The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLVIII-4-2024
ISPRS TC IV Mid-term Symposium “Spatial Information to Empower the Metaverse”, 22–25 October 2024, Fremantle, Perth, Australia

Privacy-preserving Indoor Localization in Cloud Environments Based on Ranging Transformation and Inner Product Encryption

Zhiheng Wang, Yanyan Xu , Bo Zhang, Xue Ouyang

State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430072, China-(wangzhih, xuyy, whubozhang, ouyangxue602)@whu.edu.cn

Keywords: Indoor Positioning, Privacy Preserving, Inner Product Encryption, Cloud Computing.

Abstract

Cloud-based indoor positioning services offer advantages over non-cloud approaches, but also face serious privacy concerns. How to utilize an untrusted cloud server for location computation while not allowing the server to obtain the localization results is the most challenge in solving the privacy concerns, which has not been solved by the existing research. In this paper, a privacy-preserving indoor positioning scheme was designed to address this challenge. Based on the previous work using Inner Product Encryption for the protection of ranging information and anchor location information during the localization process, a transformation method was additionally proposed for the protection of localization results. The ranging information was transformed by the target, which enables the localization server to get only the transformed localization result, and only the target can recover the real location from it. In addition, this transformation is designed to be performed on the ciphertexts of the Inner Product Encryption so that the private information required for transformation is in the ciphertext form thus avoiding privacy leakage. Theoretical analysis and experimental results demonstrated that this scheme can protect the ranging information, localization results and anchor location information. At the same time, it has lower computation and communication overhead and hardly degrades the localization accuracy.

1. Introduction

Indoor Positioning Service (IPS) not only brings great convenience to people’s activities indoors, but also plays a significant role in various fields, such as Industry 4.0, Smart Cities and so on. Since positioning signals of Global Navigation Satellite System (GNSS) cannot be received in indoor environments, IPSs are usually provided by IPS providers (Wang et al., 2024). The user collects location-related measurement information, such as ranging information from anchors or Received Signal Strength (RSS), and sends it to the localization server deployed by the IPS provider, where the location estimation algorithms are executed and the obtained positioning results are returned to the user. However, with the complexity of positioning algorithms, the abundance of positioning resources, and the proliferation of positioning users, IPS providers have difficulty with the growing burden of data storage and positioning computation, and therefore prefer to outsource positioning resources and positioning algorithms to resource-rich cloud environments to provide cloud-based IPS to users. As more and more IPS providers are choosing cloud-based IPS, this is expected to be an expanding trend in the future.

Although cloud-based IPS offer more benefits than traditional (non-cloud-based) IPS, it faces more serious threats of privacy leakage. In cloud-based IPS, the cloud service provider (CSP) undertakes the tasks of positioning resource storage and positioning computation. Therefore not only the user’s positioning results will be leaked to the CSP, but also the positioning resource of IPS provider is at risk of information leakage. Taking the widely used ranging-based indoor positioning as an example, the CSP takes the user’s ranging information and the IPS provider’s anchor location information as inputs, and executes the localization algorithm to obtain the positioning results. In this process, the positioning result and ranging information of users, as well as the anchor location information of the IPS provider are all leaked to the CSP. Whereas the CSP is usually considered “honest but curious”, it has the potential to actively peek at the private information it accesses. And as an open platform, it may also be attacked by external attackers causing passive leakage of private information. Therefore, the cloud-based IPS must support privacy preservation, i.e., protecting the user’s ranging information and positioning results, as well as the anchor location information of IPS providers while providing positioning services to the user.

A variety of solutions based on cryptography (Shu et al., 2014, Hussain and Koushanfar, 2016, Jiang et al., 2019) and information hiding (Shi and Wu, 2018, Wang et al., 2018, Zhao et al., 2020a) have been proposed in the field of privacy-preserving IPS. Most of these solutions however, are designed for the non-cloud localization scenarios, where the user is served as computation center, and are therefore not applicable to the scenario of cloud-based IPS with an untrusted entity as the computational center. Although these solutions prevent the disclosure of private information of the target and the anchors to each other during the location estimation process, these solutions still have a more trustworthy entity compared to the cloud environment, such as the target, to perform localization computation. Therefore, these solutions cannot be migrated to cloud-based localization scenarios, otherwise the localization results and other private information will be leaked to the untrusted cloud servers. Other solutions specifically address privacy leakage in cloud-based localization or other scenarios where untrusted localization servers are used as computational centers. The work in (Zhao et al., 2018) and (Li et al., 2016) utilizes k-anonymity to cloak a target in a cloaking set consisting of multiple targets. This prevents the location privacy of the target from being leaked to the server, but the scheme fails when there is only one target. In other k-anonymity based solution (Zhao et al., 2020b), the target generates k-1 dummy measurements, and the localization server will accordingly obtain k localization results, preventing the real location from being distinguished. However, the computational overhead of the loc-

