in the MCS task. Real-name identity authentication is one of the most effective ways to authenticate the user's validity. However, it raises serious identity privacy issues since privacy is significantly concerned by users nowadays. Furthermore, workers often need to move to a particular location to perform tasks, which makes the collected answers location-dependent. The location-dependent information would reveal workers' location privacy, resulting in the leakage of their current or historical locations. When associated with other publicly available information, historical location could be exploited to infer workers' private information, such as personal preferences, habits, behaviors and beliefs.

Even worse, the exposure of current location would cause absence or presence disclosure attacks. For example, when a person is known to be away from home, malicious attackers may commit burglary, bringing property losses to the homeowner. Moreover, when a malicious attacker knows that someone is in a particular location at the moment, he may follow that person for blackmail or personal attacks. Both attacks threaten personal interests, or even physical safety. Thus, there is a strong need for the preserving of current location privacy. Since privacy, including identity privacy and location privacy, is of great concern to users, only when they are assured of their privacy, can we expect them to participate in MCS. However, the accuracy of data is very important in some MCS applications. For example, governments who want to realize information management and maintenance of public infrastructures may ask citizens to collect and report issues about public infrastructures, including damaged guard rails, broken street lights, damaged street name plates, and pavement obstruction [6]. In this way, the government may have a more comprehensive and timely understanding of the use situation. In order to investigate the issue later, the time, location and detailed description about the issue need to be reported as accurately as possible in the issue report. Therefore, in the case of high data availability, a solution with location privacy protection is required. Since accurate location would reveal users' location privacy, a balance should be struck between location privacy and data availability.

Ring signature algorithm is a digital signature scheme, first proposed by Rivest et al. [7] in 2001. In this signature scheme, the signer can randomly select multiple ring members to form a group to complete the signature. The verifier can only verify that the signature comes from the group, but does not know who signed the signature, providing complete anonymity. However, under complete anonymity mechanism, it will cause an abuse of anonymity, resulting in an unattainability of non-repudiation. The variant traceable ring signature enables traceability on malicious signers, which is more practical for real scenarios. In this paper, we focus on the data availability and privacy concerns of answer collection in MCS. Towards the balance between location privacy and data availability, we propose a new concept named current location privacy, which means the location of the worker cannot be disclosed to anyone until a specified time. Timed-release encryption enables encrypting messages into the future. That is, the encrypted data can only be decrypted until the pre-set time has come.

With the above considerations, we first study the user authentication to ensure all collected answers are from authorized workers. We aim at achieving anonymous authentication, and as well providing malicious workers tracing when the answer is found untrustworthy. Then, we preserve the accuracy of location-related data while maximizing the protection of location privacy by considering merely the current location privacy. Our main contributions are summarized as follows.

- We design a lightweight and privacy-preserving answer collection scheme for MCS. The scheme realizes anonymous authentication based on certificate-less traceable ring signature (CL-TRS), achieving both user authentication and identity privacy preserving, and as well restricting the arbitrary signer tracing by the key generator center (KGC). The scheme enables the accuracy preservation of location-dependent data to ensure the availability of collected answers. Meanwhile, it preserves the worker's current location privacy based on timed-release encryption (TRE).
- We give a comprehensive security analysis and performance evaluation of the proposed scheme. The results indicate that lightweight operations are realized for resource-constrained mobile devices due to no pairing operations involved at the workers side. Although the computation cost of signing is related to the number of ring

signature members, workers can choose an appropriate size depending on the power of their devices.

The rest of this paper is organized as follows. In Section 2, we review previous related works about authentication and privacy preserving. Then in Section 3, we introduce cryptographic preliminaries that are relevant to our proposed scheme. In Section 4 we describe the system model, threat model and design goals. We present the proposed scheme in detail in Section 5, and in Section 6, we analyze the security and performance issues. Last, in Section 7 we make a conclusion of the paper.

2. Related Work

We focus on authentication and privacy-preserving answer collection in MCS. As mentioned above, mobile users care about both identity privacy and location privacy. Therefore, in this section, we review previous works on anonymous authentication, location privacy preserving, and some other related works.

2.1 Anonymous Authentication

There have been existing works considering authentication with privacy preserving of users [8-22]. Anonymous authentication is proposed to provide authentication on users while preserving their identity privacy, such as pseudonyms based approaches [9-12] and signature based approaches [13-22, 40].

Pseudonyms based approaches were proposed to achieve anonymous authentication by replacing the user's real identity with a pseudonym. A trusted authority (TA) is required to perform pseudonyms management, verification and revocation. To ensure untraceability, the pseudonyms need to be updated constantly, resulting in costly communication and computation overhead between users and TA. Rabieh et al. [11] proposed to use long-term shared keys to generate one-time pseudonyms, and thus users can perform pseudonyms updating locally. However, it implies a strong assumption of such a fully trusted third party. Ejaz et al. [12] proposed to generate pseudonyms by multiple certificate authorities, thus it is impossible for a single authority to link a pseudonym to the real identity. However, to obtain short time communication pseudonyms (SPCs) for communication requires frequent interaction with the pseudonym provider, which is not desirable for mobile devices with limited computing resource in MCS.

Special signature schemes such as group signature and ring signature are utilized to achieve anonymous authentication, which provides anonymity, non-repudiation as well as traceability. Shao et al. [13] proposed a group signature based anonymous authentication scheme. In this scheme, the user is allowed to sign messages on behalf of a group, which means the signature can be identified as generated by one member of the group, while the signer's identity remains unknown. Xu et al. [14] proposed a RFID batch authentication RFID protocol based on group signature. Due to the existence of the group manager, the identity of malicious signer can be revealed, thus achieving traceability and conditional anonymity, which is more practical for controlled privacy preserving scenarios. Yue et al. [15] proposed a revocable group signatures scheme. In this scheme, the authority can also revoke the membership of a user. However, the group is established and managed by the group manager. When the group changes, such as joining a new member or revoking a group member, it requires interactions between group members and the group manager, which will cause costly communication overhead.

Ring signature is a special kind of group signature that has only ring members and no group managers [16]. That is, the signer to create a group dynamically without consent of other group members. Furthermore, the identity of the signer cannot be known to anyone except the signer, providing more flexibility and complete anonymity. Kugusheva et al. [17] proposed an electronic collective voting system based on ring signature, which not only ensures the reliability of data, but also protects the privacy of group members. Mundhe et al. [18] proposed a ring signature-based authentication scheme and applied it to vehicular ad-hoc networks (VANETs). Aiming at the bottleneck that the existing PKI system cannot support a large number of users and their data, [19, 20] adopted the identity-based ring signature technology to protect the anonymity of users in the process of data sharing. Liu et al. [21] proposed an identity-based ring signature scheme for VANETs. However, complete anonymity is not always appealing in practice. That is, malicious users may send untrustworthy data. Even with a signature on the data, they can deny the misbehavior and escape from being identified. The variant traceable ring signature (TRS) provides anonymous authentication as well as traceability. Specifically, TRS enables tracing identity of the irresponsible signer, and thus ensuring non-repudiation. With such promising properties, TRS is more practical for applications with controlled anonymity. A few TRS schemes have been proposed [23-31]. Chang et al. [30] proposed a traceable and anonymous authentication scheme for wireless sensor network, but the tracking process requires interaction with each ring member. Most of the above schemes are designed based on public key cryptography and identity-based cryptography, leading to costly management of public keys or private key escrow issues. Gu et al. [31] proposed a certificate-less based TRS scheme, which avoids the problems mentioned above. Nevertheless, the signing process in [31] involves the time-consuming bilinear pairing operation. In addition, the signer tracing can be performed by KGC individually, leading to a leakage threat of identity privacy when KGC is compromised. Therefore, it cannot be directly applied to lightweight and anonymous authentication in MCS.

