A lightweight verifiable outsourced decryption of attribute-based encryption scheme for blockchain-enabled wireless body area network in fog computing

Rui Guo1,2,3, Chaoyuan Zhuang1,2, Huixian Shi4, Yinghui Zhang1,2,3 and Dong Zheng1,2,3

Abstract
Wireless body area network includes some tiny wearable sensors for monitoring the physiological data of user, which has been a promising method of promoting the quality and efficiency greatly in healthcare. The collected physical signs are aggregated into the medical documents and uploaded to cloud server for utilizing by the remote user. As these files are highly sensitive privacy data, there is a vital challenge that constructs a secure and efficient communication architecture in this application scenario. Based on this standpoint, we present a lightweight verifiability ciphertext-policy attribute-based encryption protocol with outsourced decryption in this article. Specifically, our construction enjoys the following six features: (1) Although the outsourced decryption enables to save the computation overhead of the data user sharply in an attribute-based encryption scheme, the ciphertext is out of control and the correctness cannot be guaranteed by the data owner. The proposal provides the verifiability of ciphertext that ensures the user to check the correctness efficiently. (2) The size of the ciphertext is constant that is not increased with the complexity of attribute and access structure. (3) For Internet of Things devices, it introduces the fog computing into our protocol for the purpose of low latency and relation interactions, which has virtually saved the bandwidth. (4) With the help of blockchain technique, we encapsulate the hash value of public parameter, original and transformed ciphertext and transformed key into a block, so that the tamper-resistance is facilitated against an adversary from inside and outside the system. (5) In the standard model, we prove that it is selectively chosen-plaintext attack-secure and verifiable provided that the computational bilinear Diffie–Hellman assumption holds. (6) It implements this protocol and shows the result of performance measurement, which indicates a significant reduction on communication and computation costs burden on every entity in wireless body area network.

Keywords
Verifiability, outsourced decryption, attribute-based encryption, fog computing, blockchain

Date received: 31 August 2019; accepted: 26 December 2019
Handling Editor: Zheng Chang

Introduction
Internet of Things (IoTs) connect physical devices on Internet, including sensor nodes, smart terminals, and other wireless communication equipments.1–3 As a main application of IoTs, the wireless body area

1School of Cyberspace Security, Xi’an University of Posts & Telecommunications, Xi’an, China
2National Engineering Laboratory for Wireless Security, Xi’an University of Posts & Telecommunications, Xi’an, China
3Guangxi Cooperative Innovation Center of Cloud Computing and Big Data, Guilin University of Electronic Technology, Guilin, China
4Department of Mathematics and Information Science, Shaanxi Normal University, Xi’an, China

Corresponding author:
Rui Guo, School of Cyberspace Security, Xi’an University of Posts & Telecommunications, Xi’an 710121, China.
Email: guorui@xupt.edu.cn

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
network (WBAN) has attracted a tremendous attention recently. WBAN consists of various wearable intelligent sensors on the body, which are connected in the form of wireless communication link. The sensors in WBAN provide the constant health monitoring (for example, the heart beat, the body temperature, the blood pressure, and electrocardiogram), and real-time feedback to the data user (DU) or medical staff. Taking advantages of WBAN, the patient enjoys a promising physical mobility and experiences a high-quality healthcare service at home. In addition, these collected physiological data are uploaded to the cloud platform for being utilized by the DU.

As a distributed computation model over a shared pool, cloud computing provides infrastructure as a service like physical computing resources, data partitioning, storage, and so on. In the cloud paradigm, the user just pays for enjoying the corresponding cloud services supported by the cloud service provider (CSP) instead of managing and maintaining the infrastructure, which reduces the local storage overhead and provides the convenient data access service. Uploading the physiological data in WBAN to cloud platform, it realizes the real-time data sharing, the elastic computation resource distribution and the accurate response in time. However, the data owner (DO) loses the capacity of controlling over it physically after being stored on the cloud platform, and the physiological data contains some sensitive privacy. Therefore, it is essential to implement the confidentiality protection with access control against the unauthorized user and curious CSP.

For enjoying the confidentiality and access control in cloud, the attribute-based encryption (ABE) scheme was proposed as a preeminent cryptographic primitive. ABE is an one-to-many encryption mode that the authorized entity is able to decrypt the protected data only if the access structure and attribute attached with private key and ciphertext. Moreover, this scheme is divided into two types, key-policy ABE (KP-ABE) schemes and ciphertext-policy ABE (CP-ABE) schemes. In the former, the private key is related to designated policies, while the ciphertext is labeled by some attributes. The user decrypts this ciphertext successfully unless these access policies are met by some attributes of such ciphertext, which reflects the permission of this user. On the contrary, in the latter, the ciphertext is associated with access policy, while some attribute sets are embedded into private key. CP-ABE scheme shows some requirements for the decryptor. In the cloud-assisted WBAN, the physiological data are stored on the cloud storage server (CSS), and shared among the authorized DUs. Consequently, it is more practical to adopt CP-ABE scheme to support confidentiality and access control in the cloud-assisted WBAN. Unfortunately, in the CP-ABE scheme, there is a shortcoming that the overhead is expensive due to the complexity of access structure in the phase of decryption, which impedes the application of ABE in IoTs device with limited resource.

For decreasing the computation overhead of decryption burdened on the DU, the concept of outsourced decryption was presented. Concretely, a ciphertext and a transformation key are given to CSS, and it transforms this ciphertext into a partial one, rather that is directly decrypted by the DU. The user only spends a little cost in accessing the plaintext from this partial ciphertext. Nevertheless, the validity of this transformed ciphertext cannot be ensured for an untrusted CSS. Some curious CSS may distort and tamper the transformed ciphertext. Therefore, the verifiability of the transformed ciphertext is necessary for the outsourced decryption ABE.

Moreover, the blockchain technique is a desirable method of resisting the data tampering as well. Blockchain technology is a backbone of the Bitcoin cryptocurrency, which is considered as a peer-to-peer distributed ledger technology to record data. The distinguishing features of this technology are decentralized maintenance, secure transporting and accessing the data as well as anti-tamper and undeniability. Taking blockchain into outsourced decryption ABE protocol, the ciphertext, the partial ciphertext, the transformation key, and other important parameters are encapsulated into a block chronologically, which avoids to be tampered from any entity, including the inside and outside adversary.

At the same time of enjoying the convenience, the cloud-assisted IoTs also suffers from the huge network latency, the massive data, and other various drawbacks. To avoid these drawbacks, one of the preeminent technique measure is fog computing. As shown in Figure 1, fog computing is presented for extending the cloud service to the edge of the IoTs, which promotes the resources and services to be closer to the IoTs devices. In the face of the explosion of data in IoTs, fog computing enables to provide small latency and real-time application.