alization server is k times as larger, and the privacy protection is greatly weakened if the auxiliary information is leaked (Holcer et al., 2020). Han et al. designed privacy-preserving trilateral and multilateral localization protocols based on Paillier in (Jiang et al., 2019), where the homomorphic property is leveraged so that untrusted localization servers can only get location results in ciphertext. These protocols however, suffer from a high computational overhead. The privacy-preserving localization protocol presented in (Yan et al., 2022) is based on Intel Software Guard Extensions (SGX), which isolates a trusted execution environment for the localization computation in an untrusted localization server thus prevents private information leakage. It is secure and efficient but has more requirements for the localization server equipment. In the protocol designed in (Liu and Yan, 2022), the base stations concatenates and multiplies the private ranging information and location coordinates with cancelable random matrices before sending to the server, thus hiding this private information and enabling the localization server to get only intermediate localization results protected by random numbers. This solution is computationally efficient, but security deficient, as the secret keys used to reveal the final localization results from the intermediate results of the localization server, are also owned by each base station, meaning that the scheme is not resistant to the collusion of the localization server and the base stations, which occurs when they are simultaneously compromised by an attacker. In our previous work (Wang et al., 2022), a privacy-preserving scheme based on Inner Product Encryption (IPE) was proposed for ranging-based localization systems in cloud environments, and has shown to achieve a better balance than other schemes between efficiency and security. However, k-anonymity techniques are utilized to protect the localization results, and therefore also bring about the same drawbacks in terms of efficiency and security as other k-anonymity based solutions as discussed previously. Therefore, an extended research of alternative methods is necessary for enhanced security and efficiency.

Similar to our previous study, the IPE scheme is also used in this extended research to protect the ranging information and anchor location information and to enable localization algorithms on the ciphertexts. Differently, a transformation method for ranging information was devised in the extended research to address the compromise of k-anonymity in terms of privacy preservation and efficiency. Taking the transformed ranging information as input, the localization server gets only the transformed localization result. From which, only the users are able to reveal their real locations using their secret keys. With this approach, the cloud server computes no longer for decoy results, as it did in the k-anonymity approach, thus reducing overheads. In addition, in order to prevent the leakage of location information of anchors, which was used as an assistant in the transformation process, the transformation method over the ciphertext of IPE was designed, so that all private information was transmitted and processed in the form of ciphertext. Therefore, the extended research realizes the requirement of privacy-preserving localization in cloud environments and compensates for the limitations of security and efficiency of the previous k-anonymity approach.

2. Main body

2.1 Problem formulation

2.1.1 Localization scenario The localization scenario considered in this paper is shown in Fig.1. The anchors (m in total) transmit positioning reference signals to the target. Based on these signals, the target estimates the distance to each of the anchors and sends this ranging information to the localization server provided by the CSP. The localization server, storing information about the anchor locations, performs the following least-square localization algorithm to estimate the location of the target and returns.

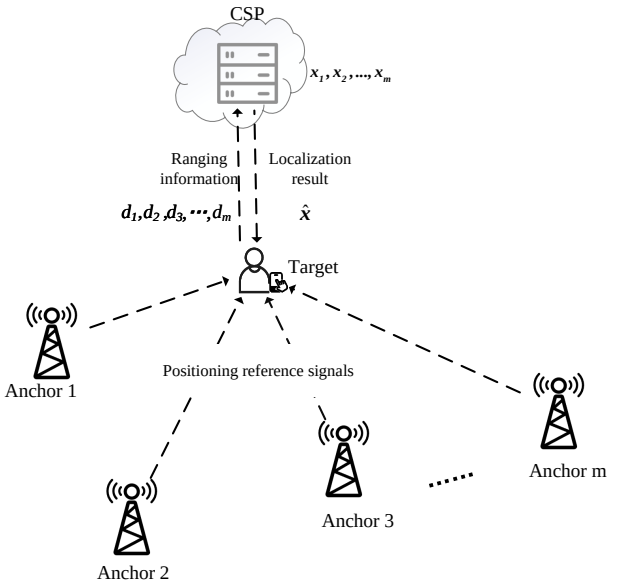


Figure 1. Ranging-based localization scenario.

$$\hat{\boldsymbol{x}} = \frac{1}{2}(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\boldsymbol{b}, \tag{1}$$

where

$$\boldsymbol{A} = \begin{bmatrix} (\boldsymbol{x_1} - \boldsymbol{x_m})^T \\ \vdots \\ (\boldsymbol{x_{m-1}} - \boldsymbol{x_m})^T \end{bmatrix}, \tag{2}$$

$$\boldsymbol{b} = \begin{bmatrix} \boldsymbol{x_1}^T\boldsymbol{x_1} - \boldsymbol{x_m}^T\boldsymbol{x_m} - (d_1^2 - d_m^2) \\ \vdots \\ \boldsymbol{x_{m-1}}^T\boldsymbol{x_{m-1}} - \boldsymbol{x_m}^T\boldsymbol{x_m} - (d_{m-1}^2 - d_m^2) \end{bmatrix}, \tag{3}$$

and $\hat{\boldsymbol{x}}$ denotes the least-square estimation result of the target location, $\boldsymbol{x_i}, i = 1, 2, \ldots, m$ denotes the location coordinates of each anchor, and $d_i, i = 1, 2, \ldots, m$ denotes the estimated distance to each anchor.