In this paper, traceable ring signature is adopted to achieve anonymous identity authentication. The signer can randomly select ring members to generate their own signatures. On the one hand, signers can be verified as authorized users, while protecting their identity privacy. On the other hand, malicious signers will be traced and revealed if necessary. In addition, the scheme is designed under certificate-less mechanism, and the signer does not need to perform bilinear pairing operation.

2.2 Location Privacy Preserving

There are many schemes proposed to preserve location privacy [32-42]. According to the employed techniques, the approaches used for location privacy preserving can mainly be classified as spatial cloaking, perturbation, and cryptographic encryption.

Spatial cloaking based approaches [32-35] aim to generalize locations by reducing their spatial granularity or hiding them under a set of virtual locations. Gruteser et al. [36] first introduced *k*-anonymity to location privacy preserving by hiding the location among a cloaked region with a group of *k* different users. The user's location is then indistinguishable from that of other *k*-1 users, ensuring the probability of group members being identified individually is less than 1/*k*. But the drawback of spatial cloaking based approaches is that location privacy may be under attack of background knowledge [37].

In order to avoid this issue, the perturbation based differential privacy (DP) approach is introduced to location privacy preserving [37-39]. The intuitive idea behind DP is that a single change in input should not have a non-negligible effect on the output, ensuring that an

adversary cannot learn from the sanitized data whether a particular individual is present in the original data or not, even with prior knowledge. A typical way to generate perturbation is adding controlled random noise drawn from a standard probability distribution to the raw data. In this way, the user's location is obfuscated to be preserved. To et al. [38] adopted DP in spatial crowdsourcing and proposed a framework for task assignment, achieving location privacy guarantee to workers. Wang et al. [39] proposed a method by combining DP and *k*-anonymity, which overcomes the drawback of traditional *k*-anonymous and provides better security in location privacy preserving.

Both spatial cloaking and perturbation based approaches assume that location data can be obfuscated or perturbed. Although effectively protecting location privacy, the lack of consideration on data accuracy causes a degrade of data availability. Therefore, they are not suitable for scenarios with high accuracy requirements; otherwise, it affects the availability of data.

Schemes employing cryptographic encryption technique [41-44] were proposed to protect location privacy by treating location as normal data. With the property of reversible transformation, cryptographic encryption based approaches provide both privacy preserving and accuracy guarantee of data. Shen et al. [41] proposed a location privacy preserving protocol based on additive homomorphic encryption by introducing a semi-honest third party which is more practical for real-world applications. Zhou et al. [45] proposed to protect participants' location privacy from passive monitoring and inference attacks, while maintaining the accuracy of data recovery. Peng et al. [46] proposed a multidimensional privacy preservation (MPP) scheme that provides full protection for user privacy without any need for a trusted third party (TTP). However, in the above scheme, once the ciphertext is obtained, it can be decrypted and the plaintext recovered, revealing the exact location. If that location is the user's current location, he will be in danger. Therefore, a balance needs to be struck between location privacy and data availability. In this paper we pay attention to protect the current location of the user by utilizing timed-release encryption to encrypt the current location data.

2.3 Timed-Release Encryption

The notion of TRE was first proposed by May [47] in 1993 and further discussed by Rivest et al. [7]. The target of TRE is to encrypt messages into the future, so that they can only be decrypted until the pre-set time has come. TRE has been applied to many real-world applications, such as electronic auctions, regular payments, sealed bid auctions and lotteries. Generally speaking, security is enhanced when introducing TRE into the cryptography problem, since the decryption process first needs to remove time layer encryption, which is equivalent to the method of encapsulating private keys of the scheme. One approach to realize TRE is employing a trusted authority (TA) to periodically release time tokens related to the current time, which is called TA-based TRE. Earlier TA-based TRE schemes [7, 47]adopted a model in which interactions were needed between users and TA. Chan and Blake proposed a non-interactive TRE scheme [48]. Since then, many TA-based TRE schemes were proposed [49-55] under the model of [48], but most of them were constructed based on bilinear pairing, which will cause heavy computation cost for mobile users. Recently, some efforts try to model the time by capturing "real-world-time". Liu et al. [56] utilized a blockchain-based computing model to simulate real time, eliminating the role of a time server.

In MCS, energy consumption is one of the key factors affecting the willingness of users with resource-constrained mobile devices to participate in crowdsourcing tasks using. Therefore, there is an urgent need to reduce the cost of computing. In this paper, we propose a TA-based TRE scheme for mobile users which does not require bilinear pairing operation.

3. Preliminaries

In this section, we introduce preliminaries about cryptography that are related to our proposed scheme.

3.1 Bilinear Pairing

Let G_1 be a cyclic additive group of prime order and G_2 be a cyclic multiplicative group of the same order. We call e a bilinear pairing if $e: G_1 \times G_1 \to G_2$ is a map with the following properties:

1) Bilinearity: $e(aP,bQ) = e(P,Q)^{ab}$ for all $P,Q \in G_1$ and for all $a,b \in Z$.
2) Non-degeneracy: there exist $P,Q \in G_1$ such that $e(P,Q) \neq 1$.
3) Computability: there is an efficient algorithm to compute $e(P,Q)$ for all $P,Q \in G_1$.

3.2 Complexity Assumption

Discrete Logarithm (DLP) Assumption. Given $P,Q \in G_1$, the DLP assumption in G_1 is that no probabilistic polynomial-time (PPT) algorithm A can compute $x \in Z$ such that $Q = xP$ with non-negligible advantage.

3.3 Certificateless Public Key Cryptography

Certificateless public key cryptography (CL-PKC) was proposed by Al-Riyami and Paterson [57] to remove the certificates and overcome the key escrow issue inherent in identity-based PKC. In CL-PKC, certificates are not necessary any more to guarantee the authenticity of public keys. Meanwhile, the private key is not fully generated by KGC. Specifically, KGC first uses the master secret key along with an identity to generate a partial private key for the user. And then the user randomly chooses a secret value. The user's public key and private key are set by combining the partial private key and the secret chosen by the user.

3.4 Traceable Ring Signature

Traceable ring signature (TRS) is a variant of ring signature. Ring signature allows a signer to sign a message on behalf of a group of members chosen by himself, called a "ring". A verifier can check the validity of the signature, but cannot know the identity of the signer, which ensures complete anonymity. However, anonymity is not always good. TRS was proposed to restrict abusing anonymity; namely TRS provides restricted anonymity and traceability. Specifically, when an irresponsible or dishonest signer abuses anonymity, the anonymity can be revoked and his identity is revealed.

4. System Model

In this section, we first introduce the notations used in the proposed scheme, as shown in **Table 1**, and then define the system model, threat model, and design goals.

Table 1. Definitions of notations

Notations	Descriptions
ID_u	the identity of a participant
psk_u	the partial key of a participant
pk_u	the public key of a participant
sk_u	the private key of a participant
m	the collected answers
CT	the ciphertext of the collected answers
$T = \{t_1 t_2 \cdots t_n\} \in \{0,1\}^n$	the specified decryption time
tk_T	the time token corresponding to time T
d	the randomness to be signed
$L = \{ID_1, ID_2, \cdots, ID_l\}$	a list of workers' identities
$PK = \{pk_1, pk_2, \cdots, pk_l\}$	a list of workers' public keys
σ	the signature

4.1 System Model

As shown in **Fig. 1**, the proposed MCS system consists of four entities, namely requesters, workers, an MCS server, and a time server.

