Decentralized Ciphertext-Policy Attribute-Based Encryption: A Post-Quantum Construction

Mohammad Shahriar Rahman[1]*, Anirban Basu[2], and Shinsaku Kiyomoto[2]
[1]University of Asia Pacific, Dhaka, Bangladesh
shahriar.rahman@uap-bd.edu
[2]KDDI Research, Inc., Saitama, Japan
{basu, kiyomoto}@kddi-research.jp

Abstract

In Ciphertext Policy Attribute-Based Encryption (CP-ABE) system, a set of attributes is associated with the private keys of each user. Also, the ciphertext is attached with a policy which is defined over that set of attributes. A user can decrypt the ciphertext if the ciphertext's policy is satisfied by the attributes associated hith her private key. Traditional CP-ABE schemes, based on number theoretic problems, rely on a trustworthy central authority. But in many distributed applications it is expected that such authorities should be decentralized to avoid the risks of single-point failure. While the number theory-based hardness problems are prone to quantum attacks, lattice-based hardness problems can resist such attacks. In this paper, we construct a Decentralized Ciphertext-Policy Attribute-Based Encryption (DCP-ABE) scheme. Under this scheme, any participating entity can act as an authority by creating a public key. The athority utilizes the users' attributes to generate the private keys for them. Any user can encrypt data in terms of any monotone access structure over attributes issued from any chosen set of authorities. Hence the protocol does not depend on any central authority. We utilize Learning With Errors over Rings (R-LWE) as the underlying hardness assumption for te protocol. The proposed post-quantum protocol achieves security under selective-set model whereby adversaries are allowed to corrupt any authority only statically through adaptive key queries.

Keyword: Security, CP-ABE, Decentralized, Lattice

1 Introduction

The concept of Attribute-Based Encryption (ABE) system was first proposed by Sahai and Waters [30]. In this system, access to the data is expressed as a boolean formula over a defined universe of attributes and a data encryptor can specify such access. Each user is issued with a private key from an authority in such a way that the private key is related to the attributes. A user is only able to decrypt a ciphertext if the she holds the private key associated with the attributes satisfying the boolean formula assigned to the ciphertext. By using ABE, it is easy for someone to share data according to well-defined encryption policy without having any prior knowledge of the data recipient. For example, an system administrator may need to encrypt a contractual employee's performance evaluation report for all permanent employees of the cyber security department or anyone in the human resource (HR) department. The administrator will prefer the access policy ("Cyber Security" AND "Permanent") OR"HR" to be encrypted with the report. Under this scenario, only employees with attributes matching the defined policy are able to decrypt the report. However, achieving security against colluding users is one of the crucial challenges for designing

Journal of Internet Services and Information Security (JISIS), volume: 7, number: 3 (August 2017), pp. 1-16

*Corresponding author: Mohammad Shahriar Rahman, Department of Computer Science and Enginering, University of Asia Pacific, Dhaka 1215, Bangladesh, Tel: +8802-58157091(Ext. 707), Web: https://sites.google.com/site/msrahman1662 such systems. A pair of unauthorized users, where one has the two attributes of "Permanent" and "Accounts" and the other one has the attribute of "Cyber Security" should not be able to access the encrypted report. Note that neither of them is actually a permanent employee of the Cyber Security Department, as it was required by the access policy for decrypting the report . An ABE scheme is required to be resistant against such collusion attacks.

ABE schemes have mainly two variants: Key Policy Attribute-Based Encryption (KP-ABE) and Ciphertext Policy Attribute-Based Encryption (CP-ABE). In KP-ABE scheme, the ciphertext is associated with a set of descriptive attributes. The access policy is defined over a set of attributes and the private key os a user is associated with that policy. This policy specifies which type of ciphertexts the can be decrypted by the key. On the other hand, in CP-ABE scheme, the private keys are associated with a set of attributes, and the ciphertext is attached with a policy defined over that set of attributes. Any user can decrypt the ciphertext if the ciphertext's policy is satisfied by the attributes associated with her private key. Given that both of schemes support the same type access policies, a CP-ABE scheme is more flexible than a KP-ABE. This is because the users can set access policies when encrypting messages instead of the authority setting policies when extracting users' secret keys. In practice, in many applications, we just care about what attributes a user has when extracting her secret key, rather than how a user will use her attributes. In our running example, for CP-ABE, there is a central Key Generation Center (KGC) that generates a Master Secret Key (MSK) for the users in order to get them thir secret keys (SK_{S_A} or SK_{S_B}). The administrator encryots a message M with publick key PK under the policy P. Since S_A satisfies the policy, Alice can decrypt the ciphertect C. On the other hand, Bob fails to decrypt as his credentials do not satisfy the policy P. The running example of CP-ABE is illustrated in Figure 1.

