Ensuring Accountability and Outsourced Decryption in IoT Systems using Ciphertext-Policy Attribute-Based Encryption

Ambili K N[1] and Jimmy Jose[1†]

[1]Department of Computer Science and Engineering, National Institute of Technology Calicut, Street, Calicut, 673601, Kerala, India.

Contributing authors: ambili_p180002cs@nitc.ac.in; jimmy@nitc.ac.in;
[†]These authors contributed equally to this work.

Abstract

Attribute based cryptography enhances the chances of secure communication on large scale. There are several features of attribute based encryption which have been proposed as different protocols. Most of these are suitable for access control in large systems like cloud services. Very few protocols focus on reducing the computational overhead for lower end devices like Internet of Things sensors and actuators. Hence, it is desirable to have a mix of features in protocols for IoT architecture. Our protocol enforces accountability of different parties involved while reducing the computational overhead during decryption on miniature devices. We prove that our protocol is RCCA-secure in selective security model and achieve accountability and unlinkability.

Keywords: ABE, CP-ABE, Accountability, Outsourced Decryption, Paillier based Cryptography, IoT Systems

1 Introduction

Public key cryptography reached new dimensions when attribute based encryption (ABE) was introduced in 2005 [1]. ABE schemes were introduced as an extension to identity-based encryption (IBE) [2] schemes which associated users with their identities. ABE schemes built upon this by associating users with a set of attributes and their identities. The cryptographic primitives in ABE are achieved using access policy.

ABE schemes make use of access policy embedded in access structures to map user attributes. The schemes wherein access policy is transmitted together with the ciphertext and keys are based on attributes are known as ciphertext policy attribute based encryption (CP-ABE). Other schemes make use of access policy to generate keys while using attributes for encryption. These are known as key-policy attribute based encryption schemes (KP-ABE). The current work proposes CP-ABE based protocol.

ABE has been exploited by researchers in various ways to provide fine grained access control in cloud [3]. Several features have been introduced in various protocols. The paper hint at combining ABE schemes with different features to generate novel protocols that may be adapted to various Internet of Things (IoT) architectures.

A typical architecture for IoT makes use of cloud services in different ways. The innovative use of sensors and actuators in various real-life situations has made large amount of data available for storage and analysis. The secure storage of encrypted data is essential to facilitate quick and authentic analysis. The limited memory and computational power of IoT devices call for innovative methods of transformation of encrypted data for secure storage on cloud servers and also their decryption with lesser computational overhead. The parties involved in communication need to be accountable for their operations. The decryption operation should be as simple as possible for easy computation on IoT devices. We discuss accountability and outsourced decryption as they are important features of protocol with ABE for IoT architecture.

1.1 Accountability

Public key cryptography (PKC) has the ability to ensure accountability of data items with digital signatures. The increase in the number of parameters or attributes that define a user make it difficult to achieve accountability in ABE schemes. Nevertheless, there have been various attempts to propose accountable ABE schemes. Several schemes achieve whitebox traceability in which the malicious users do not tweak the decryption algorithm or the secret key. The schemes which permit changes to decryption algorithm and the secret key by malicious users during public auditing is more difficult to achieve and are said to be blackbox traceable.

Accountable CP-ABE is essential to find the malicious users who may delegate their keys to other users and malicious authorities which misuse the role of key management. A general solution has been to use multi-authority schemes

wherein the authority as well as the user are accountable. With the increasing number of IoT devices and data explosion, a simpler approach would facilitate safer storage of encrypted data. The domination of a single authority needs to be overcome while maintaining the accountability of user and authorities involved.

1.2 Outsourced Decryption

The increase in the number of miniature devices demand cryptographic systems with lesser number of computations. The applications like email on mobile phones is a typical example which can be made faster with lighter decryption key. This can be achieved by outsourcing complex operations of decryption. The extraction of data by IoT actuators from servers may also be made easier with outsourced decryption.

1.3 Our contribution

The high end servers in cloud architecture allows us to accommodate complicated methods to achieve confidentiality and accountability. The execution of complex operations involved in ABE system is time consuming on IoT devices and would hinder the performance of the overall system. Often, the servers in cloud misuse their role in key management. This leads to the key escrow problem [4]. Though most of the proposed ABE schemes prevent user collusion attacks, very few achieve accountability. These factors inspire us to think of designing a protocol which can make ABE practical on IoT devices and ensure end-to-end accountability. The user can establish a secure session with any authority that can successfully run zero knowledge protocol and all other authorities will have only transformation key to analyse the encrypted data. We propose a CP-ABE protocol with following features:

- whitebox traceability and accountability
- public auditing
- secure outsourcing of decryption
- less computational overhead during decryption
- suitability for IoT deployment
- security analysis focusing on indistinguishability under RCCA in selective security model, accountability and unlinkability

2 Related Work

There are different approaches to public key cryptography. Identity based encryption [2, 5] is one among the new approaches.The scope of identity based encryption was increased beyond biometric identities by addition of descriptive attributes. The concrete method proposed in [1] validates this. Two complementary forms of ABE were formalized in [6] as KP-ABE and CP-ABE. CP-ABE was designed earlier as a powerful public key primitive for access

control by Bethencourt et.al.[7]. The recent survey paper on attribute based encryption for cloud computing [3] describes different features of ABE schemes.