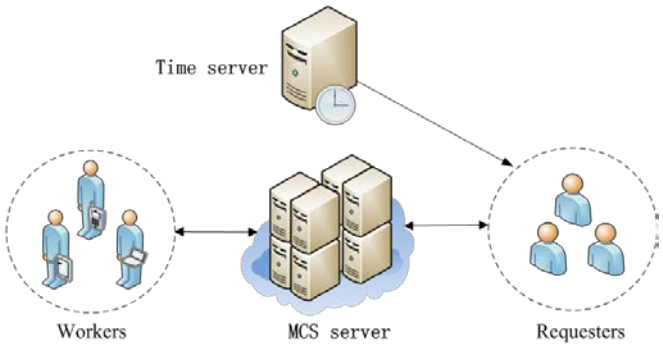


Fig. 1. System model of the proposed MCS

Requesters: Requesters may be individuals or businesses. They can make various kinds of task requests to the MCS server, and receive corresponding task results. For further use of the result, requesters hope to receive collected answers with high availability.

Workers: Workers are a group of people who perform tasks using mobile devices in the system. They first apply tasks from the MCS server then collect answers about the task with their carrying mobile devices (e.g., mobile phones, tablets and smart swatches). Workers care a lot about their privacy, including identity privacy and location privacy. Therefore, they will take measures to protect their privacy on the premise of collecting answers that meet the task requirements. Moreover, since mobile devices are resource-constrained, the

operations are supposed to be lightweight.

MCS server: MCS server acts as a mediator in the system who interacts with both requesters and workers. It offers a platform for requesters to submit task requests, and assigns MCS tasks to workers. In order to improve the quality of MCS service, the MCS server performs user authentication to ensure that only answers collected by authorized workers are accepted.

Time server (TS): TS plays as a trusted third party in the system, who will not interact with any other entity, but periodically releases time tokens at each time. Only with the corresponding time token, can requesters decrypt the ciphertext encrypted under that time.

To better explain how the system works, we show the interactions between requesters, the MCS server and workers in **Fig. 2**. Firstly, all participants including requesters and workers should register with the MCS server to get keys. Then requesters can make task requests to the MCS server. After receiving the requests, the MCS server releases them on the task list. Workers can then apply tasks from the MCS server. Since task allocation is not the consideration of this paper, we will not describe it in detail. Then the selected workers begin to complete the task by collecting answers. After that, workers encrypt the collected answers under the requester's public key and a specified decryption time, and return the ciphertext along with a signature to the MCS server. The MCS server performs verification on the signature. Only when the signature passes the verification, will the encrypted data be accepted and delivered to requesters. Requesters decrypt the ciphertext with their private keys and time tokens released by TS, and finally obtain the task results.

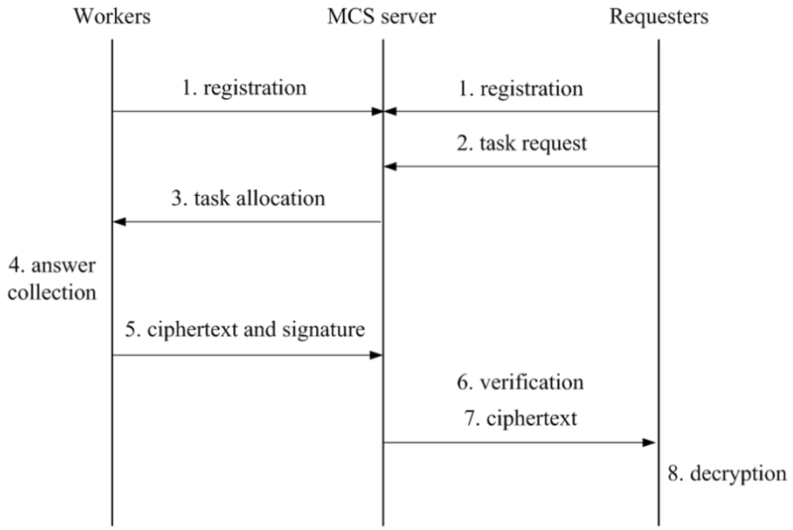


Fig. 2. The interactions between workers, MCS server and requesters

4.2 Threat Model

In the above system model, we treat TS as a fully trusted third entity who releases time tokes honestly and periodically. The MCS server is considered as semi-trusted (i.e., honest-but-curious), who will correctly perform requested operations, but has curiosity in workers' privacy. We assume that the MCS server will not collude with any other entity in the system. Additionally, there exist malicious workers in the system. We discuss the threats in detail as following.

- **Untrustworthiness of the collected answers.** Due to the openness of the MCS, any mobile user has an opportunity to participate in the MCS task and upload data to the MCS server. Some mobile users may behave maliciously in consideration of their own interests. For example, an unauthorized mobile user or a selfish authorized worker will randomly produce meaningless data as answers and return them to the MCS server. The untrustworthy answers will reduce the availability of data, resulting in an effect on the quality of service.
- **Identity privacy issue of workers.** In MCS tasks, the answers collected by workers usually can be used to infer additional information about them. For example, when a task is about collecting data near a specific hospital, the workers may be conjectured to have some health problems. If the identity is also revealed, it will not only embarrass them but also lead to an invasion of their privacy.
- **Location privacy issue in location-dependent data.** In MCS, the collected answers are usually location-dependent, which will reveal workers' location privacy. Curious MCS server or attackers may attempt to obtain workers' location for various malicious reasons. When a period of time's historical location is revealed, workers' activity trajectory is spied on. Even worse, when highly accurate location-related data is required, their current location is exposed, threatening interests and physical safety, such as being stalked or extorted.

4.3 Design Goals

To achieve both secure and privacy-preserving answer collection in MCS, our proposed scheme should realize the following goals.

- **Authentication with conditional identity privacy.** The proposed scheme should provide authentication with conditional identity privacy. This means the MCS server can check whether the mobile user is an authorized worker, but has no idea about his identity. In this way, all answers can be guaranteed to be from authorized workers. In order to prevent authorized workers from uploading untrustworthy answers, the proposed scheme should provide signer tracing to disclose malicious workers' identities. Furthermore, the tracing process should not be performed by the semi-trusted MCS server arbitrarily.
- **Highly accurate location-related data with current location privacy.** The proposed scheme should ensure high availability of data, which means the accuracy of location-related collected answers is not compromised. In addition, the collected answers are supposed to be encrypted to secure the transmission in the open channel and preserve the current location privacy of the workers. Protecting the current location privacy of the worker means that while the worker is still there, the location cannot be revealed to anyone, even if the requester decrypts the ciphertext using his private key.
- **Lightweight operations for workers.** Considering the limited computing resources of mobile devices, the proposed scheme should not involve time-consuming operations such as bilinear pairing on the workers side.

5. Design

In this section, we first introduce the overview of the proposed scheme and then give the detailed description.

5.1 Overview

The proposed scheme provides anonymous authentication based on TRS, which allows a worker to randomly select a set of other authorized workers to form a group, and then sign messages on behalf of that group. In this way, the MCS server can check whether the answers are from one member of the group, but with the identity remaining unknown. When the answers are found untrustworthy, the traceability property of TRS enables the signer tracing, resulting in the identity disclosure of the malicious worker. Moreover, the signer tracing is designed to designate a tracing performer. That is, only with the designator's consent, can someone perform the signer tracing, achieving restricted traceability.

With respect to the location privacy issue in location-dependent data, the generalization or perturbation based approaches reduce data accuracy, and thus are undesirable to scenarios that require high availability of collected answers. Though ensuring the availability of answers, cryptographic encryption based approaches disclose the location information once decryption process is performed. Therefore, we make a tradeoff between location privacy and data availability by considering merely the current location privacy of workers. Specifically, assuming a worker is collecting answers in location *LA* at time *T*1, the data associated with that location is not exposed when the worker is in *LA*. After the worker's location is updated to *LB*, the historical location *LA* can be revealed to the requester, avoiding threats like being stalked. One naive idea to preserve the current location is that the worker manually delays sending the collected answers after leaving *LA*, which works but will lead to an unfriendly user experience. We propose to delay the release of data based on TRE, ensuring that the ciphertext cannot be decrypted before the specified decryption time. Specifically, the worker first specifies a decryption time, and then encrypts the collected answers under both the requester's public key and the specified time. With a properly specified decryption time *T*2 (*T*2>*T*1) which is sufficient for workers to safely leave their current location, the current location privacy is guaranteed. When the decryption time *T*2 comes, TS releases the corresponding time token, with which the requester can decrypt the ciphertext and recover the collected answers with high availability.