2.1.2 Threat model and design goals In the localization scenario, the CSP is assumed to be “honest but curious”, which means that it faithfully executes the localization algorithm, but with the potential to steal the localization data of users and the anchor information owned by the IPS provider. The CSP could also be attacked by external attackers. The authorized users are considered credible, and the IPS provider is semi-trusted, which means that it is unwilling to leak its database information during the positioning process, but may want to analyze the user’s location privacy.

Considering these threats in the localization process, the privacy-preserving goal of the designed scheme is to both protect the location information of the anchors from being accessed by

CSP and external attackers, and to protect the user's ranging information and localization results from CSP and IPS providers. In addition, the proposed scheme is expected to have high accuracy and efficiency considering the requirements of indoor positioning applications. In order to achieve these goals, a privacy preserving localization scheme based on ranging transformation and Inner Product Encryption (IPE) is proposed. The specific details are shown in the following section.

2.2 The proposed scheme

The overall workflow is shown in Fig.2. The IPS provider encrypts the anchor information and outsources the ciphertexts to the cloud server offline. The user (target) generates a secret key, and performs, with this secret key, a transformation on the ciphertext of the ranging information encrypted by IPE, as well as on the encrypted anchor information from the cloud server, to calculate the transformed and encrypted ranging information, and send it to the cloud server. The cloud server executes the localization algorithm over the ciphertexts as already designed in (Wang et al., 2022), that performs the IPE decryption process to compute the inner product terms decomposed from the least-square localization algorithm, to finally compute the localization result. And a transformed ranging information by the proposed method in this paper as input to the localization algorithm in (Wang et al., 2022) will yield a transformed localization result, which means that even the cloud servers performing the location estimation do not know the real location of the user. In addition, since the transformation process was carried out on the ciphertexts, it does not cause the anchor's location information to be leaked to external attackers or users. This transformation method achieves the purpose of the previous k-anomymity method of hiding the user's location from the cloud server, while avoiding the localization computation for decoy results, and thus offers higher efficiency and security.

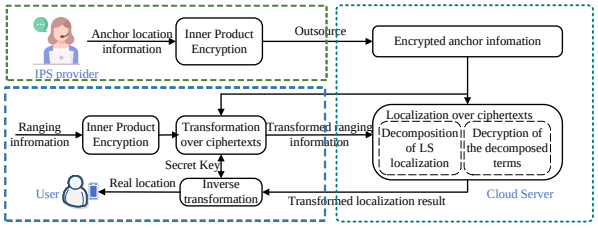


Figure 2. Workflow of the proposed scheme.

Specifically, the detailed process of this workflow is shown in Algorithm 1. This scheme starts with the encryption of anchor location information by the IPS provider during the offline phase. The IPS provider employs the IPE scheme proposed in (Kim et al., 2018) to generate the public parameters pp and the master secret key msk, and encrypts the vectors $\boldsymbol{u}, \boldsymbol{v}$ and $\boldsymbol{e_j}$ associated with the anchor location using the $IPE.KeyGen$ algorithm. In order to make the encrypted anchor information computable and thus support transformations on the ciphertexts, a modified $IPE.Encrypt$ algorithm is additionally used to encrypt $\boldsymbol{e_j}$ as in Step 1.4. These ciphertexts are outsourced to the CSP to provide the target with online indoor positioning services. During the online phase, the target encrypts and transforms the ranging information. Initially, the same modified $IPE.Encrypt$ algorithm is used to encrypt the target's ranging information to support the transformation on the ciphertexts as in Step 2.2. Subsequently, the encrypted anchor information

Algorithm 1 Privacy-preserving indoor positioning based on ranging transformation and IPE.

Result: Target with localization result $\hat{\boldsymbol{x}}$, (n-dimensional).
Private Input: IPS provider with m anchor coordinates $\boldsymbol{x_i}$ (n-dimensional); target with ranging information $\boldsymbol{w} = [d_1^2 - d_m^2, d_2^2 - d_m^2, \ldots, d_{m-1}^2 - d_m^2]^T$.
Offline Operation (IPS provider):
1.1. calculate $\boldsymbol{e_j}, \boldsymbol{u}, \boldsymbol{v}$ from $\boldsymbol{x_i}$ as :

$$\boldsymbol{d_i} = \boldsymbol{x_i} - \boldsymbol{x_m}, i = 1, 2, \ldots, m-1, \quad (4)$$

$$\boldsymbol{e_j} = [\boldsymbol{d_1}(j), \boldsymbol{d_2}(j), \boldsymbol{d_{m-1}}(j)]^T, j = 1, 2, \ldots, n, \quad (5)$$

$$\boldsymbol{u} = [\boldsymbol{x_1}^T\boldsymbol{x_1}, \boldsymbol{x_2}^T\boldsymbol{x_2}, \ldots, \boldsymbol{x_{m-1}}^T\boldsymbol{x_{m-1}}]^T, \quad (6)$$

$$\boldsymbol{v} = [\boldsymbol{x_m}^T\boldsymbol{x_m}, \boldsymbol{x_m}^T\boldsymbol{x_m}, \ldots, \boldsymbol{x_m}^T\boldsymbol{x_m}]^T; \quad (7)$$