One of the early research works on accountable ABE scheme is by Li et. al. [8]. The need arises due to the possibility of malicious behaviour of the parties involved. The key escrow problem reduces the trust in authorities. The malevolent behavior of users may cause the issue of key delegation. It becomes difficult to trace the malicious users in the system. The research on ABE takes into account two types of accountability. The schemes with whitebox traceability assume that the parties involved in the scheme are faithful to the auditor. The focus of [9, 10] are on whitebox traceability. The malicious user could manipulate or hide the tweaked decryption algorithm and the secret key that she uses from the auditor. The research work in [11, 12] achieve blackbox traceability. The blackbox traceable CP-ABE scheme of [11] is provably secure and suitable for cloud storage. The blackbox traceability in [12] can be used to detect malevolent decryption devices. The recent research also shows multi-authority schemes that have been proposed as a solution to key delegation issues [13–17].

Outsourced decryption was formalised by Dan Boneh in [18]. Due to the computational overhead, the practical implementation of ABE schemes on devices is challenging. As a solution to reduce computational effort, different methods for outsourced computation were proposed in [19–21]. The notion of proxy re-encryption is used in [22, 23]. The generation of transformation keys allows ciphertext to be shared across servers without loss of security. The functional encryption methods like homomorphism, allow certain computations to be done on ciphertext using specified inputs while keeping the underlying message undecipherable by unauthorised user.

There are few research papers that focus on making ABE schemes suitable for IoT deployment. Accountability in multi-authority environments is achieved in [24].

The proposal in [25] combines the outsourcing and accountability but its application is limited to cloud. A KP-ABE scheme with application to IoT is described in [26]. In general, there is a dearth of research works supporting efficient extension of attribute based cryptography to IoT deployment with various features. We propose a CP-ABE protocol with accountability and outsourced decryption. The relevant preliminaries are described in section 3. RCCA-secure construction is described in 4. Section 5 concludes the paper

3 Background

In this section, we provide the preliminaries needed to understand the rest of the paper. The primary actors involved are accountable authority and the user. Both are equally accountable for their behavior on the network. This is ensured by incorporating parameters from both of these into the keys generated in the system. Other authorities involved in this framework get a transformation key which has contributions from both the accountable authority and the user.

The accountable authority handles attribute set which are disjoint. Each user has a number of IoT devices she uses which map to a number of attributes. Among these, few identify the user uniquely. Each user generates a decryption key after appropriate communication with accountable authority. A ciphertext can be created by anyone using a policy. Decryption is possible only by a particular user. The apt combination of user attributes make it possible to use it on IoT devices owned by the user. The usage of transformation key makes decryption operation computationally easy. The mathematical preliminaries and definitions needed to describe this protocol is given below.

3.1 Preliminaries

Let G_1, G_2, and G_T, be multiplicative cyclic groups of prime order p. Let g be the generator of G_1, G_2 and $e : G_1 \times G_2 \Rightarrow G_T$ be a bilinear pairing with the following properties:

- Bilinearity: $e(u^a, v^b) = e(u, v)^{ab}$
- Non-degeneracy: $e(u, v) \neq 1_T$, where 1_T is the identity element of group G_T.
- Computability: there is an efficient algorithm for computing $e(u, v)$ for all $u \in G_1$ and $v \in G_2$

We consider composite order bilinear groups first proposed by [27]. The group operations are assumed to be computable in polynomial time with respect to the security parameter λ. Here, G_1, G_2 are the source groups and G_T is the target group. The groups are chosen in such a way that their orthogonality under the bilinear map is preserved. The assumptions on subgroup decision problem for three prime numbers also hold with these groups [28]. Decisional Bilinear Diffie-Hellman also hold on these groups.

The protocol uses interactive zero knowledge proof to verify the validity of the authority. The user chooses a random value t and g^t is made available to the AT. The user confirms this with an interactive session of ZK-POK before proceeding with cryptographic operations.