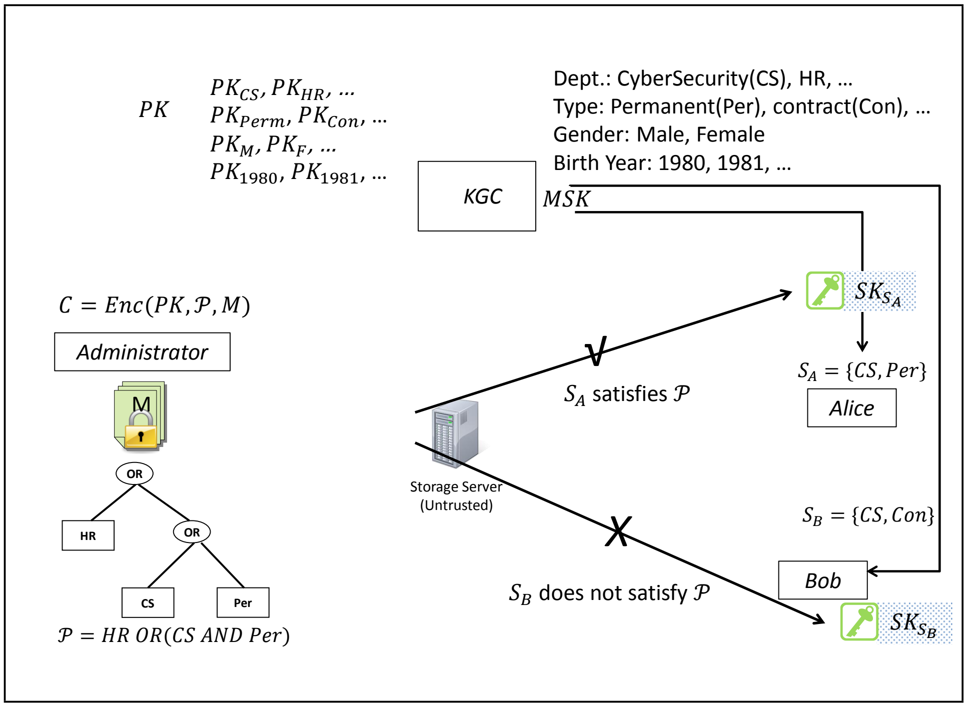

PK
$PK_{CS}, PK_{HR}, \ldots$
$PK_{Perm}, PK_{Con}, \ldots$
$PK_M, PK_F, \ldots$
$PK_{1980}, PK_{1981}, \ldots$
Dept.: CyberSecurity(CS), HR, …
Type: Permanent(Per), contract(Con), …
Gender: Male, Female
Birth Year: 1980, 1981, …
KGC
MSK
SK_{S_A}
$C = Enc(PK, \mathcal{P}, M)$
Administrator
M
S_A satisfies $\mathcal{P}$
$S_A = \{CS, Per\}$
Alice
OR
HR
OR
CS
Per
$\mathcal{P} = HR\ OR(CS\ AND\ Per)$
Storage Server (Untrusted)
$S_B = \{CS, Con\}$
Bob
S_B does not satisfy $\mathcal{P}$
SK_{S_B}

Figure 1: Ciphertext Policy - Attribute Based Encryption (CP-ABE)

1.1 Single and Multi-Authority CP-ABE

Variants of Attribute-Based Encryption and its applications are proposed in several works [5, 15, 25, 14, 32, 9, 8, 17, 31, 24].One central authority is used to issue the private keys in almost all the schemes of ABE and its variants. It is required that the central authority would need to be in a position to verify all the attributes issued by it for each user in the system. By utilizing such systems, one can share information according to a policy over some attributes which are issued within a domain or organization. However, there are many applications where it is expected that data is shared according to a policy written over attributes or credentials issued by different trust domains and organizations. For instance, a party might want to share medical data only with a user who has the attribute of "Doctor" issued by a medical organization and the attribute "Researcher" issued by the administrators of a clinical trial. On a commercial application, two organizations such as Amazon and Google might both issue attributes as part of a joint project. It can be troublesome to use single authority CP-ABE systems for such applications as it is required that a single (or, central) authority should be able to verify attributes across different organizations and issue private keys to every user in the system. This designated central authority must be globally trustworthy, and thus becomes a major bottleneck since its failure will compromise the entire system.

The first Multi Authority-ABE (MA-ABE) scheme [8] was proposed by Chase to overcome the above mentioned problems. The concept of MA-ABE is to combine a global identifier with the private key of user in order to ensure correct decryption. The scheme relies on a trusted centralized authority who knows all secret keys of any attribute authority for combining the attribute private keys that belong to the same user. Moreover, the scheme is limited to expressing a strict "AND" policy over a pre-determined set of authorities. In [23], a protocol supporting any monotone access structure (where both "AND" and "OR" access policies are supported) under a centralized authority was proposed. The proof of this scheme could handle only non-adaptive queries even though it allows one to obtain attributes from other authorities without revisiting the central authority. The idea of replacing the central authority by a distributed pseudo random function was proposed in [9]. However, the proposed scheme supported only "AND" policy with a pre-determined set of authorities. The authors in [19] proposed a threshold scheme, which was shown to be secure withstanding collusion of upto m users with m being a system parameter. The scheme is semi-decentralized in a sense that the authorities must interact during the system setup. Lewko et al. proposed a fully decentralized scheme in [18], whereby any party could simply act as an authority by creating a public key and issuing private keys to different users, and different authorities do not need to be aware of each other. The scheme also supports any monotone access structure.

1.2 Lattice-based Cryptography

All the schemes discussed in the previous section are based on traditional number theory-based hard problems which were proved to have polynomial-time solutions. In contrast, lattice-based hardness problems can resist quantum cryptanalysis and have strong worst-case/average-case security guarantees. Furthermore, the mathematical properties of lattices make them both relatively efficient and flexible to enable the construction of powerful cryptosystems. So lattices have recently emerged as a powerful mathematical platform on which to build a rich variety of cryptographic primitives. Since the work [3], there were many schemes proposed: one-way function and collision-resistant hash function [22], public-key encryption scheme [29], identity-based encryption schemes [12, 7, 1], fully homomorphic encryption schemes [11].