1.2. encrypt $\boldsymbol{u}, \boldsymbol{v}$ and $\boldsymbol{e_j}$ using $IPE.KeyGen$ algorithm to get sk_u, sk_v and sk_{ej}, respectively;
1.3. encrypt $\boldsymbol{e_1}$ using $IPE.Encrypt$ algorithm to get $ct_{e1} = (C1_{e1}, C2_{e1})$;
1.4. encrypt $\boldsymbol{e_j}, j = 2, \ldots, n$ to get $ct_{ej} = (C1_{ej}, C2_{ej})$, where $C1_{ej} = C1_{e1}, C2_{ej} = C1_{ej}^{\boldsymbol{B^*}^T\boldsymbol{e_j}}$, and $\boldsymbol{B^*}$ is a parameter in msk;
1.5. outsource $sk_u, sk_v, sk_{ej}, ct_{ej}, j = 1, 2, \ldots, n$ to CSP.
Online Operation (Target):
2.1. receive ct_{ej} from CSP and msk from IPS provider;
2.2. encrypt the ranging information $\boldsymbol{w}$ to get $ct_w = (C1_w, C2_w) = (C1_{e1}, C1_w^{(\boldsymbol{B^*})^T\boldsymbol{w}})$;
2.3. generate a random vector $\boldsymbol{x_s} = [x_{s1}, x_{s2}, \ldots, x_{sn}]^T$ as a transformation key, and transform ct_w into ct_{ws} as:

$$ct_{ws} = (C1_{ws}, C2_{ws}) = (C1_w, C2_w * \prod_{j=1}^{n} C2_{ej}^{-2x_{sj}}); \quad (8)$$

2.4. send ct_{ws} to CSP for positioning.
Online Operation (CSP):
3.1. calculate the elements of row i and column j of matrix $\boldsymbol{\mathcal{A}}, 1 \le i, j \le n$:

$$\boldsymbol{\mathcal{A}}(i, j) = IPE.Decrypt(sk_{ci}, ct_{cj}, pp); \quad (9)$$

3.2. calculate the element of the j-th $1 \le j \le n$ element in vector $\boldsymbol{\mathcal{b}_1}, \boldsymbol{\mathcal{b}_2}$ and $\boldsymbol{\mathcal{b}_3}$:

$$\boldsymbol{\mathcal{b}_1}(j) = IPE.Decrypt(sk_u, ct_{cj}, pp), \quad (10)$$

$$\boldsymbol{\mathcal{b}_2}(j) = IPE.Decrypt(sk_v, ct_{cj}, pp), \quad (11)$$

$$\boldsymbol{\mathcal{b}_3}(j) = IPE.Decrypt(sk_{cj}, ct_{ws}, pp); \quad (12)$$

3.3. calculate $\boldsymbol{x_l} = 1/2\boldsymbol{\mathcal{A}}^{-1}(\boldsymbol{\mathcal{b}_1} - \boldsymbol{\mathcal{b}_2} - \boldsymbol{\mathcal{b}_3})$ and send $\boldsymbol{x_l}$ to the target.
Online Operation (Target):
4.1. reveal the real location $\hat{\boldsymbol{x}}$ from $\boldsymbol{x_l}$ as: $\hat{\boldsymbol{x}} = \boldsymbol{x_l} - \boldsymbol{x_s}$.

ct_{ej} from the CSP and the transformation key $\boldsymbol{x_s}$ of the target's own are used to transform the encrypted ranging information ct_w to obtain the transformed and encrypted ranging information ct_{ws} as in Step 2.3, which is sent to the CSP to request IPS. Once the CSP receives the request, it executes the location estimation algorithm on the ciphertexts to get the transformed localization result. This location estimation algorithm on ciphertexts was proposed in (Wang et al., 2022), where the $IPE.Decrypt$ algorithm is executed to compute some inner product terms from the encrypted ranging information and anchor information which are decomposed from the least-square estimation algorithm, i.e,. Eq.1. Thus by computing these decomposed terms (Step 3.1–3.2) and combining them together (Step 3.3), the location estimation algorithm on the ciphertexts can be achieved. However, in the proposed scheme by this pa-

per, since the ranging information received by the CSP has been transformed, the CSP will get the localization result after a shift transformation, i.e., $\boldsymbol{x_l}$ and thus the scheme achieves the hiding of the positioning result from the CSP. The target reveals its real location by performing an inverse transformation (Step 4.1). This can be demonstrated by the following analysis.