**Related works**

ABE is a popular topic that enjoys the confidentiality and fine-grained access control. However, the weakness of original ABE scheme is that it needs some expensive operations in decryption, and the overhead is related to the complexity of access structure. Green et al. introduced the model of ABE with outsourced computing to reduce the computational cost in decryption, which transformed the decryption operation to CSS and reduced the overhead of the DU significantly. Unfortunately, the correctness of transformed ciphertext in Green et al. cannot be checked. Lai et al. presented a verifiability ABE protocol with outsourced...
decryption to verify the validity of the transformed ciphertext. To improve the efficiency, Lin et al.\textsuperscript{27} combined an attribute-based key encapsulation mechanism (KEM), a commitment protocol, and a symmetric key encryption scheme to achieve efficient verifiability. Moreover, they also put forward a unified model for outsourced decryption ABE with verifiability. Qin et al.\textsuperscript{28} encrypted the data in symmetric encryption, and this symmetric key is encrypted under ABE scheme. By comparing the hash values, this protocol realized the verification of the outsourced ciphertext in correctness. Mao et al.\textsuperscript{29} designed an improved verifiability ABE protocol with outsourced decryption to cut down the size of ciphertext and computational cost obviously, which committed to such plaintext by means of a random parameter. The scheme in Li et al.\textsuperscript{30} gave a novel verifiable outsourced decryption of ABE scheme that the size of ciphertext is constant, which not only verified the validity of transformed ciphertext, but also made the overhead be irrelevant to the complexity of access structure. Li et al.\textsuperscript{31} introduced an ABE protocol with fully verifiable outsourced decryption as well, and all the users (including authorized and unauthorized) enabled to check the correctness of transformed ciphertext. Recently, the scheme in Li et al.\textsuperscript{32} demonstrated an verifiability ABE with outsourced computing in both the encryption and decryption phases. This protocol caused the cost of transformed key generation to be constant and shifted the burden on both the DO and user.

Furthermore, the blockchain technology is also employed to guarantee the validity of the outsourced data. If only encapsulated the vital parameters into a block, any entity (including the authorized user and trusted or curious authority from inside, and the unauthorized user and adversary from outside) could not tamper these data. Guo et al.\textsuperscript{33} encapsulated the electronic health records (EHRs) in blockchain to guarantee the validity in the attribute-based cryptography primitive, every patient endorsed a message according to his attribute for avoiding to reveal his or her privacy. For applying in distribution system, the protocol in Guo et al.\textsuperscript{34} demonstrated a multi-authority ABE for medical data. Taking advantage of the blockchain technique, the integrity of these private data in cloud is protected. Liu et al.\textsuperscript{35} adopted the CP-ABE to provide strong privacy preservation in data sharing. Moreover, the index of physiological data is stored in the blockchain, which ensured that such sensitive data could not be modified arbitrarily. The schemes\textsuperscript{36–39} are all focused on the integrity and correctness of the outsourced data in cloud depending on the blockchain technology.

Although ABE scheme with outsourced decryption reduces the cost significantly, the mass data processing from sensor nodes is still greatly hindering the application of resource-limited IoT devices. Taking cloud-fog architecture into consideration, fog node (FN) is likely to be a proxy that executes partial computation. With the assistance of FN, it will need less calculation cost on the resource-limited IoT device. In the environment of fog computing, Zuo et al.\textsuperscript{40} first presented the chosen-ciphertext attack (CCA)-secure model in ABE with outsourced decryption. Integrating CP-ABE and
searchable encryption, Miao et al.\(^4^1\) proposed an efficient fine-grained ciphertext searching system, which shifted partial computation overhead from the DU to the selected FN. Fan et al.\(^4^2\) introduced an access control scheme with multiple authorities for privacy preservation in the fog-assisted IoT architecture, which operated the verifiable outsourced decryption by FN and ensured a real-time application. Considering the computing capacity of the sensor node, Wang et al.\(^4^3\) presented a fine-grained access control with distributed outsourced computing, in which the receiver and sender just executed little calculation with the help of the FN.

**Contributions**

To this article, for preserving the privacy in WBAN, a lightweight verifiability CP-ABE protocol with outsourced decryption is presented. The contributions of our protocol are listed as following.

1. By adding verification algorithm in decryption, this scheme enjoys the verifiability of ciphertext to check the correctness by the DU. Moreover, depending on the blockchain technology, it encapsulates the important data into a block chronologically and protects these data from being tampered by inside and outside adversary.
2. The size of ciphertext is constant that is independent with the complexity of attributed set and access policy. Moreover, FN affords partial computation and storage task that cuts the cost of IoT device equipped by the DO.
3. Provided that the assumption of computational bilinear Diffie–Hellman (CBDH) holds, we formally prove this proposal is verifiable in the standard model, and selectively chosen-plaintext attack (CPA)-secure.
4. As for simulation and comparison, we implement our construction and demonstrate the result of performance measurement, which indicates a significant reduction on the bandwidth of communication and computation for every entity in this protocol.

**Organization**

The remaining paper is organized as follows. Section “Preliminaries” introduces some basic knowledges and concepts, such as the notions of bilinear map, security assumption and access structure, the definition and security model of verifiability CP-ABE scheme with outsourced decryption in this article. Section “The architecture of system model” describes the detailed characters in our system model. Section “Our construction” presents our concrete CP-ABE scheme with verifiable outsourced decryption for WBAN. Section “Security analysis” proves the security and verifiability of this proposal. Section “Performance evaluation” demonstrates the experimental results on the performance comparison with the related schemes. Finally, Section “Conclusion” states our conclusions of such article.

**Preliminaries**

In this part, some preliminary knowledges regarding the cryptographic primitives that our scheme depends on are introduced.

**Bilinear map**

Suppose that \((G, +)\) and \((G_T, \times)\) are bilinear cyclic groups with the prime order \(p\). A bilinear map \(\hat{e} : G \times G \rightarrow G_T\) possesses the following three properties:

1. **Bilinearity**: \(\forall P, Q \in G, \quad a, b \in \mathbb{Z}_p^*, \quad \hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}\) holds.
2. **Non-degeneracy**: It exists \(P, Q \in G\) such that \(\hat{e}(P, Q) \neq 1 \in G_T\).
3. **Computability**: \(\forall P, Q \in G\), it exists an efficient algorithm to calculate \(\hat{e}(P, Q)\).

**Complexity assumption**

Let \(G\) be a finite cyclic group with prime order \(p\), and \(a, b, c \in \mathbb{Z}_p^*\) be selected uniformly at random. The difficult problem underlying the security of our protocol are shown as below.

**Definition 1**

CBDH problem. Given a tuple of elements \(\{A = aP, B = bP, C = cP\} \in G^3\), the CBDH problem in \((p, G, G_T, \hat{e})\) is to calculate the bilinear pairing \(\hat{e}(P, P)^{abc}\).

The CBDH assumption in \((p, G, G_T, \hat{e})\) is that there is no probabilistic polynomial-time (PPT) algorithm \(A\) to solve CBDH problem successfully with non-negligible advantage. The advantage of \(A\) is defined as

\[
\Pr[A(p, G, G_T, \hat{e}, A, B, C) = \hat{e}(g, g)^{abc}]
\]

where this probability is over the randomly chosen tuple of \((p, a, b, c)\).

**Access structure**

**Definition 2**

Access structure. Suppose that \(\{P_1, P_2, \ldots, P_n\}\) is a set of parties. There is a monotone collection \(\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}}\), where if \(B \in \mathbb{A}, B \subseteq C, C \in \mathbb{A}\) for any
B and C. Moreover, the access structure \( \mathcal{A} \) (respectively, monotone access structure) is called a collection (respectively, monotone access structure) of non-empty subsets of \( \{P_1, P_2, \ldots, P_n\} \), that is, \( \mathcal{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}} \setminus \{\emptyset\} \). Hence, the set belonging to \( \mathcal{A} \) is an authorized set. Otherwise, it is unauthorized.