1.3 Related Work

As discussed earlier, Lewko et al. [18] proposed the idea of decentralizing ABE and presented a concrete instantiation of CP-ABE. However, the construction is under the traditional number theoretic assumption which is not post-quantum. In [2], authors proposed fuzzy identity based encryption from lattices and discussed the difficulties to derive ABE from the scheme. A KP-ABE scheme for monotone access structures was proposed in [6], and its security was reduced from Learning With Errors (LWE) problem. However, the proposed scheme does not handle the decentralization of attribute authorities. In [34], a CP-ABE has been proposed, and its security is proved under the Ring-LWE (R-LWE) hardness assumption. But the protocol relies on trusted authority and is not decentralized. Also, it supports 'AND' policy only. A multi-authority CP-ABE scheme was proposed in [33], which utilizes LWE as the underlying hardness assumption. The protocol relies on a trusted central authority and does not support monotone access structure. However, to the best of our knowledge, no fully decentralized CP-ABE protocol without a trusted authority has been proposed that achieves quantum safety under R-LWE assumption supporting any monotone access structure.

1.4 Our Contribution

In this paper [1], we propose a decentralized ciphertext-policy attribute-based encryption (DCP-ABE) scheme which achieves the following features:

- It is the first DCP-ABE scheme constructed under Ring-LWE assumption (R-LWE), which is quantum-safe in selectve-ID model. It is also more efficient than the LWE-based schemes due to the algebraic structure of R-LWE.
- The protocol supports any monotone access policy (both AND and OR) that can be expressed as a Linear Secret Sharing Scheme (LSSS). We have shown that the proposed protocol achieves correctness. Through Theorem 2, we have demonstrated that the protocol is secure.

1.5 Roadmap

The preliminaries and security definition are introduced in Section 2. Our proposed DCP-ABE scheme is proposed in Section 3. Section 4 includes the security and efficiency analyses. Finally, the conclusion is drawn in Section 5.

2 Preliminaries

2.1 Lattices

A lattice is a set of points in m-dimensional space with a periodic structure, which can be described formally as follows.

Definition 1. *Given n linearly independent vectors $b_1, \cdots, b_n \in \mathbb{R}^m$, the lattice generated by them is defined as*

$$\mathscr{L}(b_1 \cdots b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z}, 1 \le i \le n \right\}$$

where $b_1, \cdots, b_n$ is the basis of the lattice.

[1] A preliminary version of this paper was published at IEEE TrustCom 2016. This is the full version. System Model, Figure 1 and 2, Decryption Correctness and Proof of Theorem 2 are newly added.

An m-dimensional lattice $\mathscr{L}$ is both:

1. *an additive subgroup*: $0 \in \mathscr{L}$, and $\mathbf{x}, \mathbf{x}+\mathbf{y} \in \mathscr{L}$ for every $\mathbf{x}, \mathbf{y} \in \mathscr{L}$; and
2. *discrete*: every $\mathbf{x} \in \mathscr{L}$ has a neighborhood in $\mathbb{R}^m$ in which $\mathbf{x}$ is the only lattice point.

The *minimum distance* of a lattice $\mathscr{L}$ is the length of a shortest nonzero lattice vector: $\lambda_1(\mathscr{L} := \min_{\mathbf{v} \in \mathscr{L} \setminus \{\mathbf{0}\}} \|\mathbf{v}\|$ (where, $\|\cdot\|$ denotes the Euclidean norm). More generally, the i-th successive minimum $\lambda_i(\mathscr{L})$ is the smallest r such that $\mathscr{L}$ has i linearly independent vectors of norm at most r.

2.2 Computational Problems

We now define some of the computational problems on lattices that have been most useful in cryptography.

Definition 2 (Shortest Vector Problem (SVP)[27])**.** *Given an arbitrary basis* $\mathbf{B}$ *of some lattice* $\mathscr{L} = \mathscr{L}(\mathbf{B})$*, find a shortest nonzero lattice vector, i.e., a* $\mathbf{v} \in \mathscr{L}$ *for which* $\|\mathbf{v}\| = \lambda_1(\mathscr{L})$*.*

Approximation problems are important for cryptographic primitives, which are parameterized by an approximation factor $\gamma \geq 1$ that is typically taken to be a function of the lattice dimension m, i.e., $\gamma = \gamma(m)$. The approximation version of SVP is as follows:

Definition 3 (Approximate SVP (SVP_γ)[27])**.** *Given a basis* $\mathbf{B}$ *of an m-dimensional lattice* $\mathscr{L} = \mathscr{L}(\mathbf{B})$*, find a nonzero vector* $\mathbf{v} \in \mathscr{L}$ *for which* $\|\mathbf{v}\| \leq \gamma(m) \cdot \lambda_1(\mathscr{L})$*.*

The standard worst-case approximation problem GapSVP$_\gamma$ is the decision version of SVP_γ, which is defined as follows.

Definition 4 (GapSVP$_\gamma$ [13])**.** *An input to GapSVP$_\gamma$ is a pair* $(\mathbf{B}, d)$ *where* $\mathbf{B}$ *is an m-dimensional lattice basis and* $d > 0$*. It is a Yes instance if* $\lambda_1(\mathscr{L}(\mathbf{B})) \leq d$*, and a No instance if* $\lambda_1(\mathscr{L}(\mathbf{B})) > \gamma(m) \cdot d$*, where* $\lambda_1(\mathscr{L}(\mathbf{B}))$ *is the minimum distance of a lattice* $\mathscr{L}(\mathbf{B})$*, and* $\gamma(m)$ *is the approximation factor.*

The Learning With Errors (LWE) problem is parameterized by positive integers n and q, and an error distribution χ over $\mathbb{Z}$, where χ is usually taken to be a discrete Gaussian of width αq for some $\alpha < 1$, which is often called the relative "error rate".