2.3 Scheme analysis

2.3.1 Security analysis The scheme in this paper is based on the previous work (Wang et al., 2022) that utilize IPE to protect the ranging information and anchor location information, and additionally proposes to utilize an transformation on ciphertexts to achieve the protection of positioning results. The security of ranging information and anchor location information has been demonstrated and can be found in (Wang et al., 2022).

As for the localization results, they are hidden by the transformation key of the target. Therefore, the security of the localization results can be analysed by the security of the transformation key $\boldsymbol{x_s}$. In the proposed scheme, the only way for adversaries to obtain the transformation key is from the transformed encrypted ranging information ct_{ws}. Adversaries may obtain encrypted anchor information $ct_{ej} = (C1_{ej}, C2_{ej}), j = 1, 2, \ldots, n$ and transformed encrypted ranging information $ct_{ws} = (C1_w, C2_w * \prod_{j=1}^{n} C2_{ej}^{-2x_{sj}})$. But it is not possible to analyse any element $x_{sj}, j = 1, 2, \ldots, n$ of the transformation key $\boldsymbol{x_s}$ from these ciphertexts, since it can be seen that this is equivalent to solving the difficult discrete logarithm problem, i.e., given group elements g and h, finding $x \in Z_n$ such that $g^x = h$ holds. Therefore, the security of the localization result is based on the difficulty of the discrete logarithm problem.

2.3.2 Correct analysis The correctness of the scheme is based on the following three sub-conclusions:

(1) The transformed ranging information ct_{ws} is the ciphertext of $\boldsymbol{w_s} = \boldsymbol{w} - 2\sum_{j=1}^{n} \boldsymbol{x_s}(j)\boldsymbol{e_j}$ encrypted by the IPE scheme. This can be found by substituting $C1_w, C2_w$ and $C2_{ej}$ in Eq.8 with their detailed forms and comparing with the $IPE.Encrypt$ algorithm in (Kim et al., 2018).

(2) The localization result obtained by Step3.1–3.3 is equivalent to a direct calculation with the following equation,

$$\boldsymbol{x_l} = 1/2(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T(\boldsymbol{b} + \boldsymbol{b_s}), \tag{13}$$

where $\boldsymbol{A}$ and $\boldsymbol{b}$ were defined as in Eq.2 and Eq.3, and $\boldsymbol{b_s} = 2\sum_{j=1}^{n} \boldsymbol{x_s}(j)\boldsymbol{e_j}$.

Steps 3.1–3.3 are the localization algorithms on ciphertexts proposed in (Wang et al., 2022). The analysis in (Wang et al., 2022) has demonstrated that for ciphertexts of real ranging information, i.e., ct_w, these steps are equivalent to the direct computation of Eq.1. However, since in reality, steps 3.1–3.3 are for the ciphertext of transformed ranging information, i.e., ct_{ws}, and ct_{ws} is the ciphertext of $\boldsymbol{w_s} = \boldsymbol{w} - 2\sum_{j=1}^{n} \boldsymbol{x_s}(j)\boldsymbol{e_j} = \boldsymbol{w} - \boldsymbol{b_s}$, this subconclusion can therefore be demonstrated by replacing $\boldsymbol{w}$ with $\boldsymbol{w_s}$ in the correct analysis of (Wang et al., 2022).

(3) The result of Eq.13 is the target's real location after a shift transformation by $\boldsymbol{x_s}$, i.e., $\boldsymbol{x_l} = \hat{\boldsymbol{x}} + \boldsymbol{x_s}$.

Note that expanding Eq.13 yields:

$$\begin{aligned}\boldsymbol{x_l} &= 1/2(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T(\boldsymbol{b} + \boldsymbol{b_s}) \\ &= 1/2(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\boldsymbol{b} + 1/2(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\boldsymbol{b_s}.\end{aligned} \tag{14}$$

Since Eq.1 holds, i.e.,

$$\hat{\boldsymbol{x}} = 1/2(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\boldsymbol{b}, \tag{15}$$

therefore, $\boldsymbol{x_l} = \hat{\boldsymbol{x}} + 1/2(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\boldsymbol{b_s}$. In addition, since