Formal definition of CP-ABE with outsourced decryption

The CP-ABE scheme with outsourced decryption consists of seven algorithms as follows.

- **Setup** \( 1^k \rightarrow (PK, MSK) \): This algorithm inputs security parameter \( 1^k \), and then it outputs the public parameters \( PK \) and master secret key \( MSK \) of this system.
- **KeyGen** \( (PK, MSK, \mathcal{A}) \rightarrow SK_{\mathcal{A}} \): This algorithm inputs the public parameters \( PK \), master secret key \( MSK \), and an attribute set \( \mathcal{A} \). Then, it returns \( SK_{\mathcal{A}} \) as a private key for \( \mathcal{A} \).
- **Encrypt** \( (PK, M, \mathcal{A}) \rightarrow CT \): This algorithm inputs public parameters \( PK \), a message \( M \) and an access policy \( \mathcal{A} \), and then it returns the ciphertext \( CT \) of \( M \) as an answer.
- **Decrypt** \( (PK, SK_{\mathcal{A}}, CT) \rightarrow M \): This algorithm inputs the public parameters \( PK \), the private key \( SK_{\mathcal{A}} \) for \( \mathcal{A} \) and the ciphertext \( CT \), and then it returns \( M \) as an answer if \( SK_{\mathcal{A}} \) satisfies the access structure \( \mathcal{A} \).
- **GenTKout** \( (PK, SK_{\mathcal{A}}) \rightarrow (TK_{\mathcal{A}}, RK_{\mathcal{A}}) \): This algorithm inputs the public parameters \( PK \) and the private key \( SK_{\mathcal{A}} \) for attribute set \( \mathcal{A} \), and then it returns a transformation key \( TK_{\mathcal{A}} \) and a retrieving key \( RK_{\mathcal{A}} \) correspondingly as an answer.
- **Transformout** \( (PK, CT, TK_{\mathcal{A}}) \rightarrow CT' \): This algorithm inputs the public parameters \( PK \), the ciphertext \( CT \), and the transformation key \( TK_{\mathcal{A}} \) for \( \mathcal{A} \), and then it returns a partial ciphertext \( CT' \) as an answer.
- **Decryptout** \( (PK, CT, CT', RK_{\mathcal{A}}) \rightarrow M \): This algorithm inputs the public parameters \( PK \), the ciphertext \( CT \), the partial ciphertext \( CT' \), and the retrieving key \( RK_{\mathcal{A}} \), and then returns message \( M \) as an answer.

**Security model for CP-ABE with outsourced decryption**

**Confidentiality.** As the traditional CCA-secure does not permit any changes on bits of ciphertext, which is not suitable for the above model of CP-ABE with outsourced decryption. Thus, it proposes the selectively CPA-secure model in the following game between a challenge \( C \) and an adversary \( A \).

- **Init:** The adversary \( A \) submits \( \mathcal{A}^* \) as a challenge access policy.

**Setup:** The challenger \( C \) selects a security parameter \( 1^k \) for executing **Setup**, and then it returns the public parameters \( PK \) to \( \mathcal{A} \) and keeps master secret key \( MSK \) secretly.

**Query Phase 1:** Challenger \( C \) maintains an empty list \( L \) and a set \( E \). Adversary \( A \) issues two queries as below.

1. **Private-Key-Extraction:** Adversary \( A \) queries this oracle on the attribute set \( \mathcal{A} \), and the challenger \( C \) executes **KeyGen** and sets \( E = E \cup \{\mathcal{A}\} \). It outputs the private key \( SK_{\mathcal{A}} \) to \( \mathcal{A} \), and it cannot make this query for the private key \( SK_{\mathcal{A}} \) that satisfies the challenge access structure \( \mathcal{A}^* \).

2. **Transformation-Key-Extraction:** Adversary \( A \) launches this query on attribute set \( \mathcal{A} \). The challenger searches \( \{\mathcal{A}, SK_{\mathcal{A}}, TK_{\mathcal{A}}, RK_{\mathcal{A}}\} \) from the list \( L \). If such tuple exists, \( C \) outputs \( TK_{\mathcal{A}} \) to \( \mathcal{A} \). Otherwise, the challenger executes **KeyGen** and **GenTKout** and stores the generated tuple \( \{\mathcal{A}, SK_{\mathcal{A}}, TK_{\mathcal{A}}, RK_{\mathcal{A}}\} \) in the list \( L \). At last, it returns transformation key \( TK_{\mathcal{A}} \) to \( \mathcal{A} \). In addition, if it has queried **Private-Key-Extraction** based on \( \mathcal{A} \), \( A \) is forbidden to make queries on **Transformation-Key-Extraction** for the same set \( \mathcal{A} \).

**Challenge:** Adversary \( A \) submits two messages \( M_0 \) and \( M_1 \) with the same length, and a challenge access policy \( \mathcal{A}^* \) that cannot be satisfied by \( \mathcal{A} \). \( C \) randomly selects \( b \in \{0, 1\} \) and calculates \( CT^* = \text{Encrypt}(PK, M_b, \mathcal{A}^*) \). After that, \( C \) returns the challenge ciphertext \( CT^* \) to \( A \).

**Query Phase 2:** The adversary continues to make the same queries on **Private-Key-Extraction** and **Transformation-Key-Extraction** as in Query Phase 1. However, the private key should not meet the challenge access policy \( \mathcal{A}^* \).

**Guess:** Adversary \( A \) returns its guess \( b' \in \{0, 1\} \) on \( b \).

If \( b' = b \), \( A \) wins the game.

The advantage of \( A \) in this game is defined as

\[
\text{Adv}^{\text{Con}_{\text{ABEout}, A}}_{\text{ABEout}, A}(1^k) = \Pr[b' = b] - \frac{1}{2}
\]

**Definition 3.** This verifiability CP-ABE protocol with outsourced decryption is selectively CPA-secure if the advantage of all the PPT adversaries is negligible in the above security model.

**Verifiability.** The verifiability for CP-ABE protocol with outsourced decryption is proposed by the interaction between adversary and challenger in the following.
\textbf{Init:} Adversary $A$ submits $A^*$ as a challenge access policy.

\textbf{Setup:} Challenger $C$ operates $\text{Setup}$ to generate the public parameters $PK$ and the master secret key $MSK$. After that, it returns $PK$ to adversary.

\textbf{Query Phase 1:} Adversary queries on $\text{Private-Key-Extraction}$ and $\text{Transformation-Key-Extraction}$ as in \textit{Query Phase 1} of the above security game.

\textbf{Challenge:} Adversary $A$ submits a message $M^*$ and a challenge access structure $A^*$ to $C$, it calculates $CT^* = \text{Encrypt}(PK, M^*, A^*)$ and responses it to $A$ as a challenge ciphertext.

\textbf{Query Phase 2:} The adversary adaptively launches the query in \textit{Query Phase 1}.

\textbf{Output:} Adversary $A$ returns attribute set $\text{Att}^*$ and transformed ciphertext $CT^*_{\text{out}}$. We suppose that the tuple $(\text{Att}^*, SK_{\text{Att}^*}, TK_{\text{Att}^*}, RK_{\text{Att}^*})$ is included in the list $L$. Otherwise, $C$ generates this tuple by querying on $\text{Private-Key-Extraction}$ and $\text{Transformation-Key-Extraction}$. $A$ wins this game if $\text{Decrypt}_{\text{out}}(PK, CT^*, CT^*_{\text{out}}, RK_{\text{Att}^*}) \in \{M^*, \bot\}$.