The ABE scheme begins by mapping attributes of universe to random elements. An access policy is framed based on the system requirements. These are mapped to the access structure, linear secret sharing scheme (LSSS). LSSS is itself represented as a matrix and is used encryption. More mathematical details are available in [29] and interested reader may refer to the same.

3.2 Security model

We analyse the security of the protocol using three different games. We consider Replayable Chosen Ciphertext Attack (RCCA) model since it eliminates the strict restriction that no bit of the ciphertext may be changed [30]. We also consider a game for accountability and another one for unlinkability [14]. We consider these in the selective security model [31]. These games are defined in the following subsections.

3.2.1 Game 1 for accountability

The adversary is allowed to corrupt a few secret keys for attribute sets of its choice. The adversary is supposed to generate a decryption box and submits it to the challenger. The challenger runs the key sanity check and trace over the pirate decryption box and returns an identifier. The adversary wins if he can generate a new valid identifier not present in identifiers generated during the query phase. Below we describe the game.

Setup. Given a security parameter 1^{λ} the challenger runs Setup and gets the public parameters, public key and secret key pairs of few users, $(params, (pk_k, sk_k)$ for $k \in 1, \ldots N)$, where pk, sk denote public key and secret key respectively. The parameters, $pk_{k k \in \{1,\ldots,N\}}$, and $sk_{k k \in \{1,\ldots,N\}}$ are given to the adversary A.

Phase 1. A queries the key generation oracle on attribute set S of its choice using set of global identities GID. This can be done polynomial number of times. At the end of this phase, A determines a decryption box and submits it to B.

Trace. B executes the key sanity check and trace algorithms with the decryption box. B determines the identities using the decryption box and outputs an identity $GID^{'}$.

A wins the game if $GID^{'} \notin GID$.

3.2.2 Game 2 for unlinkability

The goal of the adversary is to get information on the attributes of a given identity. The game is described below.
Setup. Given a security parameter 1^{λ} the challenger runs Setup and gets $(params, (pk_k, sk_k), k \in \{1, \ldots N\})$, where pk, sk denote public key and secret key respectively. These are given to A.

Phase 1. A queries key generation oracle for attribute set S using identity GID polynomial number of times.

Guess. Finally, the challenger outputs attribute set $S^{'}$ and the corresponding identity GID'.

A wins the game if $GID^{'}$ and $L^{'}$ are linkable and the success probability is greater than random guess with non-negligible probability.

Now, we provide the definitions of security in terms of the games defined above to validate the security of our protocols.

Definition : ABE scheme is said to be accountable if the probability that an adversary can win the games Game 1 and Game 2 is negligible.

Definition : ABE scheme is CPA-secure if the probability that an adversary win the IND-CPA game is negligible.

Definition : A CP-ABE scheme is said to be accountable with secure outsourced decryption if the probability that the adversary wins the IND-CPA, Game 1 and Game 2 simultaneously is negligible.

The above games and definitions will be used in protocol construction. The security analysis of protocol can be done by RCCA game described below.

3.2.3 RCCA game

To prove the indistinguishability of messages under replayable chosen-ciphertext attack (RCCA) [32] and the collusion-resistance of user secret keys, we consider an adversary A who has access to an encryption oracle and a simulator B capable of solving the chosen base scheme. During the initialisation and setup phase, A fetches public paramters and access structure from B. In the query phase, two random oracles are used that provides the values corresponding to input seed as per the algorithm without disclosing any other details. The query phase also provides algorithms to create secret key and transformation key corresponding to a set of attributes, to corrupt a key entry and also to decrypt ciphertext using the existing secret key. All these entries are also recorded in appropriate data structures. The first query phase is followed by a challenge phase wherein A submits two messages to B, B encrypts them and returns the ciphertext to A. A second query phase follows which has restriction that same entries cannot be queried for as in phase 1. Finally, A has to guess the message that was encrypted.

If A is able to correctly guess the message, then the scheme used by the simulator B is broken. RCCA-secure scheme is described in the following section.

4 RCCA-secure construction

The protocol is designed using composite bilinear pairing group G. The encryption, transformation and decryption operations ensure confidentiality. Key sanity check, trace and audit operation help achieve accountability. The protocol involves transformation of ciphertext and thus needs CCA security. It is difficult to achieve full CCA security. Hence, the security analysis of the protocol is done with respect to the games described in 3.2.3, 3.2.1 and 3.2.2 are provided in 4.2. We consider replayable CCA security described in [33]. We also prove the accountability and unlinkability of the modified scheme.

4.1 Design

The system consists of attribute authority, cloud servers and IoT devices. The initialization process sets up the public parameters. The key generation step involves user and creates transformation key TK. TK is used by cloud servers to store partially decrypted ciphertext.