Definition 5 (LWE distribution[27])**.** *For a vector* $\mathbf{s} \in \mathbb{Z}_q^n$ *called the secret, the LWE distribution* $A_{\mathbf{s},\chi}$ *over* $\mathbb{Z}_q^n \times \mathbb{Z}_q$ *is sampled by choosing* $\mathbf{a} \in \mathbb{Z}_q^n$ *uniformly at random, choosing* $e \leftarrow \chi$*, and outputting* $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e \bmod q)$*.*

It was shown in [26] that for certain q and error distributions, LWE is at least as hard as solving $GapSVP_\gamma$ in the worst case.

Now, we move on to define R-LWE problem. Let $f(x) = x^n + 1 \in \mathbb{Z}[x]$, where the security parameter n is a power of 2, making $f(x)$ irreducible over the rationals, and let $R = \mathbb{Z}[x] \,/\, \langle f(x) \rangle$ be the ring of integer polynomials modulo $f(x)$. Let $q = 1 \bmod 2n$ be a sufficiently large public prime modulus (bounded by a polynomial in n), and $R_q = R \,/\, qR = \mathbb{Z}_q[x] \,/\, \langle f(x) \rangle$ be the ring of integer polynomials modulo both $f(x)$

and q. Elements of R_q may be represented by polynomials of degree less than n, whose coefficients are in $\mathbb{Z}_q$.

In [20], R-LWE problem has been informally described as follows. Let $s \in R_q$ be a uniformly random ring element (secret). Define two distributions over $R_q \times R_q$ as follows. (1) $(a, b = a \cdot s + e) \in R_q \times R_q$, where $a \leftarrow R_q$ is uniformly random, and e is some small random error term chosen from a certain distribution over R. (2) (a, c), where $a, c \leftarrow R_q$ is uniformly random. Then the two distributions described above are indistinguishable. A more formal definition of the decisional version of R-LWE problem can be obtained as follows.

Definition 6 (Decision R-LWE (Adapted from [20, 21]))**.** *Given a distribution χ over R_q that depends on security parameter n, the Decision R-LWE problem instance consists of access to an unspecified challenge oracle $\mathscr{O}$, either a noisy pseudo-random sampler $\mathscr{O}_s$ for random secret key $s \in R_q$; or, a truly random sampler $\mathscr{O}_\$$. The Decision R-LWE problem is to distinguish the sampling between $\mathscr{O}_s$ and $\mathscr{O}_\$$, which perform respectively as follows:*

$\mathscr{O}_s$: *outputs noisy pseudo-random samples of the form $(a, b) = (a, a \cdot s + e) \in R_q \times R_q$. The element s is drawn uniformly random from R_q, where $s \leftarrow R_q$ and it is fixed for all samples. For each sample, the element a is drawn uniformly random from R_q, where $a \leftarrow R_q$ and the element e is a small error term generated with a distribution χ, where $e \leftarrow \chi$.*

$\mathscr{O}_\$$: *outputs truly random samples $(a, b) \in R_q \times R_q$, drawn independently and uniformly random in the entire domain $R_q \times R_q$.*

The Decision R-LWE problem allows repeated queries to be sent to the challenge oracle $\mathscr{O}$. The algorithm adversary $\mathscr{A}$ decides the Decision R-LWE problem if

$$| \, Pr[\mathscr{A}^{\mathscr{O}_s} = 1] - Pr[\mathscr{A}^{\mathscr{O}_\$} = 1] \, |$$

is non-negligible for a random $s \in R_q$.

Authors in [20] discussed the hardness of the R-LWE problem under the worst case assumptions on ideal lattices in the rings of integer polynomials, where an ideal lattice is simply a lattice corresponding to an *ideal* in R under some fixed choice of geometric embedding. Their R-LWE definition requires the secret s and noisy product b to be in $R_q^\vee := R^\vee / qR^\vee$, where $R^\vee$ is a certain fractional ideal that is dual to R, and is related by a certain "tweak" factor t, where $tR^\vee = R$. However, the author in [27] argued that these two forms of the problem are entirely equivalent in terms of computation, applications and analysis

Theorem 1 ([20])**.** *Suppose that it is hard for polynomialtime quantum algorithms to approximate the shortest vector problem in the worst case on ideal lattices in R to within a fixed $poly(n)$ factor. Then any $poly(n)$ number of samples drawn from the R-LWE distribution are pseudorandom to any polynomial time (even quantum) attacker.*

In [10], authors show some of the weak instances of R-LWE and construct an explicit family of number fields for which their attacks are efficient. Later, it was shown in [28] how one should instantiate R-LWE to avoid the attacks on R-LWE. We assume that the parameters in our protocol are chosen accordingly.

2.3 Access Structure and Linear Secret Sharing (LSSS)

Definition 7 (Access Structure [4]). *Let $\{P_1,\ldots,P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1,\ldots,P_n\}}$ is monotone if $\forall B,C$: if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1,\ldots,P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1,\ldots,P_n\}} \setminus \{\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.*

In our setting, attributes will play the role of parties and we will only consider monotone access structures.