Moreover, the advantage of $A$ in above model is defined as

\[
\text{Adv}_{\text{ABE}_{\text{out}}}(A^{1}) = \Pr[\text{Decrypt}_{\text{out}}(PK, CT^*, CT^*_{\text{out}}, RK_{\text{Att}^*}) \in \{M^*, \bot\}]
\]

\textbf{Definition 4}

\textit{Verifiability.} This CP-ABE scheme with outsourced decryption is verifiable, if the advantage $\text{Adv}_{\text{ABE}_{\text{out}}}(A^{1})$ for all PPT adversaries $A$ is negligible.
Table 1. Notions and meanings.

| Notions   | Meanings                                                                 |
|-----------|---------------------------------------------------------------------------|
| $G$       | The additional cyclic group with prime order $p$.                         |
| $G_T$     | The multiplicative cyclic group with prime order $p$.                     |
| $P$       | The generator of $G$.                                                     |
| $H_i$     | The collision resistance hash function $i = 1, 2$.                        |
| $PK$      | The public parameters of this system.                                    |
| $MSK$     | The master secret key of this system.                                     |
| $Att$     | The authorized attribute set.                                            |
| $I$       | The number of attribute in $Att$.                                         |
| $SK_{Att}$| The private key of user with attribute $Att$.                             |
| $TK_{Att}$| The transformation key of user with attribute $Att$.                     |
| $RK_{Att}$| The retrieving key of user with attribute $Att$.                         |

blockchain will never be distorted by anyone. Specifically, according to this mode, any variations on this key or ciphertext would change the corresponding hash value in the blockchain, and all the entities in this system will perceive these variations. Consequently, blockchain is beneficial for protecting integrity in a verifiable and permanent method from inside and outside adversary.

CSS owns considerable storage space and calculation capability, which supplies outsourced storage and computation service to the customers. In this system, CSS is responsible for storing the outsourced data from DO in the form of ciphertext, which could be accessed by DU.

$TA$ is a system parameter generator center, whose responsibility is generating the public parameters $PK$ and master secret key, and distributing secret key to the registered DO and DU. Furthermore, it executes Setup and KeyGen algorithms as well.

$DU$ represents the medical staff for diagnosis, the researcher for medical science and the relatives for solicitude, and so on. Each of registered user accepts the attribute secret key relying on its characteristics. If their attributes meet the access policy of DO, DU enables to access his or her medical data. In detail, after receiving the partial encrypted medical file (i.e. the transformed ciphertext $CT'$) from FN, DU downloads the ciphertext $CT$ from CSS for verification and decryption by taking advantage of attribute secret key and transformation key pair to achieve the accurate plaintext medical data.

**Our construction**

In this section, it lists some employed notations in Table 1. Furthermore, it designs seven concrete algorithms that are demonstrated in the following.

$Setup(1^k) \rightarrow (PK, MSK)$: $TA$ takes $1^k$ as input, it selects a bilinear map $\hat{e} : G \times G \rightarrow G_T$, where $G$ and $G_T$ are additional and multiplicative cyclic groups with prime order $p$. Let $P$ be a generator of $G$, $TA$ chooses $\alpha, \beta \in Z_p^*$ randomly and calculates $A = \hat{e}(P, P)^\alpha, B = \hat{e}(P, P)^\beta = (1/\beta)P$. Then, it picks two collision resistance hash functions $H_1 : \{0, 1\}^* \rightarrow Z_2^*$ and $H_2 : G_T \rightarrow \{0, 1\}^*$. At last, $TA$ returns the public parameters $params = (\hat{e}, G, G_T, P, A, B, B', B, H_1, H_2)$ and master secret key $MSK = (\alpha, \beta)$.

$KeyGen(PK, MSK, Att) \rightarrow SK_{Att}$: Considering that II is linear secret sharing scheme (LSSS) for an access policy $\Lambda, \Lambda_0$ $Att$ is an authorized attribute set and $I = |Att|$. Then, it obtains shares $\{a_i\}_{i \in I}$ of the secret $\gamma \in Z_2^*$, and $\gamma = \sum_{i \in I} a_i t_i$ denotes the party corresponding to shares $\{a_i\}_{i \in I}$ as $Att_i \in Att$, where $\{t_i \in Z_p\}_{i \in I}$ is the attribute underlying $Att_i$. For the different $Att$ and $Att'$, $(\gamma = \sum_{i \in I} a_i t_i)_{\forall Att_i \neq (\gamma' = \sum_{i \in I} a_i t'_i)_{\forall Att_i'}}$ holds. $TA$ computes $K_1 = ((\alpha + \gamma)/\beta)P$, $K_2 = \gamma P$, and sends $(SK_{Att} = (K_1, K_2))$ to DU with attribute $Att$.

$Encrypt(PK, \Lambda, \Lambda_0) \rightarrow CT$: To encrypt $M \in \{0, 1\}^*$, it first selects $M \in \{0, 1\}^*$ and $s, s' \in Z_p^*$. Next, DO computes

$$\tilde{C} = H_1(M)H_1(M)P, C_1 = M \oplus H_2(A'), C_2 = sB, C_3 = sP, C_1' = M \oplus H_2(A'), C_2' = s' B, C_3' = s' P.$$  

After that, it returns the ciphertext

$$CT = (\Lambda, \tilde{C}, C_1, C_2, C_3, C_1', C_2', C_3')$$

$Decrypt(PK, SK_{Att}, CT) \rightarrow M$: Input the private key $SK_{Att}$ and ciphertext $CT$, $DU$ calculates $(D, D')$ as follows

$$D = \hat{e}(C_2, K_1) / \hat{e}(C_3, K_2) = \hat{e}(sB, ((\alpha + \gamma)/\beta)P) / \hat{e}(sP, \gamma P)$$

$$= \hat{e}(P, P)^{\alpha + \gamma} / \hat{e}(P, P)^{\gamma} = \hat{e}(P, P)^\alpha$$

$$D' = \hat{e}(C_2', K_1) / \hat{e}(C_3', K_2) = \hat{e}(s' B, ((\alpha + \gamma)/\beta)P) / \hat{e}(s' P, \gamma P)$$

$$= \hat{e}(P, P)^{\alpha + \gamma} / \hat{e}(P, P)^\gamma = \hat{e}(P, P)^\alpha$$

Then, it computes $M = C_1 \oplus H_2(D)$ and $\tilde{M} = C_1 \oplus H_2(D')$. At last, if $\hat{e}(\tilde{C}, P) = \hat{e}(H_1(M)B, H_1(M)B')$ holds, it outputs the message $M$. Otherwise, outputs $\perp$ and aborts.

$GenTK_{Att}(PK, SK_{Att}) \rightarrow (TK_{Att}, RK_{Att})$: This algorithm takes the private key $SK_{Att}$ as input, DU generates its transformation key pair by choosing $t \in Z_p^*$ randomly and computing $TK_{Att} = (K'_t = (1/t)K_1,$
$K'_2 = (1/i)K_2$ as a pair of transformation key, and $RK_{\text{Att}} = t$ as a retrieving key. 