4.1.1 Setup

The system is setup using group generator G with λ, the security parameter as input. A composite bilinear group G of order $N = p_1p_2p_3$ (three distinct primes) is chosen. G_{p_i} is a subgroup of order p_i in G and g_1, g_3 the generator of the subgroup G_{p_1}, G_{p_3} respectively are chosen.

A random value u_i is chosen from the set of natural numbers Z_N corresponding to each attribute i in U.

A group element $v \in G_{p_1}$ and exponents $f_1, f_2, f_3, f_4 \in Z_N$ are chosen randomly. Two random primes p and q are also chosen such that $p \neq q$, $\mathsf{p} = \mathsf{q}$, $gcd(pq, (p-1)(q-1)) = 1$. Let $n = pq$, $\pi = lcm(p-1, q-1)$, $h = (1+n)$ and $Q = \pi^{-1} mod\ n$.

The public parameters are set as $pp = (N, n, h, v, g^{f_2}, g^{f_3}, g^{f_4}, e(g,g)^{f_1}, g^{u_i}{}_{i \in U})$.

Master secret is set as $msk = (p, q, f_1, g_3)$.

4.1.2 Key Generation

The key generation protocol involves interaction between attribute authority and a user with the identity id.

1. User chooses $t \in Z_N$ randomly and computes $R_U = g^t$. Next, it sends R_U, id, S to authority. An interactive ZK-POK is executed on R_U with respect to g with authority. The various ZK-PoK methods are detailed in [34].
2. The authority checks the validity of ZK-POK. If the check fails, the interaction is aborted. Otherwise, a random c is chosen from Z_N, a random r from Z_n^* and random elements $R, R_0, R_{0'}, R_{ii \in S}$ fromn G_{p_3}. The secret key is computed as follows:
   $< S, \overline{K} = g^{f_1/(f_2+T)} g^{f_3/(f_2+T)} v^c R, \overline{T} = h^{id} r^n \bmod n^2, \overline{L} = g^c R_0, \overline{L}' = g^{ac} R_0', \overline{K}_i = U_i^{(f_2+\overline{T})c} R_{i_{i \in S}} >$.
   It sends (c, sk_{pri}) to U.
3. User checks the following conditions:
   (a) $e(\overline{L}', g) = e(\overline{L}, g^a) e(g^a, g^c)$
   (b) $e(\overline{K}, g^{f_2}\overline{T}) = e(g,g)^{f_1} e(\overline{L}'\overline{L}^{\overline{T}}, v) e(R_U, g^{f_3})$

(c) $\forall x \in S$ such that $e(U_x, \overline{L}'\overline{L}^{\overline{T}}) = e(\overline{K}_x, g)$

The interaction is aborted if the above conditions do not hold. In case all these conditions are satisfied, the user computes $t_{id} = c/t$ and computes $\overline{K} = g^{f_1/(f_2+T)}$. This is used to create transformation key as follows: $TK = < S, K = \overline{K}g^{f_4 t_{id}}, T = \overline{T}, L = \overline{L}, L' = \overline{L}', R_U, t_{id}, K_i = \overline{K}_{ii\in S} >$.

User sets his secret key as $sk_U = (t, TK)$. It is assumed that the cloud servers that use transformation key cannot eavesdrop on interaction between AT and U to determine c.

4.1.3 Encryption

The algorithm takes access structure encoded in a LSSS policy, the public parameters *pp* and a plaintext messages as input.

The algorithm chooses $\overrightarrow{y} = (s, y_2, ..., y_n) \in Z_N^{n*1}$ randomly. Here, s is the first element of the vector. It is the random secret to be shared among the shares. Then, $r_j \in Z_N$ is chosen for each row A_j of access structure A randomly. The encryption uses two hash functions H1 and H2. A random number R is generated. The ciphertext is set as follows:

$r = H2(R)$

$C = M \oplus r$

$C =< R.e(g,g)^{f_1 s}, C' = g^s, C_1 = g^{f_2 s}, C_2 = g^{f_3 s}, C_3 = g^{f_4 s}, C_4 = M \oplus r,$

$\{C_{j,1} = v_{\rho(j)}^{A_j \overrightarrow{y} U^{-r_j}}, C_{j,2} = g^{r_j}\}_{j\in[l]}, (A, \rho) >$

4.1.4 Transformation

The ciphertext and transformation key are taken as input and a pair of ciphertexts T_0, T_1 are generated. Each user has an identity *id* associated with the attribute set S which satisfies the access structure.