5.2 Concrete Design

In this section, we give a detailed description of the proposed scheme. Suppose that an MCS scheme consists of 4 phases: Initialization, Registration, Answer Collection and Answer Processing.

- **Initialization.** The system initialization includes two steps. Firstly, the MCS server runs the setup algorithm to generate system parameters for the following phases. The MCS server takes as input the security parameter k and integers n, ρ, generates a prime q, two groups G_1, G_2 of order q, two elements $P,Q \in G_1$, and a bilinear map $e: G_1 \times G_1 \to G_2$. The algorithm then randomly selects a secret key $s \in Z_q^*$, and sets $h = sP$, $h' = sQ$. In addition, hash functions are chosen as follows: $H_1 : \{0,1\}^n \times \{0,1\}^\rho \to Z_q^*$, $H_2 : G_2 \to \{0,1\}^{n+\rho}$, $H_3 : \{0,1\}^* \to Z_q^*$, $H_4 : \{0,1\}^* \times G_1 \to Z_q^*$. The system parameters are defined as $params = (q, G_1, G_2, e, P, Q, h, h', H_1, H_2, H_3, H_4)$ and published. The master secret key $msk = s$ is privately kept by the MCS server. Secondly, TS generates its public/private keys using system parameters. TS selects private key $pri = \{a, r_1, r_2, \cdots, r_n\}$, where

$a, r_i \in Z_q^*$ for $i \in \{1, \cdots, n\}$, then computes $pub = \{r_1 P, r_2 P, \cdots, r_n P\}$ and $\alpha = e(P,Q)^a$, and then publishes them as public keys. Briefly, we denote all the public parameters as $pps = (q, G_1, G_2, e, P, Q, h, h', H_1, H_2, H_3, H_4, pub, \alpha)$.

- **Registration.** Any participant including requesters and workers who wants to join in the MCS should register to the MCS server. In the phase of registration, registered participants get public/private keys. Since the proposed scheme is designed under CL-PKC, keys are produced by both participants and the MCS server. Specifically, when a participant with identity ID_u comes for registration, the MCS server first chooses a random d_u, and then computes $Y_u = d_u P$, $Q_u = H_4(ID_u, Y_u)$, $y_u = d_u + sQ_u$, finally returns the partial key $psk_u = (y_u, Y_u)$ to the participant through a secure channel. After receiving the partial key, the participant first checks whether the equation $Y_u + H_4(ID_u, Y_u)h = y_u P$ holds to verify the validity of the partial key. With a valid partial key, the participant then randomly selects a secret value x_u and computes $X_u = x_u P$. He finally sets the public key as $pk_u = (X_u, Y_u)$, and the private key as $sk_u = (x_u, y_u)$. The specific description of the registration phase is shown in **Fig. 3**.

MCS server
Input: ID_u
Output: $psk_u = (y_u, Y_u)$
(1) Randomly choose d_u;
(2) Compute $Y_u = d_u P$, $Q_u = H_4(ID_u, Y_u)$, $y_u = d_u + sQ_u$;
Return psk_u

Workers/Requesters
Input: ID_u, $psk_u = (y_u, Y_u)$
Output: $pk_u = (X_u, Y_u)$, $sk_u = (x_u, y_u)$
(1) Check $Y_u + H_4(ID_u, Y_u)h \stackrel{?}{=} y_u P$;
(2) Randomly choose x_u;
(3) Compute $X_u = x_u P$;
Return (pk_u, sk_u)

Fig. 3. Algorithm of registration

- **Answer Collection.** In this phase, assuming that a worker with identity ID_w has been assigned an MCS task and received the specification about the task from the MCS server. The task specification includes at least the task descriptions, the requester's public key pk_r, and a randomness d. After finishing collecting the required answers denoted as m, the worker performs encryption operations on m which is location-related. Firstly, he specifies the decryption time $T = (t_1, t_2, \cdots, t_n)$, and then encrypts m under the requester's public key pk_r and the specified time T. The worker randomly chooses $\omega \in \{0,1\}^\rho$, and then computes $r = H_1(m \| \omega)$, $R = r\sum_{i=1}^{n} t_i$, $\beta = \alpha^R$, $c_1 = rxP$, $c_2 = r\sum_{i=1}^{n} t_i r_i P$, and $c_3 = H_2(\beta) \oplus (m \| \omega)$. Finally, the algorithm

returns the ciphertext $CT=(T,c_1,c_2,c_3)$. The specific description of the encryption algorithm is shown in **Fig. 4**. Furthermore, in order to provide proof of the validity of identity, the worker generates a signature on randomness d contained in the task specification based on TRS. He first chooses other $(l-1)$ authorized workers and forms a group with l members. Let $L=(ID_1,ID_2,\cdots,ID_l)$ be the list of l members' identities, and $PK=(pk_1,pk_2,\cdots,pk_l)$ be the corresponding public keys. For $i\in(1,2,\cdots,l)\backslash\{w\}$, the worker randomly chooses a_i, and then computes $U_i=a_iP$, $h_i=H_3(U_i,d,L)$, $Q_i=H_4(ID_i,Y_i)$. For $i=w$, he computes $U_w=rh-\sum_{i\neq w}^{l}(h_i(X_i+Y_i+Q_ih)+U_i)$, $h_w=H_3(U_w,d,L)$, $V=h_w(x_w+y_w)Q+rh'$. The signature is set as $\sigma=(L,U_1,U_2,\cdots,U_l,V)$. The specific operations of the signing algorithm are described in **Fig. 5**. Finally, the worker uploads the ciphertext CT along with a signature σ as task results to the MCS server.

Worker ID_w
Input: m, $pk_r=(xP,xQ)$, $T=\{t_1t_2...t_n\}$
Output: $CT=(T,c_1,c_2,c_3)$
(1) Randomly choose $\omega\in\{0,1\}^{\rho}$;
(2) Compute $r=H_1(m\|\omega)$, $R=r\sum_{i=1}^{n}t_i$, $\beta=\alpha^R$,
$c_1=rxP$, $c_2=r\cdot\Sigma_{i=1}^{n}t_i\cdot r_iP$, $c_3=H_2(\beta)\oplus(m\|\omega)$;
Return CT

Fig. 4. Algorithm of encryption

Worker ID_w
Input: r, d, $L=\{ID_1,ID_2,....,ID_l\}$, $PK=\{pk_1,pk_2,....,pk_l\}$
Output: $\sigma=(L,U_1,U_2,....,U_l,V)$
(1) For $i\in\{1,2,....,l\}\backslash\{w\}$, randomly choose a_i;
(2) Compute $U_i=a_iP$, $h_i=H_3(U_i,d,L)$,
$Q_i=H_4(ID_i,Y_i)$;
(3) Compute $U_w=rh-\sum_{i\neq w}^{l}(h_i(X_i+Y_i+Q_ih)+U_i)$,
$h_w=H_3(U_w,d,L)$, $V=h_w(x_w+y_w)Q+rh'$;
Return σ