Definition 8 (LSSS [6]). *An LSSS Π over a set of parties $\{P_1,\ldots,P_n\}$ consists of an index map ρ and a share generating matrix $L \in \mathbb{Z}_q^{l\times\theta}$ with l rows and θ columns, where l is the number of shares specified by Π, and θ depends on the structure of Π. For all $h = 1,\ldots,l$, the function ρ maps the h-th row of L to its corresponding party. The matrix L maps an input θ-vector $\boldsymbol{v} = (s, r_2,\ldots,r_\theta)$, where $s \in \mathbb{Z}_q$ is the secret to be shared, and $r_2,\ldots,r_\theta \in \mathbb{Z}_q$ are random, into an output l-vector $L\boldsymbol{v} = (s_1,\ldots,s_l)$ containing the shares of the secret s according to Π. The share $s_h = (L\boldsymbol{v})_h$ is assigned to party $\rho(h)$.*

Given that Π is an LSSS for access structure $\mathbb{A}$, then the following holds as the *linear reconstruction* property. Let $S \in \mathbb{A}$ be any authorized set, and let $I \subset \{1,2,\ldots,l\}$ be defined as $I = \{h : \rho(h) \in S\}$. Then, there exists constants $\{\omega_h \in \mathbb{Z}_q\}$ for $h \in I$, such that, if the $\{\delta_h = (L\mathbf{v})_h\}$ are valid shares of any secret s according to Π, then $\sum_{h\in I} \delta_h \omega_h = s$. Furthermore, these constants ω_h can be found in polynomial time in the size of share-generating matrix L [4]. For any unauthorized set, no such constants exists. In this paper, the LSSS matrix (L,ρ) will be used to express an access structure associated to a ciphertext.

2.4 Decentralized CP-ABE

A decentralized Ciphertext-Policy Attribute-Based Encryption [18] system is comprised of the following five algorithms:

Global Setup$(n) \to GP$: The global setup algorithm takes in the security parameter n and outputs global parameters GP for the system.

Authority Setup$(GP) \to (SK,PK)$: Each authority runs the authority setup algorithm with GP as input to produce its own secret key and public key pair, (SK,PK).

Encrypt$(M,(L,\rho),GP,\{PK\}) \to CT$: The encryption algorithm takes in a message M, an access matrix (L,ρ), the set of public keys for relevant authorities, and the global parameters. It outputs a ciphertext CT.

KeyGen$(GID,GP,i,SK) \to K_{i,GID}$: The key generation algorithm takes in an identity GID, the global parameters, an attribute i belonging to some authority, and the secret key SK for this authority. It produces a key $K_{i,GID}$ for this attribute, identity pair.

Decrypt$(CT,GP,\{K_{i,GID}\}) \to M$: The decryption algorithm takes in the global parameters, the ciphertext, and a collection of keys corresponding to attribute, identity pairs all with the same fixed identity GID. It outputs either the message M when the collection of attributes i satisfies the access matrix corresponding to the ciphertext. Otherwise, decryption fails.

2.5 Security Definition

Our definition of security for decentralized CP-ABE systems uses the following chosen-plaintext selective-set game between a challenger and an attacker adapted from [15]. We assume that adversaries can corrupt authorities only statically, but key queries are made adaptively as used in [9, 18, 30]. We assume each attribute is assigned to one authority (though each authority may control multiple attributes). If multiple authorities choose the same string attribute, these will still correspond to distinct attributes in the system.

Setup: The global setup algorithm is run. The adversary $\mathscr{A}$ declares a set of attributes η, one for each authority, that he wishes to be challenged upon. He must also provide a list of corrupt authorities. The challenger runs the authority setup algorithm for the non-corrupt and gives the public keys to $\mathscr{A}$.

Phase 1: $\mathscr{A}$ is allowed to make key queries by submitting pairs (i, GID) to the challenger, where i is an attribute belonging to a non-corrupt authority and GID is an identity. The challenger responds by giving the attacker the corresponding key, $\{K_{i,GID}\}$.

Challenge: $\mathscr{A}$ submits two equal length message M_0, M_1, and an access matrix (L, ρ). The access matrix must satisfy the following constraint. We let V denote the subset of rows of $\mathscr{A}$ labeled by attributes controlled by corrupt authorities. For each identity GID, we let V_{GID} denote the subset of rows of L labeled by attributes i for which the attacker has queried (i, GID). For each GID, we require that the subspace spanned by $V \cup V_{GID}$ must not include $(1, 0, \ldots, 0)$. (In other words, the attacker cannot ask for a set of keys that allow decryption, in combination with any keys that can obtained from corrupt authorities.) The challenger flips a random coin b, and encrypts M_b with η. The ciphertext is passed to $\mathscr{A}$.

Phase 2: Phase 1 is repeated.

Guess: $\mathscr{A}$ outputs a guess b' of b.

The advantage of an adversary $\mathscr{A}$ in this game is defined as $Adv(\mathscr{A}) = \mid Pr(b = b') - 1/2 \mid$.

Definition 9. *A DCP-ABE system under decision R-LWE assumption (DCP-ABE$_{R-LWE}$) is secure against static corruption of authorities if attackers have at most a negligible advantage in the above security game.*

Remark: To construct a DCP-ABE system from R-LWE, two major requirements are needed to be satisfied. First, the system should be collusion resistant, whereby collusion of multiple users whose individual attributes are insufficient to satisfy the access policy should not be able to pool their attributes to form a valid secret key allowing to recover the original message. To make our scheme collusion resistant, we use the private key randomization technique as discussed in [32]. Each user's private key, associated with a set of attributes, will be blinded with a random element $(t \cdot GID)$ during the KeyGen algorithm. This random value, $(t \cdot GID)$ will be wiped out if they are from the same user during the Decrypt algorithm. The global identity ties together the various attributes belonging to a specific user so that they cannot be successfully combined with another user's attributes in decryption. If two users with different identities GID and GID' attempt to collude and combine their keys, then there will be some terms with different random values involving t and t', and these will not cancel with each other, thereby preventing the recovery of the blinding term that includes the shared secret s. However, encryption does not utilize the unique GID, and the ability to decrypt is the same with traditional ABE scheme independent of the *GID*. Second, the scheme must be able to support the scalability of users [16]. The increasing numbers of authorized users should not affect the performance of the systems. In the proposed scheme, the access policy is embedded into the ciphertext, and the user's private key is associated with a set of attributes. This subsequently allows to encrypt the message without knowing the actual number of users. The new users can access the encrypted data if and only if their private key satisfies the access policy in the encrypted data.