Let $\omega_j \in Z_p$ where $j \in I_j$ such that $\rho(j) \in S$ be set of constants such that if λ_j are valid shares of any secret s according to the access structure then $\sum_{j\in I} \omega_j \lambda_j = s$.

The algorithm computes

$D = e(C_0^T C_1, K)(e(C_2, R_u)e(C_3, (g^T g^{f_2})^{t_{id}}))^{-1}$

$E = \Pi\rho(j) \in S(e(C_{j,1}, L^T L')e(C_{j,2}, K_{\rho(j)}))^{\omega_j}$

$F = D/E$

The transformed text is $T_0 = C, T_1 = F$

4.1.5 Decryption

The decryption takes secret key (t,TK) of the user and the transformed ciphertext (T_0, T_1) as input.

$R = T_0/T_2^t$

$M = T_1 \oplus H_2(R)$

The values in T_0 and T_1 are verified. The message M is output if these are equal, else an error is reported.

4.1.6 Key Sanity Check

The algorithm checks the sanity of the secret key of a user. Here, the secret key submitted by a user is used.

The secret key submitted by a user $sk_U = (t, TK)$

1. Pick the second term TK from the user secret key which is $\overline{K}g^{f_4 t_{id}}$. Compute $K/g^{f_4 t_{id}}$ to get $\overline{K}^t$. This calculation helps determine the second term of the secret key sk_{pri} originally derived using public parameters from the authority and using which the transformation key was made.
2. Verify $e(L', g) = e(L, g^{f_2})$
3. Verify $e(K, g^{f_2} g^T) = e(g, g)^{f_1} e(L' L_T, v) e(R_U, g^{f_3}) e((g^{f_2} g^T)_{id}^t, g^{f_4})$
4. $\forall x \in S$ such that $e(U_x, L' L^T) = e(K_x, g)$

If all above are true, the algorithm outputs 1. Else it outputs 0.

4.1.7 Trace

If key sanity check fails, a null output is generated. The success of the key sanity check ensures that the input key provided is a well-formed decryption key. The identity is extracted from T as follows:

$Q = \pi^{-1} mod$ n

$T^{\pi Q} = 1 + id.n \ mod$ n.

Thus, id is evaluated and output.

4.1.8 Audit

If a user with identity id and decryption key sk_{id} is identified as malicious by the system using the traced key (sk_{id*} of the suspected device) but claims to be innocent, the user will interact with the public auditor PA as follows:

1. User sends its decryption key to public auditor. If key sanity check fails, public auditor aborts the interaction.
2. Else the public auditor checks $t_{id} = t_{id*}$. If it does not hold, it outputs "innocent" which indicates that user is innocent and wrongly framed by the system. Otherwise, it outputs "guilty" which indicates that user is malicious and secret key was leaked by user.

4.2 Security Analysis and Discussion

We claim RCCA security for the proposed protocol. RCCA is stronger security notion than CPA. It is apt to prove the security of our protocol since our ciphertext undergoes alteration during partial decryption. The authorised cloud server at the proximity hold the transformation key and will not be able to decrypt the message or infer any meaningful information.

We consider the adversarial model and games described in Section 3.2 to analyse the security of our proposal. The scheme in [35] is referred to as $\sum_{accCPABE}$. We refer to our proposal as $\sum_{CPABE}$.

4.2.1 RCCA Security

Theorem: Suppose the construction of $\sum_{accCPABE}$ is CPA-secure. Then, our proposed CPABE scheme $\sum_{CPABE}$ with accounatability and outsourced decryption is RCCA-secure.

Proof:

Suppose there exist a PPT adversary A that can attack our protocol $\sum_{CPABE}$ with non-negligible advantage ϵ. Then, a simulator B can be constructed that can attack the scheme $\sum_{accCPABE}$ with advantage ϵ minus a negligible amount. A PPT algorithm A is constructed that has an advantage in breaking our protocol which is same as the advantage in breaking the underlying scheme $\sum_{accCPABE}$.

Init B runs A, which chooses (A^*, ρ^*) as challenge and returns to B. B sends this to $\sum_{accCPABE}$ challenger on which it is challenged.

Setup The adversary B fetches the public parameters and returns them to A.

Query Phase 1 B initializes an empty set D, empty tables T, T_1, T_2, integer $j = 0$. It has two hash functions G_1 and G_2 which act as random oracles. It answers A's queries as follows:

- $H_1(R, m)$ - If an entry $(R, m, e(g, g)^{f_1 s}, s)$ exists in T_1, return s. Else, choose s randomly in Z_p, add entry $(R, m, e(g, g)^{f_1 s}, s)$ in T_1 and return s.
- $H_2(R)$ - If entry (R, r) exists in T_2, return r. Else, choose a random $r \in 0, 1^k$,add entry (R, r) in T_2 and return r.
- Create(S) - If S satisifies the access structure specified at the beginning of the game, then it chooses a fake transformation key TK by choosing a random $d \in Z_p$ and running key generation part and obtaining secret key. Else, it calls the key generation oracle of $\sum_{CPABE}$ to obtain secret key. A

proper choice of t is then done to generate transformation key. The table T stores (j, S, SK, TK). TK is provided to A.