Fig. 5. Algorithm of signing

- **Answer Processing.** After receiving the task results from the worker, the MCS server first authenticates the worker by verifying the signature to check whether it is generated by one member of the claimed group L, whose members are all authorized workers. For $i\in\{1,2,\cdots,l\}$, the MCS server computes $h_i=H_3(U_i,d,L)$ and $Q_i=H_4(ID_i,Y_i)$. If $e(V,P)=e(\sum_{i=1}^{l}(h_i(X_i+Y_i+Q_ih)+U_i),Q)$ holds, the signature passes the verification and the task results are accepted; otherwise, they are discarded. The correctness can be verified as following.

$$\begin{aligned}
&e(\sum_{i=1}^{l}(h_i(X_i+Y_i+Q_ih)+U_i),Q)\\
&=e(\sum_{i\neq w}^{l}(h_i(X_i+Y_i+Q_ih)+U_i)+h_w(X_w+Y_w+Q_wh)+U_w,Q)\\
&=e(h_w(X_w+Y_w+Q_wh)+rh,Q)\\
&=e((h_w(x_w+y_w)+rs)Q,P)\\
&=e(V,P)
\end{aligned}\tag{1}$$

Next, the MCS server delivers the valid ciphertext $CT=(T,c_1,c_2,c_3)$ to the requester. Since the plaintext is encrypted under both specified decryption time T and requester's public key, the requester should obtain the time token tk_T corresponding to time T before performing decryption. Periodically, TS releases time tokens as following: given the time

$T = \{t_1 t_2 \cdots t_n\} \in \{0,1\}^n$, TS randomly selects $t \in Z_q^*$ and computes the time token $tk_T = (d_1, d_2) = (a + t + \sum_{i=1}^{n} t_i r_i, tQ)$, where $a, r_i \in pri$. Therefore, the requester cannot obtain the corresponding time token tk_T until time T. Once tk_T is obtained, the requester can decrypt the ciphertext using his private key $sk_r = x$. He first computes $A = e(c_1, d_1 Q - d_2)$, $B = e(c_2, Q)$, $\beta' = \frac{A^{x^{-1}}}{B}$, $R' = \sum_{i=1}^{n} t_i$, $(m' \| \omega') = H_2(\beta'^{R'}) \oplus c_3$. If $H_1(m' \| \omega') xP = c_1$, the requester obtains answers $m = m'$. The specific description of the encryption is shown in **Fig. 6**. The correctness can be verified as following.

$$
\begin{aligned}
(m' \| \omega') &= H_2(\beta'^{\sum_{i=1}^{n} t_i}) \oplus c_3 \\
&= H_2((\frac{A^{x^{-1}}}{B})^{\sum_{i=1}^{n} t_i}) \oplus c_3 \\
&= H_2(\frac{e(rP, (a + \sum_{i=1}^{n} t_i r_i) Q)}{e(r \sum_{i=1}^{n} t_i r_i P, Q)}^{\sum_{i=1}^{n} t_i}) \oplus c_3 \\
&= H_2(e(rP, aQ)^{\sum_{i=1}^{n} t_i}) \oplus c_3 \\
&= H_2(\alpha^{r \sum_{i=1}^{n} t_i}) \oplus c_3 \\
&= H_2(\beta) \oplus c_3 \\
&= (m \| \omega)
\end{aligned}
\tag{2}
$$

Requester ID_r
Input: $sk_r = x$, $tk_T = (d_1, d_2)$, $CT = (T, c_1, c_2, c_3)$
Output: m or "$\perp$"
(1) Compute $A = e(c_1, d_1 Q - d_2)$, $B = e(c_2, Q)$,
$\beta' = \frac{A^{x^{-1}}}{B}$, $R' = \sum_{i=1}^{n} t_i$, $(m' \| \omega') = H_2(\beta'^{R'}) \oplus c_3$;
(2) Compare $H_1(m' \| \omega') xP \stackrel{?}{=} c_1$;
Return $m = m'$ or "$\perp$"

Fig. 6. Algorithm of decryption

The proposed scheme also provides malicious workers tracing performed by the MCS server and requesters. If the answers m are found untrustworthy, the requester can ask the MCS server for help to trace the malicious worker who uploaded the answers. Firstly, he computes $D = e(x^{-1} c_1, h) = e(rP, h)$ from the ciphertext and sends D to the MCS server. On receiving the signer tracing request and D, the MCS server then computes

$U=\sum_{i=1}^{l} h_i(X_i+Y_i+Q_ih)+U_i$. For $u \in \{1,2,\cdots,l\}$, the MCS server compares $De(P,h_u(X_u+Y_u+Q_uh))=e(P,U)$. If index u satisfies the formula, pk_u denotes the public key of the signer, and thus, the malicious worker is identified. The correctness can be verified as following.

$$\begin{aligned} e(P,U) &= e(P,\sum_{i=1}^{l} h_i(X_i+Y_i+Q_ih)+U_i) \\ &= e(P,rh+h_u(X_u+Y_u+Q_uh)) \\ &= e(P,rh)e(P,h_u(X_u+Y_u+Q_uh)) \\ &= e(P,rh)e(P,h_u(X_u+Y_u+Q_uh)) \\ &= De(P,h_u(X_u+Y_u+Q_uh)) \end{aligned} \tag{3}$$

6. Security and Performance Analysis

In this section, we present analyses on security and performance of the proposed scheme.

6.1 Security and Performance Analysis

In the following, we analyze the design goals defined in Section 4.3, which are authentication with conditional identity privacy preserving, privacy preserving of the current location and lightweight operations for workers.

- **Authentication with conditional identity privacy preserving.** The authentication is performed based on TRS. Specifically, to generate a ring signature on the message d contained in the task specification, the worker selects other $(l-1)$ authorized workers to form a group. With the anonymity property of TRS, any external attacker who is not in the group has probability less than $1/l$ in identifying the actual signer. Take the ring signature $\sigma=(L,U_1,U_2,\cdots,U_l,V)$ as an example. L is the set of group members' identities, and $\{U_i=a_iP\}(i \in \{1,2,\cdots,l\}\backslash\{w\})$ are computed by randomly chosen a_i . Both $U_w=rh-\sum_{i\neq w}^{l}(h_i(X_i+Y_i+Q_ih)+U_i)$ and $V=h_w(x_w+y_w)Q+rh'$ are randomized by r . That is, the ring signature σ is uniformly distributed and does not reveal any identity information about the actual signer. Therefore, the signature can be verified as generated by one member of the group, but the identity remains unknown or can be identified with probability less than $1/l$ by external attackers. The only way to identify the actual signer is by checking whether $e(P,U)=De(P,h_w(X_w+Y_w+Q_wh))$ holds or not, where D is generated by the requester. When the collected answers are found untrustworthy, the requester can ask the MCS server to perform the tracing process to identify the malicious worker. Therefore, the identity privacy of the actual signer is conditionally preserved. In addition, $D=e(x^{-1}c_1,h)$ can only be computed by the requester's private key $sk_r=x$. Namely, without consent of the requester, the MCS server cannot perform the signer tracing arbitrarily, ensuring the security of the tracing process.