3 Our Decentralized CP-ABE System

In this Section, we first give an overview of the proposed DCP-ABE system model and then construct our proposed scheme.

3.1 System model

We assume there is a system for medical data. We consider four parties in our system: *N* number of Attribute Authorities, Data Storage server, Data Owner, and Data User. An attribute authority is an entity responsible for supervising medical data storage and access mechanism. It could be any health information entity or other national-level organization. The server stores encrypted medical data designed to support CP-ABE scheme. A data owner could be a patient who owns the medical data. A data owner should be able to manage, control, and share her medical data with a variety of legitimate data users. A data user could be any person or entity who has access rights to patient's medical data. Data users, such as medical practitioners and researchers, can access data owner's medical data for professional purposes. The system is illustrated in Figure 2.

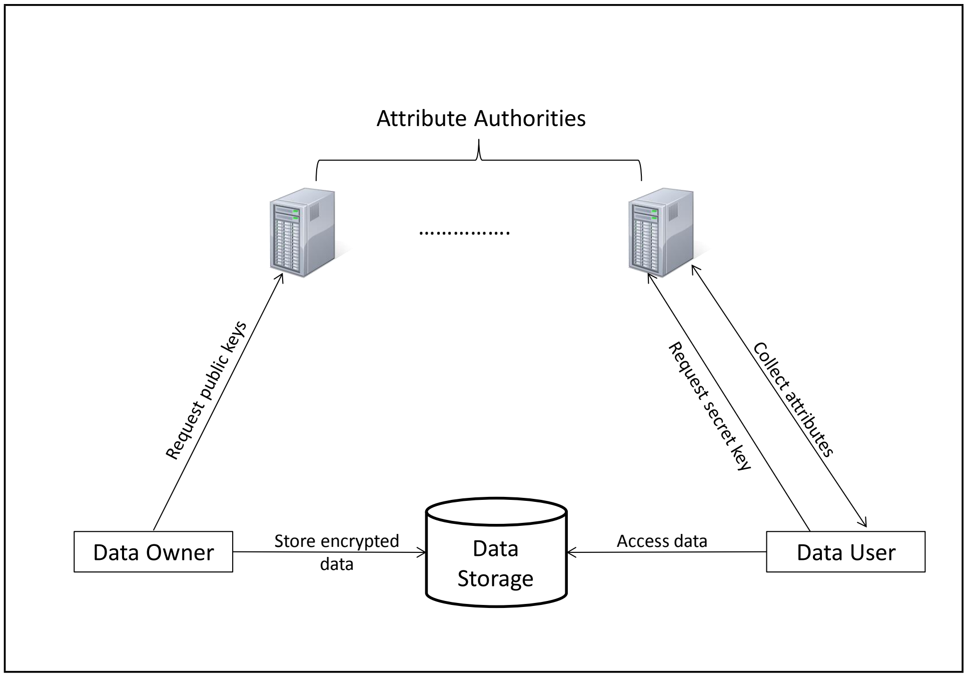


Figure 2: System Model

3.2 Protocol Contruction

Global Setup$(n) \rightarrow GP$: Given a security parameter n (where n is a power of 2), a sufficiently large prime modulus $q = 1 \bmod 2n$ and a small positive integer p is chosen. Let $f(x) = x^n + 1 \in \mathbb{Z}[x], R = \mathbb{Z}[x]/\langle f(x)\rangle$ and $R_q = \mathbb{Z}_q[x]/\langle f(x)\rangle$. Let $\chi \subset R_q$ be an error distribution. A uniformly random $a \in R_q$ is also chosen. The global public parameters, GP, are a, p, R_q, χ.

Authority Setup$(GP) \rightarrow (SK, PK)$: For each attribute i belonging to the authority, the authority does the following. Randomly selects $\beta_i \leftarrow R_q$, chooses a small noise term $e \leftarrow \chi$, computes $z_i = a\beta_i + pe \in R_q$. Then, for each attribute select a pair of uniformly random $(y_i, y_i^{-1}) \in R_q$, where y_i^{-1} is the inverse of y_i in R_q, and a small noise term $e_i \in \chi$. Compute $\alpha_i = y_i + pe_i \in R_q$. Finally, it publishes $PK = \{z_i, \alpha_i\}$ as its publis key. It keeps $SK = \{\beta_i, y_i\}$ as its secret key.

Encrypt$(M, (L, \rho), GP, \{PK\}) \rightarrow CT$: The encryption algorithm takes in a message M, an $l \times \theta$ access matrix L with ρ mapping its rows to attributes, the set of public keys for relevant authorities, and the global parameters. It generates a vector $\mathbf{v} = (s, r_2, \ldots, r_\theta)$, where $s \in R_q$ is the secret to be shared and $r_2, \ldots, r_\theta \leftarrow R_q$ are randomly chosen. Then, $L\mathbf{v}$ is the vector of l shares of the secret according to secret sharing scheme Π over a set of attributes. For each h, it calculates the secret share $\delta_h = L_h \times \mathbf{v} \in R_q$, where L_h is the vector corresponding to h-th row of L. Next, it selects a uniformly random $r \leftarrow R_q$ and noise terms $e', e'' \leftarrow \chi$. The ciphertext, CT, is computed as:

$$C'_h = z_{\rho(h)} \cdot r \cdot s + M + pe' \in R_q$$
$$C_h = a \cdot \alpha_{\rho(h)} \cdot r \cdot \delta_h + pe'' \in R_q$$