$$\begin{aligned}\boldsymbol{b_s} &= 2\sum_{j=1}^{n} \boldsymbol{x_s}(j)\boldsymbol{e_j} \\ &= \begin{bmatrix} 2(\boldsymbol{x_1} - \boldsymbol{x_m})^T\boldsymbol{x_s} \\ \vdots \\ 2(\boldsymbol{x_{m-1}} - \boldsymbol{x_m})^T\boldsymbol{x_s} \end{bmatrix} \\ &= \begin{bmatrix} 2\boldsymbol{x_1}^T\boldsymbol{x_s} - 2\boldsymbol{x_m}^T\boldsymbol{x_s} \\ \vdots \\ 2\boldsymbol{x_{m-1}}^T\boldsymbol{x_s} - 2\boldsymbol{x_m}^T\boldsymbol{x_s} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{x_1}^T\boldsymbol{x_1} - \boldsymbol{x_m}^T\boldsymbol{x_m} \\ \vdots \\ \boldsymbol{x_{m-1}}^T\boldsymbol{x_{m-1}} - \boldsymbol{x_m}^T\boldsymbol{x_m} \end{bmatrix} \\ &- \begin{bmatrix} (\boldsymbol{x_1} - \boldsymbol{x_s})^T(\boldsymbol{x_1} - \boldsymbol{x_s}) \\ \vdots \\ (\boldsymbol{x_{m-1}} - \boldsymbol{x_s})^T(\boldsymbol{x_{m-1}} - \boldsymbol{x_s}) \end{bmatrix} \\ &+ \begin{bmatrix} (\boldsymbol{x_m} - \boldsymbol{x_s})^T(\boldsymbol{x_m} - \boldsymbol{x_s}) \\ \vdots \\ (\boldsymbol{x_m} - \boldsymbol{x_s})^T(\boldsymbol{x_m} - \boldsymbol{x_s}) \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{x_1}^T\boldsymbol{x_1} - \boldsymbol{x_m}^T\boldsymbol{x_m} - (d_{s1}^2 - d_{sm}^2) \\ \vdots \\ \boldsymbol{x_{m-1}}^T\boldsymbol{x_{m-1}} - \boldsymbol{x_m}^T\boldsymbol{x_m} - (d_{sm-1}^2 - d_{sm}^2) \end{bmatrix}\end{aligned} \tag{16}$$

where $d_{si}, i = 1, 2, \ldots, m$ denotes the distance from location $\boldsymbol{x_s}$ to each anchor. According to the least-square localization algorithm, it is obtained that:

$$\boldsymbol{x_s} = 1/2(\boldsymbol{A}^T\boldsymbol{A})^{-1}\boldsymbol{A}^T\boldsymbol{b_s}, \tag{17}$$

therefore, $\boldsymbol{x_l} = \hat{\boldsymbol{x_0}} + \boldsymbol{x_s}$.

To summarize the above three sub-conclusions, it can be derived that the localization server in the scheme can obtain the transformed localization results based on the user's request, therefore the correctness of the scheme is demonstrated.

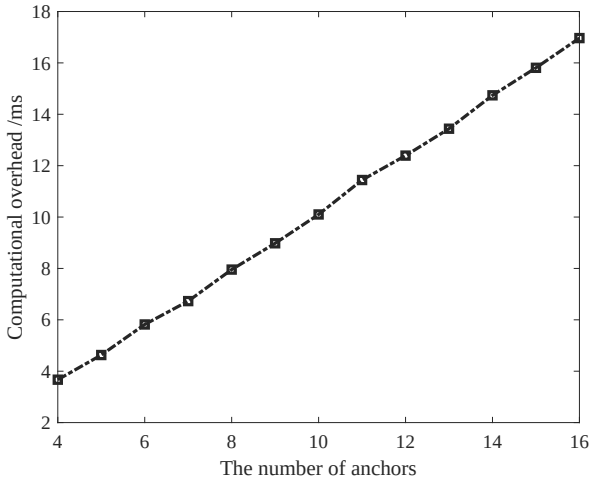
2.4 Scheme evaluation

The computational and communication overhead, as well as localization accuracy of the scheme were evaluated in a simulated experimental environment, where multiple anchors were generated and the location of the target is random in the localization scenario. The distances between the target and the anchors were calculated based on their locations. Based on this settings, the privacy preserving indoor positioning scheme were implemented in C++ on a Ubuntu platform with a 2.10GHz Intel Xeon Silver 4216 CPU. During the experiments, the computation and communication costs were measured based on its computation time and transferred data size, respectively. The localization accuracy were evaluated by the Root Mean Square Error, defined as:

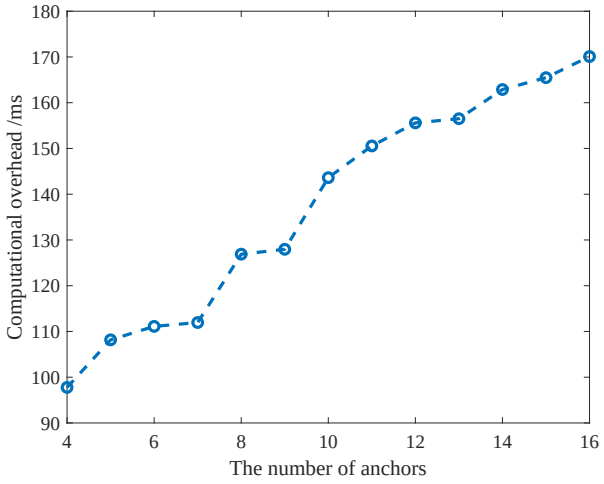
$$e = \sqrt{\frac{\sum_{i=1}^{N} \left\| \hat{\boldsymbol{x^{(i)}}} - \boldsymbol{x^{(i)}} \right\|}{N}}, \tag{18}$$

where N is the number of experiments, which in our case is 100.