- Corrupt(i) - B retrieves ith entry from T if it exists, sets $D = D \bigcup S$ and returns SK to A. NULL is returned if no such entry exists.
- Decrypt(i, CT) - This query decrypts CT using the ith entry from table T. The transformation key is available to both A and B. Let $CT = T_0, T_1$ be associated with the challenge access structure specified at the beginning. Assume that all the ciphertexts are partially decrypted. If ith entry does not exist in table or the set of attributes corresponding to the ith entry does not consform to the specified access structure, NULL is returned to A. If ith entry exists, (i, S, SK, TK) is obtained from table T. The decryption of message m is done by checking if the key i satisfies the access structure. If key i does not satisfy the challenge structure, proceed as follows:

  1. Parse SK = (t, TK). Compute $R = T_0/T_1^t$.
  2. Retrieve (R, m_i, s_i) from T_1. If none exist, return NULL.
  3. If there exists duplicate entries for R in T_1, then abort the simulation.
  4. Else, obtain (R, r) from T_2. B outputs NULL if an entry does not exist.
  5. Check if $C = Re(g, g)^{f_1 s} e(g, g)^z$ and $T_0/T_1^t = C$.
  6. If there exists an i that passes the above test, output the message m, else output NULL.

  If key i does not satisfy the challenge structure, proceed as follows:

  1. Get $SK = (t, TK)$. Calculate $X = T_0/T_1^t$.
  2. For each entry corresponding to index i in T_1, check if $X = me(g, g)^{1/t}$.
  3. If there is no match, B returns NULL to A.
  4. The simulation is aborted if multiple entries exist.
  5. Else, get (R, r) corresponding to R from T_2. Abort the simulation if it does not exist.
  6. Check if $C = Re(g, g)^{f_1 s} e(g, g)^z$ and $T_0/T_1^t = C$.
  7. If there exists an i that passes the above test, output the message m, else output NULL.

Challenge A submits two messages m_0, m_1 and access structure to B. B randomly picks one and generates the ciphertext using encryption algorithm with the challenge access structure of $\sum_{accCPABE}$. The challenge ciphertext is then given to A.

Query Phase 2 Queries are repeated as in phase 1 with the restriction that the messages and access structure used in challenge phase cannot be queried upon.

Guess A outputs a guess $b\prime$ of the message. If is unable to output bit or abort, B takes up the role and searches in the available tables T_1, T_2 and T. If a valid entry is found for a message, the corresponding bit number is returned. Else, a random bit is output as the guess.

If the adversary A correctly guesses the bit number, it means there is considerable advantage in breaking the simulation of $\sum_{accCPABE}$ using B.

This would further mean that $\sum_{accCPABE}$ is not secure which is not the case. Hence, there is negligible advantage for any adversary A to break our protocol.

We hereby deduce the CPA security also of our protocol since RCCA security implies CPA security.

4.2.2 Accountability

Theorem: $\sum_{CPABE}$ is accountable.

Proof:

Setup The challenger B executes the setup, retrieves parameters and passes them on to the adversary A.

Query The key generation oracle is run in this phase. A runs queries using attribute set S, public key and tampered secret key. The challenger returns identifier.

Guess The adversary A submits the decryption box she identifies. A wins the game if she is able to identify the decryption box correctly.

The probability of challenger generating a valid identifier using pirate decryption box depends on the probability to successfully pass all the steps of key sanity check and generate identifier. The identifier can be generated only if Q, π can be correctly evaluated. This further depends on the probability of factorising n which is negligible. Hence, probability that the decryption box will be correctly guessed by adversary A is negligible. Hence, $\sum_{CPABE}$ is accountable.

4.2.3 Unlinkability

Theorem: $\sum_{CPABE}$ is unlinkable.

Proof:

Our protocol uses ZK-POK between user and the authority for key generation. Hence, the authority cannot deduce any information about the underlying attributes. The identity of the user cannot be linked by any of the authorities that hold the transformation key to the attribute of the user. The probability that A determines the identity is negligible. Hence, $\sum_{CAPABE}$ is unlinkable.