KeyGen$(GID, GP, i, SK) \rightarrow K_{i,GID}$: The key generation algorithm takes in an identity GID for an attribute i belonging to an authority, the global parameters, and the secret key SK for this authority. It produces a key $K_{i,GID}$ for this attribute, identity pair as follows. It selects a pair of freshly random element and it's inverse $(t, t^{-1}) \in R_q$, uniformly random noise terms $\tilde{e}', \tilde{e}'' \leftarrow \chi$. A user's private key $K_{i,GID}$ is computed as:

$$K'_i = \beta_i \cdot t^{-1} \cdot GID^{-1} + p\tilde{e}' \in R_q$$
$$K_i = y_i^{-1} \cdot t \cdot GID + p\tilde{e}'' \in R_q$$

Decrypt$(CT, GP, \{K_{i,GID}\}) \rightarrow M$: Given the global parameters, the ciphertext, and a collection of keys, it outputs either the message M when the collection of attributes i satisfies the access matrix corresponding to the ciphertext. Let $S \in \mathbb{A}$ be any authorized set, and let $I \subset \{1, 2, \ldots, l\}$ be defined as $I = \{h : \rho(h) \in S\}$. Then, there exists constants $\{\omega_h \in \mathbb{Z}_q\}$ for $h \in I$, such that, if the $\{\delta_h = (L\mathbf{v})_h\}$ are valid shares of any secret s according to Π, then $\sum_{h\in I} \delta_h \omega_h = s$. Now, it calculates $M' = C'_h - K'_{\rho(h)} \sum_{h\in I} C_h \cdot \omega_h \cdot K_{\rho(h)}$, and outputs $M = M'$. Otherwise, the decryption fails.

Correctness: The correctness of the proposed DCP-ABE protocol can be checked as follows.

$$\begin{aligned}
M' =& C'_h - K'_{\rho(h)} \sum_{h\in I} C_h \cdot \omega_h \cdot K_{\rho(h)} \\
=& C'_h - K'_{\rho(h)} \sum_{h\in I} (a\alpha_{\rho(h)} r\delta_h + pe'') \cdot \omega_h \cdot K_{\rho(h)} \\
=& C'_h - K'_{\rho(h)} \sum_{h\in I} (a\alpha_{\rho(h)} r\delta_h \cdot \omega_h \cdot K_{\rho(h)}) \\
& - pK'_{\rho(h)} \sum_{h\in I} e'' \cdot \omega_h \cdot K_{\rho(h)} \\
=& C'_h - K'_{\rho(h)} \sum_{h\in I} (ars\alpha_{\rho(h)} \cdot K_{\rho(h)}) \\
& - pK'_{\rho(h)} \sum_{h\in I} e'' \cdot \omega_x \cdot K_{\rho(h)}
\end{aligned}$$

$$\begin{aligned}
=& C'_h - K'_{\rho(h)} \sum_{h\in I} ars(y_{\rho(h)} + pe) \cdot (y^{-1}_{\rho(h)} \cdot t \cdot GID + p\tilde{e}'') \\
& - pK'_{\rho(h)} \sum_{h\in I} e'' \cdot \omega_x \cdot K_{\rho(h)} \\
=& C'_h - arsK_{\rho(h)} \sum_{h\in I} tGID + y_{\rho(h)} p\tilde{e}'' + ty^{-1}_{\rho(h)} GIDpe \\
& + pe\tilde{e}'' - pK_{\rho(h)} \sum_{h\in I} e'' \cdot \omega_h \cdot K_{\rho(h)} \\
=& C'_h - arstGIDK_{\rho(h)} - arspK_{\rho(h)} \sum_{h\in I} (y_{\rho(h)} \tilde{e}'' + y^{-1}_{\rho(h)} \\
& GIDe + e\tilde{e}'') - pK_{\rho(h)} \sum_{h\in I} e'' \cdot \omega_h \cdot K_{\rho(h)} \\
=& (z_{\rho(h)} rs + M + pe') - arstGID(\beta_{\rho(h)} t^{-1} GID^{-1} + p\tilde{e}') \\
& - arspK_{\rho(h)} \sum_{h\in I} (y_{\rho(h)} \tilde{e}'' + y^{-1}_{\rho(h)} GIDe + e\tilde{e}'') \\
& - pK_{\rho(h)} \sum_{h\in I} e'' \cdot \omega_h \cdot K_{\rho(h)} \\
=& (a\beta_{\rho(h)} + pe_0) rs + M + pe' - ars\beta_{\rho(h)} - arstGIDp\tilde{e}' \\
& - arspK_{\rho(h)} \sum_{h\in I} (y_{\rho(h)} \tilde{e}'' + y^{-1}_{\rho(h)} GIDe + e\tilde{e}'') \\
& - pK_0 \sum_{x\in I} e'' \cdot \omega_x \cdot K_{\rho(h)} \\
=& pe_0 rs + M + pe' - arstGIDp\tilde{e}' - arspK_{\rho(h)} \sum_{h\in I} (y_{\rho(h)} \tilde{e}'' \\
& + y^{-1}_{\rho(h)} GIDe + e\tilde{e}'') - pK_{\rho(h)} \sum_{h\in I} e'' \cdot \omega_x \cdot K_{\rho(h)} \\
=& M + p(e_0 rs + e') - pars(tGID\tilde{e}' + K_{\rho(h)} \sum_{h\in I} (y_{\rho(h)} \tilde{e}'' \\
& + y^{-1}_{\rho(h)} GIDe + e\tilde{e}'') - pK_{\rho(h)} \sum_{h\in I}^{''} \cdot \omega_x \cdot K_{\rho(h)}
\end{aligned}$$