$\text{Transform}_{\text{out}}(PK, CT, RK_{\text{Att}}) \to CT'$: Given ciphertext $CT$ and transformation key $RK_{\text{Att}}$, FN computes as belows

$$\hat{e}(C_2, K'_2) = \frac{\hat{e}(s\beta P, ((\alpha + \gamma)/t)\beta P)}{\hat{e}(sP, (\gamma/i)P)} = \frac{\hat{e}(P, P)^{(a + \gamma)/t}}{\hat{e}(P, P)^{(a/i)T}} \Rightarrow \hat{e}(P, P)^{a/t} = T$$

$$\hat{e}(C_3, K'_3) = \frac{\hat{e}(s^{\prime} \beta P, ((\alpha + \gamma)/t)\beta P)}{\hat{e}(sP, (\gamma/i)P)} = \frac{\hat{e}(P, P)^{(a + \gamma)/t}}{\hat{e}(P, P)^{(a/i)T'}} \Rightarrow \hat{e}(P, P)^{a/t} = T'$$

Outputting the transformed ciphertext as 

$$CT' = (\hat{T} = \hat{C}, T, T').$$

$\text{Decrypt}_{\text{out}}(PK, CT, CT', RK_{\text{Att}}) \to M$: DU downloads the ciphertext $CT$ from CCS and checks whether $\hat{T} = \hat{C}$. If not, it outputs $\bot$ and aborts. Otherwise, computes $M = C_1 \oplus H_2(T')$ and $\hat{M} = C'_2 \oplus H_2(T'')$. Then, it verifies $\hat{e}(\hat{T}, P) = \hat{e}(H_1(M)B, H_1(M)B')$ holds or not. If it is, it returns the message $M$. Otherwise, outputs $\bot$ and aborts.

**Security analysis**

In this part, it proves that this protocol is selectively CPA-secure and verifiable in the standard model.

**Theorem 1.** Provided that the protocol in Waters\textsuperscript{17} is selectively CPA-secure, our proposal is selectively CPA-secure as well.

**Proof.** This protocol is selectively CPA-secure under the following two games.

**Game$_0$:** It is the original selectively CPA-secure game in CP-ABE protocol.

**Game$_1$:** Challenger picks $\hat{C} \in G$ at random, and keeps the rest of challenge ciphertext to generate $CT = (\hat{a}, \hat{C}, C_1, C_2, C_3, C'_2, C'_3)$ as in Game$_0$.

The proof of this theorem consists of the following two lemmas. Lemma 1 proves the indistinguishability between Game$_0$ and Game$_1$, while Lemma 2 demonstrates that the advantage of adversary in Game$_1$ is negligible. Consequently, it concludes that the advantage in Game$_0$ is also negligible.

**Lemma 1.** Assume that the scheme in Waters\textsuperscript{17} is selectively CPA-secure, Game$_0$ and Game$_1$ are computationally indistinguishable.

**Proof.** Suppose that an adversary $A$ distinguishes Game$_0$ and Game$_1$ with non-negligible probability, and an simulator $B$ attacks the scheme\textsuperscript{17} under the selective CPA security model with non-negligible advantage.

$C$ is a challenger in the selective CPA security model in Waters\textsuperscript{17}. A simulator interacts with $A$ by executing the following algorithms.

**Init:** The adversary $A$ delivers $\hat{a}^*$ to $B$ as a challenge access structure. Then, the simulator gives this policy to $C$. The challenger feeds back the public parameters in additional group $PK' = \{p, G, G_T, \hat{e}, P, aP, \hat{e}(P, P)^t, \{T, sT\}_G\}$ of Waters\textsuperscript{17}.

**Setup:** $B$ chooses $x, y \in Z_p$ at random and gets $B = xP, B' = yP$. Moreover, it chooses $H_1: \{0, 1\} \to Z_p^*$ and $H_2: G_T \to \{0, 1\}^*$ as two collision-resistant hash functions. $B$ transmits $PK = (\hat{e}, G, G_T, p, P, A, B, B', H_1, H_2)$ to $A$.

**Query Phase 1:** The adversary $A$ makes a private key query on attribute set $Att$. Simulator queries Private-Key-Extraction with $C$ on $Att$, and then accesses the private key $SK_{\text{Att}}$. At last, $B$ returns the private keys $SK_{\text{Att}}$ to adversary.

**Challenge:** $A$ submits two challenge plaintexts $M_0$ and $M_1$ with equal size to the simulator. It picks a value $\eta \in \{0, 1\}$ and two message $M_0, M_1 \in \{0, 1\}^*$ randomly. Then, it sends $\langle M_0, M_1, \hat{a}^* \rangle$ to the challenger. $C$ selects random $\theta \in \{0, 1\}$, encrypits the message $M_\theta$ under $PK'$ and $\hat{a}^*$ according to the encryption in Waters\textsuperscript{17}. After that, the ciphertext $CT' = (\hat{a}^*, C_1, C_2, C_3)$ is sent to $B$. The simulator chooses $s \in Z_p$ randomly and computes $\hat{C} = H_1(M_0)H_2(M_1)pP, C_1 = M_0 \oplus H_2(A'), C_2 = sB$ and $C_3 = sP$. At last, $B$ transmits the challenge ciphertext $CT'' = (\hat{a}^*, \hat{C}, C_1, C_2, C_3)$ to $A$.

**Query Phase 2:** $A$ queries on Private-Key-Extraction adaptively as in Query Phase 1, and $B$ responds it as before.

**Guess:** $A$ returns its guess $\eta' \in \{0, 1\}$ for $B$, and it outputs $\eta'$ as its guess for $\theta$.

Provided that $\eta = \theta$, $B$ has simulated Game$_0$ appropriately. Otherwise, $B$ has appropriately simulated Game$_1$ with non-negligible advantage, we design an algorithm $B$ as a simulator who attacks the selectively CPA-secure protocol with non-negligible advantage.

**Lemma 2.** Provided that the scheme in Waters\textsuperscript{17} is selectively CPA-secure, the adversary’s advantage in Game$_1$ is negligible.
Proof. Suppose that the advantage of $A$ in Game$_1$ is non-negligible. Besides, there is an algorithm $B$ as a simulator who attacks the protocol $^{17}$ in the selectively CPA-secure model with a non-negligible advantage.

Assume that $C$ is a challenger in selective CPA-security model, $B$ interacts with $A$ by running the algorithms as below.

Init: $A$ transmits a challenge access structure $\lambda^*$ to $B$. Simulator also gives $\lambda^*$ to $C$. The challenger $C$ delivers the public parameters in the additional group $PK' = \{p, G,GT, e, p, aP, e(P,P)^0, \{T_i = s_iP\}_s\}$ of Waters$^{17}$ back to simulator.

Setup: Simulator picks random $x, y \in Z_p$, computes $B = xp, B' = yp$, and there are two hash functions $H_1: \{0,1\}^* \rightarrow Z_p$ and $H_2: GT \rightarrow \{0,1\}^*$ with collision-resistant. After that, $B$ transmits $PK = \langle e, G, GT, p, A, B, B', H_1, H_2 \rangle$ to adversary.

Query Phase 1: $A$ adaptively issues the private key query on $Att$. Simulator receives a private key $SK_{Att}$ by querying Private-Key-Extraction with $C$ on $Att$. Then, the simulator returns the private key $SK_{Att}$ to adversary.