- **Privacy preserving of the current location.** Under the secure transmission mechanism, the collected answers are encrypted with the requester's public key and a specified decryption time. For answers m, they are encrypted in $c_3 = H_2(\beta) \oplus (m \| \omega)$, in which $\beta = e(P,Q)^{ar\sum_{i=1}^{n} t_i}$ is related to r, a and the specified time T. Under the assumption of DLP, someone is hard to learn the randomness r from c_1 or c_2. Similarly, the privately kept a, which is hidden in the public parameter $\alpha = e(P,Q)^a$, cannot be obtained. As a result, only with the time token related to time T, can someone compute and obtain β. Due to the randomness t, it is hard to get private keys a and $\{r_i\}$ of TS from the released time tokens, without which the time token $tk_T = (a + t + \sum_{i=1}^{n} t_i r_i, tQ)$ cannot be obtained. Therefore, the requester cannot decrypt the ciphertext CT until time T, when TS releases the corresponding time token tk_T. As a result, when a worker specifies the decryption time which is sufficient enough for him to leave, the current location can be preserved and will not be exposed to any other entity until the specified decryption time. When the specified decryption time T comes, the encrypted data can be fully recovered by the requester using tk_T and his private key sk_r, guaranteeing the availability of collected answers. In addition, due to the lack of the requester's private key, though obtaining tk_T from TS, the curious MCS server cannot decrypt the ciphertext, ensuring only the requester can obtain the collected answers.
- **Lightweight operations for workers.** We analysis the performance of the proposed scheme on computation overhead. We define and calculate the required cryptographic operations in the proposed scheme and compared schemes. In this paper, we mainly focus on time-consuming operations, such as bilinear pairing, scalar multiplication in G_1, parallel scalar multiplication in G_1 and exponentiation in G_2. For brevity, we use Pa, Sm, Psm and Ex to denote the above operations, respectively. **Table 2** and **Table 3** present the computational cost comparisons of schemes. Note that the bilinear pairing is the most expensive one among all operations mentioned above, we adopt the pre-computation technique to reduce the computation burden of resource-constrained mobile devices. Specifically, TS computes $\alpha = e(P,Q)^a$ in advance, which is then involved in public parameters. From **Table 2**, we observe that in the proposed scheme, the worker only needs to perform the scalar multiplication in G_1 operation twice and the exponentiation in G_2 operation once (i.e., $2Sm + 1Ex$). Neither BC-TRE, HYL-TRE nor DT-TRE supports bilinear pairing pre-computation, since the sender must compute a pairing related to the release time, resulting in more expensive computation costs in the encryption operation. Thus, the utilization of pre-computation greatly reduces the cost of computing for the worker. It can be noticed that the computation cost of decryption operation of the proposed scheme is slightly higher than that of compared schemes. This is expected, as it supports plaintext validation during decryption while BC-TRE does not. Further, the decryption operation is performed by the requester, not by the worker. Therefore, this does not affect the computation cost of the worker. Assuming the number of group members is l, from **Table 3**, we observe

that when a worker generates ring signature on message, he needs to perform scalar multiplication in G_1 operation $(l+1)$ times and parallel scalar multiplication in G_1 operation l times (i.e., $(l+1)Sm + lPsm$). Compared with YMZ-TRS and HYC-TRS, the proposed signing operation is linearly dependent on the number of group members. As a result, the worker can select the size of the group based on his mobile device, taking energy consumption into account. When the MCS server verifies the signature, he needs to perform the bilinear pairing twice and parallel scalar multiplication in G_1 operation l times. The tracing operation is performed by the MCS server and the requester, and the total computation cost is $2Pa + 2Sm + 1Ex$.

Table 2. Computational cost comparisons in terms of TRE

Scheme	Encrypt	Decrypt
BC-TRE [48]	$1Pa + 2Sm$	$1Pa$
CLQ-TRE [49]	$1Psm + 1Ex$	$1Pa + 1Psm + 1Ex$
HYL-TRE [50]	$1Pa + 2Sm + 1Psm$	$2Pa + 1Sm$
DT-TRE [51]	$1Pa + 3Sm + 1Ex$	$1Pa + 1Sm$
the proposed scheme	$2Sm + 1Ex$	$2Pa + 2Sm + 1Ex$

Table 3. Computational cost comparisons in terms of TRS

Scheme	Sign	Verify	Trace (the worst case)
YMZ-TRS [58]	$4lSm + 1Psm$	$2Pa + lSm$	$4lPa$
HYC-TRS [59]	$(3l+1)Sm + 1Psm$	$2Pa + lSm$	$4lPa + 3lSm$
the proposed scheme	$(l+1)Sm + lPsm$	$2Pa + lPsm$	$2lPa + lSm + 2lPsm$

6.2 Evaluation

In this section, we evaluate the running time of the proposed algorithms by implementing them using the JPBC Library on a desktop with 3.20 GHz CPU and 8 GB memory. We choose groups of 5, 10, 15, 20, 25, 30 members to evaluate performance. All the average results were obtained by running each algorithm 1,000 times. The results are shown in **Fig. 7** and **Fig. 8**.

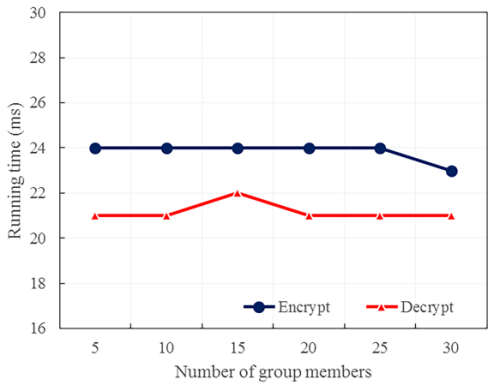


Fig. 7. Running time of data Encryption and decryption

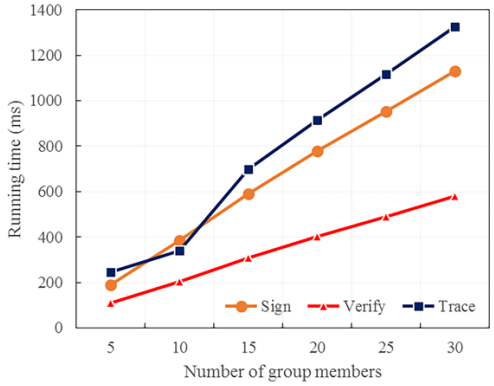


Fig. 8. Running time of data signing, verification, and tracing a misbehavior worker

From **Fig. 7**, we learn that the running time of encryption and decryption is independent of the number of group members. And the running time is generally stable between 20*ms* to 24*ms*. Therefore, it is acceptable for a worker who uses a resource-constrained mobile device for encryption. From **Fig. 8**, we observe that the running time of signing, verification and tracing is roughly linearly dependent on the number of group members. When the number of group members is 25, the running time is less than 1.2*s*, 1*s*, 0.5*s*, respectively. For workers, it provides the flexibility to select groups of the appropriate size based on the power of the mobile device.

7. Conclusion

In this paper, we proposed a lightweight and privacy-preserving answer collection scheme for MCS. We first considered the authentication with identity privacy of workers, and proposed to perform authentication anonymously based on certificate-less traceable ring signature. The anonymous authentication achieves both authentication and anonymity, and as well traceability when the collected answers are found untrustworthy. Next, we considered location privacy of workers since collected answers are usually location-dependent. The proposed scheme encrypts the collected answers based on timed-release encryption, which achieves preserving of the current location privacy, and as well high availability of collected answers. Finally, we compared the computation cost of the proposed algorithms in the proposed scheme with existing works and evaluated the running time of the proposed scheme. The results indicate that the proposed scheme provides lightweight operations and flexibility for resource-constrained mobile devices.

References

[1] J. Howe, "The rise of crowdsourcing," *Wired Magazine*, vol. 14, no. 6, pp. 1-4, Jun. 2006. [Online]. Available: https://disco.ethz.ch/courses/fs10/seminar/paper/michael-8.pdf

[2] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J. Liu, Y. Xiang, and R. Deng, "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1251-1266, 2019. Article (CrossRef Link)

[3] E. Niforatos, A. Vourvopoulos, and M. Langheinrich, "Weather with you: Evaluating report reliability in weather crowdsourcing," in *Proc. of the 14th International Conference on Mobile and Ubiquitous Multimedia*, New York, USA, ACM, pp. 152-162, 2015. Article (CrossRef Link)

[4] B. V. Haak and M. Parks, "The future of journalism: networked journalism," *Chinese Journal of Journalism and Communication*, vol. 6, pp. 2923-2938, 2013. Article (CrossRef Link)

[5] Z. Liu, Z. Li, M. Li, W. Xing, and D. Lu, "Mining road network correlation for traffic estimation via compressive sensing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 7, pp. 1880-1893, Jul. 2016. Article (CrossRef Link)

[6] [Online]. Available: https://www:birmingham:gov:uk=info=20110=report road and pavement issues.