5 Conclusion and Future Work

We proposed CP-ABE schemes with outsourced decryption and accountability. The storage of transformed ciphertext on untrusted server paves way to the execution of functional encryption methods without disclosing details of the underlying message. This also ensures the security of the ever increasing data from billions of IoT devices. The schemes are useful to trace malevolent IoT devices which may be operated as bots also.

The transformation of ciphertext allows decryption on resource constrained devices with a simple exponentiation operation and a bilinear operation

compared to more operations in [36–38]. The interactive zero knowledge protocol involved in key generation phase ensures security while maintaining user anonymity. The derivation of cryptographic keys with participation from authorities as well as the user provides whitebox traceability. We have also achieved the stronger notions of public auditing in outsourced decryption compared to [25] which achieves accountability with a trusted auditor. Our method achieves outsourced decryption with public accountability using composite groups.

Future research may include conversion of the protocol to use prime order groups and practical implementation of a prototype based on the proposed schemes in a real-world IoT setting.

References

[1] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) Advances in Cryptology – EUROCRYPT 2005, pp. 457–473. Springer, Berlin, Heidelberg (2005)

[2] Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) Advances in Cryptology — CRYPTO 2001, pp. 213–229. Springer, Berlin, Heidelberg (2001)

[3] Zhang, Y., Deng, R.H., Xu, S., Sun, J., Li, Q., Zheng, D.: Attribute-based encryption for cloud computing access control: A survey. ACM Comput. Surv. **53**(4) (2020). https://doi.org/10.1145/3398036

[4] Maher, D.P.: Crypto backup and key escrow. Commun. ACM **39**(3), 48–53 (1996). https://doi.org/10.1145/227234.227241

[5] Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) Advances in Cryptology - EUROCRYPT 2004, pp. 223–238. Springer, Berlin, Heidelberg (2004)

[6] Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute based encryption. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) Automata, Languages and Programming, pp. 579–591. Springer, Berlin, Heidelberg (2008)

[7] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy (SP '07), pp. 321–334 (2007). https://doi.org/10.1109/SP.2007.11

[8] Li, J., Ren, K., Zhu, B., Wan, Z.: Privacy-aware attribute-based encryption with user accountability. In: Samarati, P., Yung, M., Martinelli, F.,

Ardagna, C.A. (eds.) Information Security, pp. 347–362. Springer, Berlin, Heidelberg (2009)

[9] Ning, J., Dong, X., Cao, Z., Wei, L., Lin, X.: White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Transactions on Information Forensics and Security **10**(6), 1274–1288 (2015). https://doi.org/10.1109/TIFS.2015.2405905

[10] Liu, Z., Cao, Z., Wong, D.S.: White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Transactions on Information Forensics and Security **8**(1), 76–88 (2013). https://doi.org/10.1109/TIFS.2012.2223683

[11] Qiao, H., Ba, H., Zhou, H., Wang, Z., Ren, J., Hu, Y.: Practical, provably secure, and black-box traceable cp-abe for cryptographic cloud storage. Symmetry **10**(10) (2018). https://doi.org/10.3390/sym10100482

[12] Liu, Z., Cao, Z., Wong, D.S.: Blackbox traceable cp-abe: How to catch people leaking their keys by selling decryption devices on ebay. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. CCS '13, pp. 475–486. Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2508859.2516683. https://doi.org/10.1145/2508859.2516683

[13] Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) Theory of Cryptography, pp. 515–534. Springer, Berlin, Heidelberg (2007)

[14] Li, J., Chen, X., Chow, S.S.M., Huang, Q., Wong, D.S., Liu, Z.: Multi-authority fine-grained access control with accountability and its application in cloud. Journal of Network and Computer Applications **112**, 89–96 (2018). https://doi.org/10.1016/j.jnca.2018.03.006

[15] Doshi, N., Jinwala, D.: Constant ciphertext length in multi-authority ciphertext policy attribute based encryption. In: 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011), pp. 451–456 (2011). https://doi.org/10.1109/ICCCT.2011.6075139

[16] Yundong, F., Xiaoping, W., Jiasheng, W.: Multi-authority attribute-based encryption access control scheme with hidden policy and constant length ciphertext for cloud storage. In: 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), pp. 205–212 (2017). https://doi.org/10.1109/DSC.2017.10

[17] Chase, M., Chow, S.S.M.: Improving privacy and security in multi-authority attribute-based encryption. In: Proceedings of the

16th ACM Conference on Computer and Communications Security. CCS '09, pp. 121–130. Association for Computing Machinery, New York, NY, USA (2009). https://doi.org/10.1145/1653662.1653678. https://doi.org/10.1145/1653662.1653678

[18] Boneh, D., Sahai, A., Waters, B.: Functional encryption: Definitions and challenges. In: Ishai, Y. (ed.) Theory of Cryptography, pp. 253–273. Springer, Berlin, Heidelberg (2011)