Challenge: The adversary $A$ submits two equal size messages $M_0$ and $M_1$. Simulator sends $\langle M_0, M_1, \lambda^* \rangle$ to $C$. After that, $C$ picks $\theta \in \{0,1\}$ at random, encrypts $M_\theta$ under $PK'$ and $\lambda^*$ as the encryption in Waters$^{17}$. Then, it gives the result ciphertext $CT' = \langle \lambda^*, C_1, C_2, C_3 \rangle$ back to $B$. The simulator $B$ chooses $s' \in Z_p^*$, $M \in \{0,1\}^*$ and $C \in GT$ randomly, and calculates $C'_1 = M \oplus H_2(A')$, $C'_2 = s'B$, $C'_3 = s'P$. At last, $B$ transmits $CT = \langle \lambda^*, C_1, C_2, C_3, C'_1, C'_2, C'_3 \rangle$ to $A$ as a challenge ciphertext.

Query Phase 2: Adversary queries on Private-Key-Extraction adaptively as in Query Phase 1. Simulator responds this query correspondingly.

Guess: Finally, adversary returns a guess $\eta' \in \{0,1\}$ to simulator, it also takes $\eta'$ as its guess for $\theta$.

Obviously, $B$ has simulated Game$_1$ appropriately. Provided that the advantage of adversary in Game$_1$ is non-negligible, $B$ attacks selectively CPA-secure protocol$^{17}$ with non-negligible advantage.

In conclusion, these two lemmas show that the first four algorithms in our protocol as basic CP-ABE protocol is selectively CPA-secure. After that, in the following theorem, we will prove that if basic CP-ABE protocol is selectively CPA-secure, the whole protocol is selectively CPA-secure as well.

Theorem 2. Provided that basic CP-ABE protocol is selectively CPA-secure, this protocol with outsourced decryption is selectively CPA-secure as well.

Proof. Suppose that, in the selectively CPA-secure model, the advantage of $A$ is non-negligible. $B$ acts as a simulator to attack the basic CP-ABE scheme with non-negligible advantage.

$C$ is a challenger in the selectively CPA-secure model of basic CP-ABE protocol. Simulator interacts with $A$ according to the algorithms as below.

Init: The adversary $A$ gives $\lambda^*$ to $B$ as a challenge access structure. Then, simulator transmits this structure to $C$. Challenger outputs the public parameters $PK = \langle e, G, GT, p, A, B, B', H_1, H_2 \rangle$ of basic CP-ABE scheme to $B$.

Setup: Simulator gives the above parameters $PK$ to $A$.

Query Phase 1: $B$ maintains an empty list $L$ as well as a set $E$. $A$ launches the following queries adaptively.

Private-Key-Extraction: Based on the attribute set $Att$, $B$ queries the key generation oracle to receive the private key $SK_{Att}$. After that, $B$ sets $E = E \cup \{Att\}$ and responds a private key $SK_{Att}$ to $A$.

Transformation-Key-Extraction: Based on the attribute set $Att$, $B$ searches $\langle Att, SK_{Att}, TK_{Att} \rangle$ from the list $L$. And outputting the transformation key $TK_{Att}$ to the adversary $A$ if it exists. Otherwise, $B$ picks $u, v \in Z_p^*$, computes $K'_1 = \langle (u + v)/\beta\rangle$, $P, K'_2 = vP$, and $B$ stores this tuple $\langle Att, *, TK_{Att} = (Att, K'_1, K'_2), u \rangle$ into $L$ and transmits it to $A$.

Note that, the simulator $B$ is unable to access the actual retrieving key $RK_{Att} = \alpha/\eta$. It computes the following:

$$\begin{align*}
ed(C_2, K'_1) &= \frac{\tilde{e}(sP, \frac{v+u}{\beta})P}{\tilde{e}(sP, vP)} = \frac{\tilde{e}(e(P,P)^{u+v})}{\tilde{e}(e(P,P)^{uv})} = T
C_1 \oplus H_2(T^{RK_{Att}}) = M \oplus H_5(\tilde{e}(e(P,P)^{uv})H_2(\tilde{e}(e(P,P)^{uv})) = M
\end{align*}$$

Challenge: Adversary submits two equal size messages $\langle M_0, M_1 \rangle$ and $\lambda^*$ as a challenge access policy. $B$ transmits the tuple $\langle M_0, M_1, \lambda^* \rangle$ to challenger to compute $CT^*$ on $M_\eta$ as a challenge ciphertext, where $\eta \in \{0,1\}$. After that, $B$ returns $CT^*$ to $A$.

Query Phase 2: $A$ makes a private key query adaptively as in Query Phase 1. $B$ returns the answer correspondingly.

Guess: $A$ returns a value $\eta'$ as its guess on $\eta$, and $B$ responds $\eta'$ as well.

Provided that the guess $\eta'$ of $A$ in this protocol is correct, the guess in basic CP-ABE scheme is also
correct. Therefore, it concludes that if $A$ enables to attack the proposal with non-negligible advantage, in the selectively CPA-secure model, there is a simulator $B$ that attacks basic CP-ABE protocol with non-negligible advantage.

**Theorem 3.** Provided that the CDH assumption defined in Definition 1 holds, this CP-ABE protocol with outsourced decryption is verifiable.

**Proof.** Assume that $A$ attacks verifiability of this scheme with non-negligible advantage. In addition, $B$ acts as a simulator that enables to solve the CDH problem with non-negligible advantage.

Setup: Simulator $B$ randomly picks $\alpha, x, y \in \mathbb{Z}_p^*$, let $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ and $H_2: G_T \rightarrow \{0,1\}^*$ be collision-resistant hash functions. After that, simulator defines the public parameters $PK = \langle \hat{e}, G, G_T, P, P, A = \hat{e}(P, P)^\beta, B = xP, B' = yP, H_1, H_2 \rangle$, and master secret key $MSK = \alpha$. It returns $PK$ to adversary.

Query Phase 1: $A$ makes some queries on $KeyGen(PK, MK, Att)$, $Encrypt(PK, CT, TK_{Att})$, $GenTK_{out}(PK, CT, TK_{Att})$ and $Decrypt(PK, SK_{Att}, CT)$ algorithms. As simulator possesses master secret key $MSK$, it is able to respond these queries properly.

Challenge: $A$ submits a message $M^*$ and a challenge access policy $\mathcal{h}$ to $B$. The simulator calculates the ciphertext $CT' = \langle \hat{T} = \hat{C}, T', T'' \rangle$. $A$ returns $CT' = \langle \hat{h}, C, C_1, C_2, C_3, C_4, C_5 \rangle$ to $A$, where $\hat{C} = H_1(M')H_1(M')P$ and $M' \in \{0,1\}^*$ is selected by the simulator at random. Note that, $B$ is forbidden to access the random parameter $s$.

Query Phase 2: Adversary launches the same query on private key as in Query Phase 1, and simulator responses as before.

Output: $A$ returns an attribute set $Att^*$ and the transformed ciphertext $CT'' = \langle \hat{T} = \hat{C}, T', T'' \rangle$. Simulator $B$ computes $C_1 \oplus H_2(T_{Att^*}) = M$ and $C_1 \oplus H_2(T_{Att^*}) = M$. $T_{Att^*}$ is a retrieving key for the attribute set $Att^*$ controlled by simulator $B$.