2.4.1 Computational overhead The computational overheads of the scheme on the target side and the cloud server side are shown in Fig.3a and Fig.3b respectively. As can be seen, the computational burden of the target is very small, e.g., when setting the number of anchors in the experiment to 8, the time consumption is only about 8ms, and thus it satisfies the resource and energy constrained mobile-side environments. Compared to lightweight operations on the target, the server performs relatively time-consuming operations, such as decryption and localization. However, the time consumed for positioning is still much less than 1s, and therefore it can satisfy the real-time requirements of positioning services.



(a) Computational overhead on the target



(b) Computational overhead on the server

Figure 3. Computational overhead of the scheme.

2.4.2 Communication overhead The communication overhead of the scheme is shown in Fig.4. It is demonstrated that the proposed scheme has a low communication overhead, and this is due to the fact that the proposed scheme only requires the target to transmit the encrypted ranging information and receive the final result without any intermediate results that need to be encrypted or transmitted. The scheme therefore does not place significant burdens on the network and the consequent delays in communications and indoor positioning services.

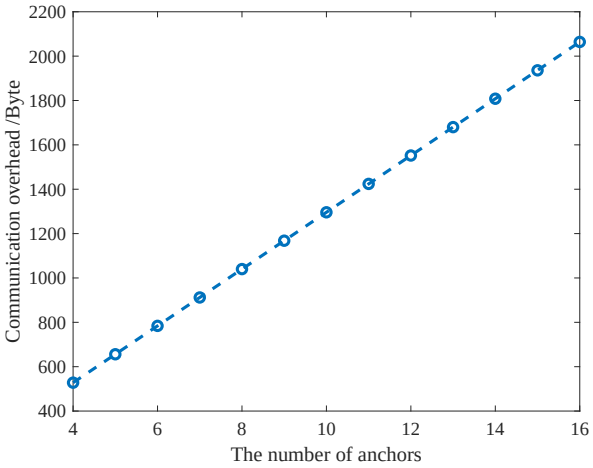


Figure 4. Communication overhead of the scheme.

2.4.3 Localization accuracy The localization accuracy of the scheme with different measurement errors was evaluated and compared with the original, i.e., the localization algorithm without privacy protection, and the results are shown in Fig.5. It can be seen that the positioning error of the proposed scheme is extremely close to that of the original algorithm, indicating that the privacy-preserving approach and the transformation method proposed in this paper do not significantly lead to a loss of positioning accuracy and a consequent degradation of the quality of the positioning service.

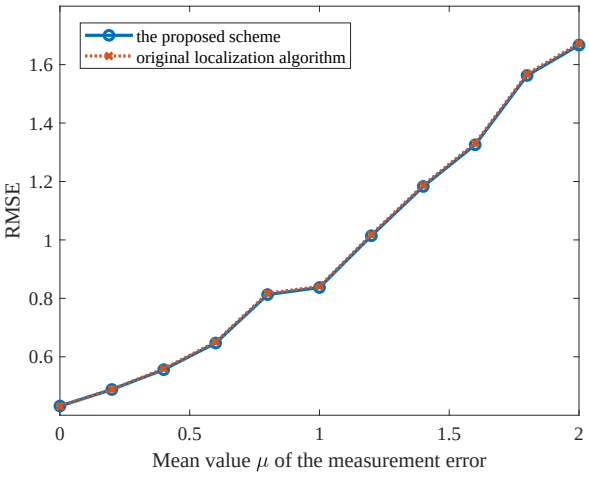


Figure 5. Localization accuracy of the schemes.

2.4.4 Comparison with other schemes Comparisons with other schemes were carried out and the results are summarised in Table 1, where “Pai1” and “Pai2” refer to the two Paillier based schemes in (Jiang et al., 2019), and “kIPE” refers to the scheme based on k-anonymity and IPE in (Wang et al., 2022). In this comparison experiment, the number of anchors was set to 4 to be consistent with the other schemes. The results demonstrate that the proposed scheme has higher efficiency with almost no loss of localization accuracy. Compared to the Paillier based schemes, the computational and communication overheads of the scheme were reduced by 85% and 88%, respectively. Besides, compared to the alternative k-anonymity approach, the proposed transformation method reduces the time

and communication overhead to 1/k approximately, which saves computational and communication resources in the cloud environment.

Schemes	Accuracy loss (/m)	Communication overhead (byte)	Computational overhead (ms)
Ours	0.01	528	97.7
Pai1	0.14	4576	665.5
Pai2	0.59	5720	932.5
kIPE	0.01	2496	286.9

Table 1. Experimental results and comparisons.