[7] R. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," March, 1996. [Online]. Available: https://people.csail.mit.edu/rivest/pubs/RSW96.pdf

[8] A. Mehmood, I. Natgunanathan, Y Xiang, H. Poston, and Y. Zhang, "Anonymous authentication scheme for smart cloud based healthcare applications," *IEEE Access*, vol. 6, pp. 33552-33567, 2018. Article (CrossRef Link)

[9] J. Li, H. Lu, and M. Guizani, "Acpn: A novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938-948, Apr. 2015. Article (CrossRef Link)

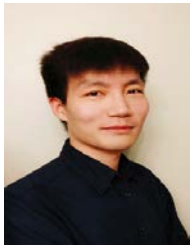
[10] A. Yang, J. Xu, J. Weng, J. Zhou, and D. S. Wong, "Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 212-225, 2021. Article (CrossRef Link)
[11] K. Rabieh, M. M. E. A. Mahmoud, M. Azer, and M. Allam, "A secure and privacy-preserving event reporting scheme for vehicular ad hoc networks," *Security & Communication Networks*, vol. 8, no. 17, pp. 3271-3281, 2015. Article (CrossRef Link)
[12] A. Q. Ejaz, N. Ahmad, M. A. Haseeb, et al., "SPATA: Strong Pseudonym-Based Authentication in Intelligent Transport System," *IEEE Access*, vol. 6, pp. 79114-79128, Nov. 2018. Article (CrossRef Link)
[13] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for vanets," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711-1720, Mar. 2016. Article (CrossRef Link)
[14] J. Xu, L. Dang, "An efficient RFID anonymous batch authentication protocol based on group signature," *Discrete & Continuous Dynamical Systems*, vol. 12(4&5), pp. 1489-1500, Dec. 2019. Article (CrossRef Link)
[15] X. Yue, M. Xi, B. Chen, et al., "A Revocable Group Signatures Scheme to Provide Privacy-Preserving Authentications," *Mobile Networks and Applications*, 2020. Article (CrossRef Link)
[16] Y. Xu, W. Wei, J. K. Liu, and X. Chen, "Lightweight anonymous authentication for ad hoc group: A ring signature approach," in *Proc. of International Conference on Provable Security*, pp. 215-226, Nov. 2015. Article (CrossRef Link)
[17] A. Kugusheva, Y. Yanovich, "Ring Signature-Based Voting on Blockchain," in *Proc. of ICBTA 2019: 2019 2nd International Conference on Blockchain Technology and Applications*, pp. 70-75, 2019. Article (CrossRef Link)
[18] P. Mundhe, V. K. Yadav, A. Singh, et al., "Ring Signature-Based Conditional Privacy-Preserving Authentication in VANETs," *Wireless Personal Communications*, 114(5), pp. 853-881, 2020. Article (CrossRef Link)
[19] K. Patil and C. T. Wasnik, "An ID-based block ring signature system for secret sharing of data," in *Proc. of 2017 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, pp. 1-5, 2017. Article (CrossRef Link)
[20] V. Pandey and U. Kulkarni, "Effective data sharing with forward security: Identity based ring signature using different algorithms," in *Proc. of 2017 International Conference on Intelligent Computing and Control (I2C2)*, Coimbatore, pp. 1-6, 2017. Article (CrossRef Link)
[21] F. Liu, Q. Wang, "IBRS: An Efficient Identity-based Batch Verification Scheme for VANETs Based on Ring Signature," in *Proc. of 2019 IEEE Vehicular Networking Conference (VNC)*, 2019. Article (CrossRef Link)
[22] L. Wang, Q. Xie, and H. Zhong, "Cooperative query answer authentication scheme over anonymous sensing data," *IEEE Access*, vol. 5, pp. 3216-3227, 2017. Article (CrossRef Link)
[23] E. Fujisaki and K. Suzuki, "Traceable ring signature," in *Proc. of the 10th International Conference on Practice and Theory in Public-key Cryptography*, Berlin, Heidelberg: Springer-Verlag, pp. 181-200, 2007. Article (CrossRef Link)
[24] E. Fujisaki, "Sub-linear size traceable ring signatures without random oracles," in *Proc. of Cryptographers' Track at the RSA Conference*, pp. 393-415, Apr. 2011. Article (CrossRef Link)
[25] K. Gu and N. Wu, "Constant size traceable ring signature scheme without random oracles," *IACR Cryptology ePrint Archive*, 2018. [Online]. Available: https://eprint.iacr.org/2018/288.
[26] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, "Id-based ring signature scheme secure in the standard model," in *Proc. of the 1st International Conference on Security*, Berlin, Heidelberg: Springer-Verlag, pp. 1-16, 2006. Article (CrossRef Link)
[27] F. YIN, Z. H, H. W, "A Traceable and Anonymous Authentication Scheme Based on ECC," *Wuhan University Journal of Natural Sciences*, vol. 6, pp. 521-526, 2020. Article (CrossRef Link)
[28] P. Branco, P. Mateus, "A Traceable Ring Signature Scheme Based on Coding Theory," *Post-Quantum Cryptography*, Springer, Cham, pp. 387-403, 2019. Article (CrossRef Link)

[29] X. Bultel, P. Lafourcade, "k-Times Full Traceable Ring Signature," in *Proc. of International Conference on Availability, Reliability and Security (ARES)*, IEEE, 2016. Article (CrossRef Link)
[30] F. Chang, J. Cui, L. Wang, "A Traceable and Anonymous Authentication Scheme Based on Elliptic Curve for Wireless Sensor Network," *Journal of Computer Research and Development*, vol. 54, no. 9, pp. 2011-2020, 2017. Article (CrossRef Link)
[31] K. Gu, L. Wang, N. Wu, and N. Liao, "Traceable certificateless ring signature scheme for no full anonymous applications," *International Journal of Network Security*, vol. 20, no. 4, pp. 762-773, 2018. Article (CrossRef Link)
[32] L. Kazemi and C. Shahabi, "A privacy-aware framework for participatory sensing," *SIGKDD Explor. Newsl.*, vol. 13, no. 1, pp. 43-51, Aug. 2011. Article (CrossRef Link)
[33] Khuong Vu, Rong Zheng, and Jie Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing," in *Proc. of 2012 Proc. IEEE INFOCOM*, pp. 2399-2407, Mar. 2012. Article (CrossRef Link)
[34] L. Pournajaf, L. Xiong, V. Sunderam, and S. Goryczka, "Spatial task assignment for crowd sensing with cloaked locations," in *Proc. of* 2014 *IEEE 15th International Conference on Mobile Data Management*, vol. 1, pp. 73-82, Jul. 2014. Article (CrossRef Link)
[35] 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, pp. 351-380, Apr. 2011. Article (CrossRef Link)
[36] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of the First International Conference on Mobile Systems, Applications, and Services*, pp. 31-42, May. 2003. Article (CrossRef Link)
[37] L. Wang, D. Yang, X. Han, W. Tianben, D. Zhang, and X. Ma, "Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation," in *Proc. of International Conference*, pp. 627-636, Apr. 2017. Article (CrossRef Link)
[38] H. To, G. Ghinita, and C. Shahabi, "A framework for protecting worker location privacy in spatial crowdsourcing," *Proc. VLDB Endow.*, vol. 7, no. 10, pp. 919-930, Jun. 2014. Article (CrossRef Link)
[39] J. Wang, Z. Cai, D. Li, D. Yang, J. Li, and H. Gao, "Protecting query privacy with differentially private k-anonymity in location-based services," *Personal and Ubiquitous Computing*, vol. 22, pp. 453-469, Mar. 2018. Article (CrossRef Link)
[40] M. Azees, P. Vijayakumar, and L. J. Deboarh, "Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467-2476, Sep. 2017. Article (CrossRef Link)
[41] Y. Shen, L. Huang, L. Li, X. Lu, S. Wang, and W. Yang, "Towards preserving worker location privacy in spatial crowdsourcing," in *Proc. of 2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, Dec. 2015. Article (CrossRef Link)
[42] B. Liu, L. Chen, X. Zhu, Y. Zhang, C. Zhang, and W. Qiu, "Protecting location privacy in spatial crowdsourcing using encrypted data," *Advances in Database Technology - EDBT*, pp. 478 - 481, Mar. 2017. Article (CrossRef Link)
[43] E. De Cristofaro and C. Soriente, "Extended capabilities for a privacy-enhanced participatory sensing infrastructure (pepsi)," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2021-2033, Dec. 2013. Article (CrossRef Link)
[44] L. Kong, L. He, X. Liu, Y. Gu, M. Wu, and X. Liu, "Privacy-preserving compressive sensing for crowdsensing based trajectory recovery," in *Proc. of 2015 IEEE 35th International Conference on Distributed Computing Systems*, pp. 31-40, Jun. 2015. Article (CrossRef Link)
[45] T. Zhou, Z. Cai, B. Xiao, et al., "Location Privacy-Preserving Data Recovery for Mobile Crowdsensing," in *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 3, pp. 1-23, 2018. Article (CrossRef Link)