[19] Chung, K.-M., Kalai, Y., Vadhan, S.: Improved delegation of computation using fully homomorphic encryption. In: Rabin, T. (ed.) Advances in Cryptology – CRYPTO 2010, pp. 483–501. Springer, Berlin, Heidelberg (2010)

[20] Gennaro, R., Gentry, C., Parno, B.: Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In: Rabin, T. (ed.) Advances in Cryptology – CRYPTO 2010, pp. 465–482. Springer, Berlin, Heidelberg (2010)

[21] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. STOC '09, pp. 169–178. Association for Computing Machinery, New York, NY, USA (2009). https://doi.org/10.1145/1536414.1536440. https://doi.org/10.1145/1536414.1536440

[22] Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur. **9**(1), 1–30 (2006). https://doi.org/10.1145/1127345.1127346

[23] Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: Nyberg, K. (ed.) Advances in Cryptology — EUROCRYPT'98, pp. 127–144. Springer, Berlin, Heidelberg (1998)

[24] Banerjee, S., Roy, S., Odelu, V., Das, A.K., Chattopadhyay, S., Rodrigues, J.J.., Park, Y.: Multi-authority cp-abe-based user access control scheme with constant-size key and ciphertext for iot deployment. Journal of Information Security and Applications **53**, 102503 (2020). https://doi.org/10.1016/j.jisa.2020.102503

[25] Ning, J., Cao, Z., Dong, X., Liang, K., Ma, H., Wei, L.: Auditable σ -time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security **13**(1), 94–105 (2018). https://doi.org/10.1109/TIFS.2017.2738601

[26] Touati, L.: Grouping-proofs based access control using kp-abe for iot applications. In: 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 301–308

(2017). https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.251

[27] Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-dnf formulas on ciphertexts. In: Kilian, J. (ed.) Theory of Cryptography, pp. 325–341. Springer, Berlin, Heidelberg (2005)

[28] Agrawal, S., Libert, B., Stehlé, D.: Fully secure functional encryption for inner products, from standard assumptions. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016, pp. 333–362. Springer, Berlin, Heidelberg (2016)

[29] Beimel, A.: Secret-sharing schemes: A survey. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) Coding and Cryptology, pp. 11–46. Springer, Berlin, Heidelberg (2011)

[30] Canetti, R., Krawczyk, H., Nielsen, J.B.: Relaxing chosen-ciphertext security. In: Boneh, D. (ed.) Advances in Cryptology - CRYPTO 2003, pp. 565–582. Springer, Berlin, Heidelberg (2003)

[31] Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. CCS '93, pp. 62–73. Association for Computing Machinery, New York, NY, USA (1993). https://doi.org/10.1145/168588.168596. https://doi.org/10.1145/168588.168596

[32] Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. Journal of Cryptology **26**, 80–101 (2013). https://doi.org/10.1007/s00145-011-9114-1

[33] Green, M., Hohenberger, S., Waters, B.: Outsourcing the decryption of abe ciphertexts. In: Proceedings of the 20th USENIX Conference on Security. SEC'11, p. 34. USENIX Association, USA (2011)

[34] Bangerter, E., Barzan, S., Krenn, S., Sadeghi, A., Schneider, T., Tsay, J.-K.: Bringing zero-knowledge proofs of knowledge to practice. In: Security Protocols Workshop (2009)

[35] Ning, J., Dong, X., Cao, Z., Wei, L.: Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In: Pernul, G., Y A Ryan, P., Weippl, E. (eds.) Computer Security – ESORICS 2015, pp. 270–289. Springer, Cham (2015)

[36] Lai, J., Deng, R.H., Guan, C., Weng, J.: Attribute-based encryption with verifiable outsourced decryption. IEEE Transactions on Information Forensics and Security **8**(8), 1343–1354 (2013). https://doi.org/10.1109/TIFS.2013.2271848

[37] Lin, S., Zhang, R., Ma, H., Wang, M.: Revisiting attribute-based encryption with verifiable outsourced decryption. IEEE Transactions on Information Forensics and Security **10**(10), 2119–2130 (2015). https://doi.org/10.1109/TIFS.2015.2449264

[38] Ma, H., Zhang, R., Wan, Z., Lu, Y., Lin, S.: Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions on Dependable and Secure Computing **14**(6), 679–692 (2017). https://doi.org/10.1109/TDSC.2015.2499755

[39] Katz, J., Lindell, Y.: Introduction to Modern Cryptography (Chapman; Hall/Crc Cryptography and Network Security Series). Chapman ; Hall/CRC, ??? (2007)