3. Conclusion

In this paper, a privacy-preserving scheme was designed to solve the privacy concerns in cloud-based IPS, addressing the challenge that an untrusted localization server performing location estimation will get the real localization result of the target. By transforming the ranging information, the localization server is not able to obtain the real location of the target but only a transformed result. And by designing this transformation process to be executed on ciphertext, the leakage of private information required for the transformation process is prevented. Theoretical analysis and experimental results suggest that the scheme has high security strength with low computational and communication overheads, and that the scheme has a less impact on positioning accuracy.

Acknowledgements

This work is supported by National Key Research and Development Program of China (No. 2021YFB2501103); National Natural Science Foundation of China (No. 42271431).

References

Holcer, S., Torres-Sospedra, J., Gould, M., Remolar, I., 2020. Privacy in Indoor Positioning Systems: A Systematic Review. *2020 International Conference on Localization and GNSS (ICL-GNSS)*, IEEE, 1–6.

Hussain, S. U., Koushanfar, F., 2016. Privacy preserving localization for smart automotive systems. *Proceedings of the 53rd Annual Design Automation Conference*, 05-09-June, ACM, New York, NY, USA, 1–6.

Jiang, H., Wang, H., Zheng, Z., Xu, Q., 2019. Privacy preserved wireless sensor location protocols based on mobile edge computing. *Computers & Security*, 84, 393–401. https://linkinghub.elsevier.com/retrieve/pii/S0167404818311295.

Kim, S., Lewi, K., Mandal, A., Montgomery, H., Roy, A., Wu, D. J., 2018. Function-Hiding Inner Product Encryption Is Practical. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11035 LNCS, 544–562.

Li, H., He, Y., Cheng, X., Sun, L., 2016. A Lightweight Location Privacy-Preserving Scheme for WiFi Fingerprint-Based Localization. *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, IEEE, 525–529.

Liu, S., Yan, Z., 2022. Efficient Privacy Protection Protocols for 5G-Enabled Positioning in Industrial IoT. *IEEE Internet of Things Journal*, 9(19), 18527–18538. https://ieeexplore.ieee.org/document/9739352/.

Shi, X., Wu, J., 2018. To Hide Private Position Information in Localization Using Time Difference of Arrival. *IEEE Transactions on Signal Processing*, 66(18), 4946–4956. https://ieeexplore.ieee.org/document/8417931/.

Shu, T., Chen, Y., Yang, J., Williams, A., 2014. Multilateral privacy-preserving localization in pervasive environments. *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, IEEE, 2319–2327.

Wang, G., He, J., Shi, X., Pan, J., Shen, S., 2018. Analyzing and Evaluating Efficient Privacy-Preserving Localization for Pervasive Computing. *IEEE Internet of Things Journal*, 5(4), 2993–3007. https://ieeexplore.ieee.org/document/8103755/.

Wang, Z., Xu, Y., Yan, Y., Ouyang, X., Zhang, B., 2024. Privacy-Preserving WiFi Localization Based on Inner Product Encryption in a Cloud Environment. *IEEE Internet of Things Journal*, 11(10), 17264–17282. https://ieeexplore.ieee.org/document/10414030/.

Wang, Z., Xu, Y., Yan, Y., Zhang, Y., Rao, Z., Ouyang, X., 2022. Privacy-preserving indoor localization based on inner product encryption in a cloud environment. *Knowledge-Based Systems*, 239, 108005. https://doi.org/10.1016/j.knosys.2021.108005 https://linkinghub.elsevier.com/retrieve/pii/S0950705121011126.

Yan, Z., Qian, X., Liu, S., Deng, R., 2022. Privacy Protection in 5G Positioning and Location-based Services Based on SGX. *ACM Transactions on Sensor Networks*, 18(3), 1–19. https://dl.acm.org/doi/10.1145/3512892.

Zhao, H., Yan, J., Luo, X., Gua, X., 2020a. Privacy preserving solution for the asynchronous localization of underwater sensor networks. *IEEE/CAA Journal of Automatica Sinica*, 7(6), 1511–1527. https://ieeexplore.ieee.org/document/9146983/.

Zhao, P., Jiang, H., Lui, J. C. S., Wang, C., Zeng, F., Xiao, F., Li, Z., 2018. P3-LOC: A Privacy-Preserving Paradigm-Driven Framework for Indoor Localization. *IEEE/ACM Transactions on Networking*, 26(6), 2856–2869. https://ieeexplore.ieee.org/document/8542955/.

Zhao, P., Liu, W., Zhang, G., Li, Z., Wang, L., 2020b. Preserving Privacy in WiFi Localization With Plausible Dummy Locations. *IEEE Transactions on Vehicular Technology*, 69(10), 11909–11925. https://ieeexplore.ieee.org/document/9130897/.