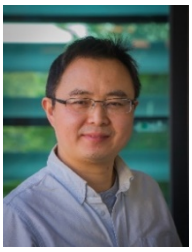
[46] T. Peng, Q. Liu, G. Wang, et al., "Multidimensional privacy preservation in location-based services," *Future Generation Computer Systems*, vol. 93, pp. 312-326, Apr. 2019. Article (CrossRef Link)
[47] T. May, "Timed-release crypto," 1993. [Online]. Available: http://www.cyphernet.org/cyphernomicon/chapter14/14.5.html
[48] A. C. Chan and I. F. Blake, "Scalable, server-passive, user-anonymous timed release cryptography," in *Proc. of 25th IEEE International Conference on Distributed Computing Systems*, pp. 504-513, Jun. 2005. Article (CrossRef Link)
[49] J. Cathalo, B. Libert, and J.-J. Quisquater, "Efficient and noninteractive timed-release encryption," in *Proc. of the 7th International Conference on Information and Communications Security*, Berlin, Heidelberg: Springer-Verlag, pp. 291-303, 2005. Article (CrossRef Link)
[50] Y. H. Hwang, D. H. Yum, and P. J. Lee, "Timed-release encryption with pre-open capability and its application to certified e-mail system," in *Proc. of the 8th International Conference on Information Security*, Berlin, Heidelberg: Springer-Verlag, pp. 344-358, 2005. Article (CrossRef Link)
[51] A. W. Dent and Q. Tang, "Revisiting the security model for timed-release encryption with pre-open capability," in *Proc. of the 10th International Conference on Information Security*. Berlin, Heidelberg: Springer-Verlag, pp. 158-174, 2007. Article (CrossRef Link)
[52] A. Fujioka, Y. Okamoto, and T. Saito, "Generic construction of strongly secure timed-release public-key encryption," in *Proc. of Australasian Conference on Information Security and Privac*, pp. 319-336, Jul. 2011. Article (CrossRef Link)
[53] Y. Watanabe, T. Seito, and J. Shikata, "Information-theoretic timed-release security: Key-agreement, encryption, and authentication codes," in *Proc. of International Conference on Information Theoretic Security*, vol. 7412, pp. 167-186, Aug. 2012. Article (CrossRef Link)
[54] Y. Watanabe, J. Shikata, "Timed-Release Secret Sharing Scheme with Information Theoretic Security," *Cryptography and Information Security in the Balkans*, 2015.
[55] C. I. Fan, J. C. Chen, S. Y. Huang, et al., "Provably Secure Timed-Release Proxy Conditional Reencryption," *IEEE Systems Journal*, vol. 11, pp. 2291-2302, Dec. 2017. Article (CrossRef Link)
[56] J. Liu J, T. Jager, S. A. Kakvi, et al., "How to build time-lock encryption," *Designs Codes and Cryptography*, vol. 86, no. 2, pp. 2549-2586, 2018. Article (CrossRef Link)
[57] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, pp. 452-473, Jan. 2003. Article (CrossRef Link)
[58] J. Yang, X. Miao, H. Zhu, and Y. Li, "Efficient certificate ring signature scheme with identity tracing," *Information security and technology*, vol. 7, no. 5, pp. 32-35, Jul. 2014. [Online]. Available: http://en.cnki.com.cn/Articleen/CJFDTOTAL-AQJS201407009.htm
[59] D. W. Huang, X. Y Yang, and H. B. Chen, "Ring signature scheme with revocable anonymity," *Computer Engineering and Applications*, vol. 46, no. 24, pp. 88-89, 2010. Article (CrossRef Link)

Yingling Dai is currently pursuing the master degree in Jinan University. Her research mainly focuses on information security and cryptography.

Jian Weng received the Ph.D. degree in computer science and engineering from Shanghai Jiao Tong University, in 2008. From 2008 to 2010, he held a post-doctoral position with the School of Information Systems, Singapore Management University. He is currently a Professor and the Dean with the College of Information Science and Technology, Jinan University. His research interests include public key cryptography, cloud security, blockchain, etc. He has published over 100 papers in cryptography and security conferences and journals, such as CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, TPAMI, TIFS, and TDSC. He served as a PC co-chairs or PC member for more than 30 international conferences. He also serves as associate editor of IEEE Transactions on Vehicular Technology.



Anjia Yang received the Ph.D. degree in department of Computer Science from the City University of Hong Kong in 2015. He held a post-doctoral position in the City University of Hong Kong from 2015 to 2016, and in Jinan University from 2016 to 2019, respectively. From 2018 to 2019, he was a visiting scholar in BBCR group in University of Waterloo. He is currently an associate professor in Jinan University, Guangzhou. His research interests include security and privacy in internet of things, vehicular networks, blockchain and cloud computing, etc. He has published over 30 international papers including journals and conferences, such as IEEE TDSC, IEEE TMC, IEEE TPDS, IEEE TSC, IEEE TCC, IEEE TITS, IEEE TVT, ESORICS, WiSec et al. He served as PC members or organizers for more than 20 international conferences. He also serves as an academic editor for Security and Communication Networks.



Shui Yu is a professor in the School of Computer Science, University of Technology Sydney, Australia, and a guest professor at Zhengzhou University, China. He is currently serving on a number of prestigious Editorial Boards, including IEEE Communications Surveys & Tutorials (Area Editor) and IEEE Communications Magazine. He is a member of AAAS and ACM, and a Distinguished Lecturer of the IEEE Communications Society.

Robert H. Deng is AXA Chair Professor of Cybersecurity, School of Information Systems, Singapore Management University (SMU). His research interests are in the areas of data security and privacy, cloud security and Internet of Things security. He received the Outstanding University Researcher Award from National University of Singapore, Lee Kuan Yew Fellowship for Research Excellence from SMU, and Asia-Pacific Information Security Leadership Achievements Community Service Star from International Information Systems Security Certification Consortium. He has served in many editorial boards and conference committees, including the editorial boards of IEEE Security & Privacy Magazine, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, International Journal of Information Security, Journal of Computer Science and Technology, and Steering Committee Chair of the ACM Asia Conference on Computer and Communications Security. He is an IEEE Fellow.