Furthermore, if $A$ wins the above game, $B$ has ability of computing

$$\left[ \frac{\hat{e}(C_2, K_1)}{\hat{e}(C_2, \gamma B')} \right]^\frac{1}{\beta} = \left[ \frac{\hat{e}(sxP, (\alpha + \gamma)P)}{\hat{e}(sxP, \gamma P)} \right]^\frac{1}{\beta} = \left[ \frac{\hat{e}(P, P)^{\alpha + \gamma}}{\hat{e}(P, P)^{\gamma \gamma}} \right]^\frac{1}{\beta} = \hat{e}(P, P)^{\gamma \gamma}$$

where $\alpha$ and $\gamma$ are controlled by the simulator $B$. Thus, $B$ solves the CDH problem, which is paradoxical. Therefore, this CP-ABE protocol with outsourced decryption is verifiable.

### Performance evaluation

In this section, it demonstrates the cost evaluation between this protocol and other related schemes from the aspects of communication and computation overhead.

#### Communication overhead

Let $|G|$ and $|G_T|$ be the element length in the additional cyclic group $G$ and the multiplicative cyclic group $G_T$, respectively. $N$ denotes the number of attribute, and $L_M$ denotes the length of message. For scheme in Qin et al., $L_{SE}$ is denoted to the length of a symmetric encryption ciphertext, and $L_{VK}$ is the length of a verification key. Moreover, for protocol in Mao et al., $L_{CM}$ is represented to the length of commit on a message. As shown in Table 2, it compares the communication cost in the phase of $KeyGen, Encrypt, GenTK_{out}$, and $Transform_{out}$. In the algorithm of $KeyGen$, the communication overhead between TA and DU is $2|G|$. In the algorithm of $Encrypt$, the communication overhead between DO and CSS in our scheme is $(5|G| + 2L_M)$. In the phase of transformation key generation, the overhead in communication is also $2|G|$. Meanwhile, in the algorithm of $Transform_{out}$, the communication overhead between FN and DU is $(|G| + 2|G_T|)$. To sum up, from this table, we can conclude that the size of the transmitted data with constant length in every

| Schemes | KeyGen | Encrypt | GenTK_{out} | Transform_{out} |
|---------|--------|---------|-------------|-----------------|
| Lai et al.$^{19}$ | $(N + (N + 2)|G_T|$ | $(N + (N + 3)|G| + 2|G_T|)$ | $N + (N + 2)|G_T|$ | $|G| + 4|G_T|$ |
| Qin et al.$^{38}$ | $(N + 2)|G_T|$ | $(2N + 1)|G| + |G_T| + L_{SE} + L_{VK}$ | $(N + 2)|G_T|$ | $2|G_T| + L_{SE} + L_{VK}$ |
| Mao et al.$^{29}$ | $(N + (N + 2)|G_T|$ | $(2N + 2)|G| + L_M + L_{CM}$ | $N + (N + 2)|G_T|$ | $|G| + |G_T| + L_M + L_{CM}$ |
| Li et al.$^{30}$ | $2|G_T|$ | $5|G| + 2|G_T|$ | $2|G_T|$ | $|G| + 4|G_T|$ |
| Li et al.$^{31}$ | $(N + (N + 2)|G_T|$ | $(2N + 2)|G| + L_M$ | $N + (N + 2)|G_T|$ | $2|G_T| + |G| + L_M$ |
| Zuo et al.$^{40}$ | $(2N + 1)|G_T|$ | $(N + 2)|G| + 2L_M$ | $(2N + 1)|G| + 2L_M$ | $2|G| + 2L_M$ |
| Ours | $2|G|$ | $5|G| + 2L_M$ | $2|G|$ | $|G| + 2|G_T|$ |
phase is the smallest, which indicates a significant advantage of our protocol in communication.

**Computation overhead**

We implement our scheme with previous works depending on pairing-based cryptography (PBC) library, the operations are executed on the 64-bit Windows 10 operation system, 2.20-GHz Intel Core i5-5200u CPU with 8-GB RAM. Concretely, we select the Type A elliptic curve parameter with the 160-bit order. Figures 3–7 demonstrate the experimental results in the average time of 100 operations. Specifically, in Figure 3, because of integrating the attribute into $g$, it is obvious that the overhead of key generation in this protocol is constant and more efficient than others. We compare the time of encryption spent among these four schemes in Figure 4, which shows that our cost is much less than others for the reason that the overhead in this protocol is not increased with the quantity of attribute embedded in the access policy. Figures 5 and 7 show that the cost of decryption and outsourced decryption, respectively. However, the overhead of our proposal is a little more than Li et al.’s protocol for the reason that it needs one more bilinear pairing operations in our verification algorithm. Finally, in Figure 6, it demonstrates that the operation cost of this proposal is equal to the scheme in Li et al. in the phase of transformation. Conclusions as a result, this protocol shows a better performance in the phases of KeyGen, Encrypt, Decrypt, Transformout, and Decryptout, respectively.

**Conclusion**

In this article, it presents a lightweight verifiable outsourced CP-ABE protocol for the typical WBAN in IoT, which enables a user to verify the correctness of the transformed ciphertext. The security is proven to be selectively CPA-secure, and the verifiability is reduced to CBDH assumption in the standard model. In addition, the complicated decryption operation is outsourced to the FN instead of being laid on the device of DU. As for the communication and computation.
overhead, they do not depend on the amount of attributes, which reduces the cost of the whole system greatly. Therefore, this scheme has some applications in the limited power devices, such as IoTs. Moreover, our scheme takes advantage of fog computing to provide low latency and real-time interactions, while the blockchain protects the public parameter and ciphertext from being tampered by the inside and outside adversary.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the National Key R&D Program of China under Grant 2017YFB0802000; the Natural Science Foundation of China under Grants 61802303, 61772418, and 61602378; the Key Research and Development Program of Shaanxi under Grant 2019KW-053; the Innovation Ability Support Program in Shaanxi Province of China under Grant 2017KJXX-47; the Natural Science Basic Research Plan in Shaanxi Province of China under Grants 2019JQ-866, 2018JZ6001, and 2016JM6033; the Research Program of Education Bureau of Shaanxi Province under Grant 19JK0803; the New Star Team of Xi’an University of Posts and Telecommunications under Grant 2016-02; the Fundamental Research Funds for the Central Universities under Grant GK201903005; and Guangxi Cooperative Innovation Center of Cloud Computing and Big Data under Grant YD1903.

ORCID iD
Rui Guo https://orcid.org/0000-0003-2603-2775

Figure 7. The cost of Decryptout algorithm.

References
1. International Telecommunication Union (ITU). Internet of Things global standards initiative, https://www.itu.int/en/ITU-T/sgi/iot/pages/default.aspx
2. Li X, Peng JY, Niu JW, et al. A robust and energy efficient authentication protocol for industrial internet of things. IEEE Internet Things J 2018; 5(3): 1606–1615.
3. Sun SF, Lyu C, Gu DW, et al. Towards efficient, secure, and fine-grained access control system in MSNs with flexible revocations. Int J Distrib Sens Netw 2015; 11: 857405.
4. Latré B, Brarr M, Moerman I, et al. A survey on wireless body area networks. Wirel Netw 2011; 17(1): 1–18.
5. Li X, Ibrahim MH, Kumari S, et al. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput Netw 2017; 129(2): 429–443.
6. Hu CQ, Li HJ, Hao Y, et al. Secure and efficient data communication protocol for wireless body area networks. IEEE Trans Multi-Scale Comput Syst 2016; 2(2): 94–107.
7. Mell PM and Grance T. The NIST definition of cloud computing (SP 800-145), 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
8. Zhang YH, Deng R, Zheng D, et al. Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. IEEE Trans Ind Inform 2019; 15: 5099–5108.
9. Zhang YH, Deng R, Liu XM, et al. Outsourcing service fair payment based on blockchain and its applications in cloud computing. IEEE Trans Serv Comput. Epub ahead of print 7 August 2018. DOI: 10.1109/TSC.2018.2864191
10. Sahai A and Waters B. Fuzzy identity-based encryption. In: Proceedings of the 24th annual international conference on theory and applications of cryptographic techniques (EUROCRYPT’05), Aarhus, 22–26 May 2005, pp.457–473. Berlin: Springer.
11. Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security (CCS’06), Alexandria, VA, 30 October–3 November 2006, pp.89–98. New York: ACM.
12. Ostrovsky R, Sahai A and Waters B. Attribute-based encryption with non-monotonic access structures. In: Proceedings of the 14th ACM conference on computer and communications security (CCS’07), Alexandria, VA, 28–31 October 2007, pp.195–203. New York: ACM.
13. Lewko A and Waters B. Unbounded HIBE and attribute-based encryption. In: Proceedings of the 30th annual international conference on theory and applications of cryptographic techniques (EUROCRYPT’11), Tallinn, 15–19 May 2011, pp.547–567. Berlin: Springer.
14. Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Proceedings of the 29th annual international conference on theory and applications of cryptographic techniques (EUROCRYPT’10), French Riviera, 30 May–3 June 2010, pp.62–91. Berlin: Springer.
15. Okamoto T and Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption. In: *Proceedings of the 30th annual conference on advances in cryptology (CRYPTO'10)*, Santa Barbara, CA, 15–19 August 2010, pp.191–208. Berlin: Springer.

16. Bethencourt J, Sahai A and Waters B. Ciphertext-policy attribute-based encryption. In: *Proceedings of the 2007 IEEE symposium on security and privacy (SP’07)*, Berkeley, CA, 20–23 May 2007, pp.321–334. New York: IEEE.

17. Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: *Proceedings of the 14th international conference on practice and theory in public key cryptography conference on public key cryptography (PKC’11)*, Taormina, 6–9 March 2011, pp.53–70. Berlin: Springer.

18. Green M, Hohenberger S and Waters B. Outsourcing the decryption of ABE ciphertexts. In: *Proceedings of the 20th USENIX conference on security (SEC’11)*, San Francisco, CA, 8–12 August 2011, pp.34–34. New York: ACM.

19. Lai JZ, Deng RH, Guan CW, et al. Attribute-based encryption with verifiable outsourced decryption. *IEEE Trans Inf Foren Sec* 2013; 8(8): 1343–1354.

20. Zhang YH, Deng RH, Liu XM, et al. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Inform Sciences* 2018; 462: 262–277.

21. Zhang Y and Wen JT. The IoT electric business model: using blockchain technology for the Internet of Things. *Peer Peer Netw Appl* 2017; 10(4): 983–994.

22. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf

23. Puliafito C, Mingozi E and Anastasi G. Fog computing for the internet of mobile things: issues and challenges. In: *Proceedings of the 2017 IEEE international conference on smart computing (SMARTCOMP’17)*, Hong Kong, 29–31 May 2017, pp.1–6. New York: IEEE.

24. Bonomi F, Milito R, Zhu J, et al. Fog computing and its role in the Internet of Things. In: *Proceedings of the first edition of the MCC workshop on mobile cloud computing (MCC’12)*, Helsinki, 17 August 2012, pp.13–16. New York: ACM.

25. Roca D, Milito R, Nemirovsky M, et al. Tackling IoT ultra large scale systems: fog computing in support of hierarchical emergent behaviors. In: Rahmani A, Liljeberg P, Preden JS, et al. (eds) *Fog computing in the Internet of Things*. Cham: Springer, 2018, pp.33–48.

26. Hu PF, Dhelimen S, Ning HS, et al. Survey on fog computing: architecture, key technologies, applications and open issues. *J Netw Compu Appl* 2017; 98: 27–42.

27. Lin SQ, Zhang R, Ma H, et al. Revisiting attribute-based encryption with verifiable outsourced decryption. *IEEE Trans Inf Foren Sec* 2015; 10(10): 2199–2130.

28. Qin BD, Deng RH, Liu SL, et al. Attribute-based encryption with efficient verifiable outsourced decryption. *IEEE Trans Inf Foren Sec* 2015; 10(7): 1384–1393.

29. Mao XP, Lai JZ, Mei QX, et al. Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption. *IEEE Trans Depend Secure* 2016; 13(5): 533–546.

30. Li JG, Sha FJ, Zhang YC, et al. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length. *Secur Commun Netw* 2017; 2017(2): 1–11.

31. Li JG, Wang Y, Zhang YC, et al. Full verifiability for outsourced decryption in attribute based encryption. *IEEE Trans Serv Comput*. Epub ahead of print 31 May 2017. DOI: 10.1109/TSC.2017.2710190

32. Li ZD, Li WM, Jin ZP, et al. An efficient ABE scheme with verifiable outsourced encryption and decryption. *IEEE Access* 2019; 7: 29023–29037.

33. Guo R, ShiHX, Zhao QL, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access* 2018; 6: 11676–11686.

34. Guo R, ShiHX, Zheng D, et al. Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system. *IEEE Access* 2019; 7: 88012–88025.

35. Liu JW, Li XL, Ye L, et al. BPDS: a blockchain based privacy-preserving data sharing for electronic medical records. In: *Proceedings of the 2018 IEEE global communications conference (Globecom’18)*, Abu Dhabi, United Arab Emirates, 9–13 December 2018. New York: IEEE.

36. Oliveira MT, Reis LHA, Carrano RC, et al. Towards a blockchain-based secure electronic medical record for healthcare applications. In: *Proceedings of the ICC 2019-2019 IEEE international conference on communications (ICC’19)*, Shanghai, China, 20–24 May 2019. New York: IEEE.

37. Rahman MDA, Hossain MS, Loukas G, et al. Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE Access* 2018; 6: 72469–72478.

38. Ferrag MA, Derdour M, Mukherjee M, et al. Blockchain technologies for the Internet of Things: research issues and challenges. *IEEE Internet Things* 2019; 6(2): 2188–2204.

39. Zhu LH, Wu YL, Gai KK, et al. Controllable and trustworthy blockchain-based cloud data management. *Future Gener Comput Syst* 2019; 91: 527–535.

40. Zuo C, Shao J, Wei YG, et al. CCA-secure ABE with outsourced decryption for fog computing. *Future Gener Comput Syst* 2018; 78: 730–738.

41. Miao YB, Ma JF, Liu XM, et al. Lightweight fine-grained search over encrypted data in fog computing. *IEEE Trans Serv Comput* 2019; 12: 772–785.

42. Fan K, Xu HY, Gao LX, et al. Efficient and privacy-preserving access control scheme for fog-enabled IoT. *Future Gener Comput Syst* 2019; 99: 134–142.

43. Wang QH, Wang HQ, Wang YF, et al. A distributed access control with outsourced computation in fog computing. *Secur Commun Netw* 2019; 2019: 6782753.

44. Lynn B. *PBC (pairing-based cryptography) library*, 2012, http://crypto.stanford.edu/pbc/