As in lattice-based encryption schemes, the proposed scheme adds noise terms into ciphertext. To ensure the correctness of the decryption, the overall noise terms $(e_0, e, e', e'', \tilde{e}', \tilde{e}'')$ in the ciphertext must be small enough compared to the ratio of q to p such that after involving these values with other terms the resultant values remain small enough during a Fast Fourier Transform (FFT). Under the suitably chosen parameter values, the decryptor can compute $M' \bmod p = M$. We leave it to the programmers to measure the exact values of the parameters while deploying the protocol.

4 Analysis

4.1 Security

The security of the proposed scheme is constructed based on the hardness of the Decision R-LWE problem. This section shows that the DCP-ABE$_{R-LWE}$ scheme is secure under a selective-set model with the hardness of Decision R-LWE problem as in Definition 6.

Theorem 2. *If there exists a Probabilistic Polynomial Time (PPT) algorithm adversary $\mathscr{A}$ with an advantage ε in selective-set model for the DCP-ABE$_{R-LWE}$ scheme, then there exists a PPT algorithm simulator $\mathscr{B}$, that decides the Decision R-LWE problem with advantage $\varepsilon/2$.*

Proof: As described in Definition 6, the Decision R-LWE problem instance is conditioned as sample oracle $\mathscr{O}$, that can be either a noisy pseudo-random sampelr $\mathscr{O}_s$ for some secret $s \in R_q$ or a truly random sampler $\mathscr{O}_\$$. Then, the simulator $\mathscr{B}$ will simulate an attack environment and exploit the adversary $\mathscr{A}$ to decide which oracle it is given. Firstly, $\mathscr{B}$ queries $\mathscr{O}$ for $(d+1)$ times and receives fresh R-LWE pairs $(w_f, v_f) \in R_q \times R_q$, where $f \in \{0, 1, \ldots, d\}$. Then, proceeds as follows.

- **Initialization** The adversary $\mathscr{A}$ declares a set of atrributes u from a universe of attribute U, an access structure $\mathbb{A}^*$ that he wishes to be challenged upon, and announces these to $\mathscr{B}$.

- **Setup** $\mathscr{B}$ runs the Global Setup and Authority Setup algorithms to construct the global parameters GP and authority public key as follows:

  - For each $i \in U$, define $z_i = pw_0 \in R_q$
  - Define $\alpha_i = pw_i \in R_q$ if $i \in \mathbb{A}^*$; otherwise, define $\alpha_i = y_i + pe \in R_q$ as defined in Section 3.

  $\mathscr{B}$ returns the public parameters $a, \{z_i, \alpha_i\}_{i=1}^{u}$ to $\mathscr{A}$.

- **Phase 1** $\mathscr{A}$ sends private key queries for an attribute paired with GID for all i, where i is an attribute belonging to a non-corrupt authority and GID is an identity. $\mathscr{B}$ runs KeyGen algorithm of the DCP-ABE$_{R-LWE}$ scheme to construct private key $K_{i,GID}$ as follows.

$$K_i' = \beta_i \cdot t^{-1} \cdot GID^{-1} + p\tilde{e}' \in R_q$$
$$K_i = y_i^{-1} \cdot t \cdot GID + p\tilde{e}'' \in R_q$$

- **Challenge** $\mathscr{A}$ signals that he is ready to accept challenges and sends a challenge message bit, $M \in \{0, 1\}$ to $\mathscr{B}$. $\mathscr{B}$ flips a fair binary coin σ and generates challenge ciphertext M_σ encrypted under the access structure $\mathbb{A}^*$ for u as follows.

  - If $\sigma = 0$, $\mathscr{B}$ randomly chooses $(g_0, g_i) \in R_q$ and sets $C_i' = pg_0 \in R_q$ and $C_i = pg_i \in R_q$
  - If $\sigma = 1$, $\mathscr{B}$ defines $C_i' = pv_0 + M \in R_q$ and $C_i = pv_i \in R_q$

- **Phase 2** The adversary $\mathscr{A}$ and the simulator $\mathscr{B}$ act exactly as they did in Phase 1.

- **Guess** The adversary outputs a guess σ'. The simulator $\mathscr{B}$ uses the guess to determine an answer $\mathscr{O}'$ to the R-LWE challenge. If $(\sigma' = \sigma)$, output $\mathscr{O}' = \mathscr{O}_s$. Otherwise, output $\mathscr{O}' = \mathscr{O}_\$$.

From the definition of selective-set model, the advantage ε of adversary $\mathscr{A}$ is defined as $\mid Pr[\sigma' = \sigma] - 1/2 \mid$. Therefore, when the decisional R-LWE oracle $\mathscr{O}$ is:

- A noisy pseudo-random $\mathscr{O}_s$: $\mathscr{A}$ has an advantage ε, then $Pr[\sigma' = \sigma \mid \mathscr{O} = \mathscr{O}_s] = 1/2 + \varepsilon$ and $Pr[\mathscr{O}' = \mathscr{O} \mid \mathscr{O} = \mathscr{O}_s] = 1/2 + \varepsilon$.

- A truly random $\mathscr{O}_\$$: $\mathscr{A}$ has no advantage ε and has no idea regarding the σ, then $Pr[\sigma' \neq \sigma \mid \mathscr{O} = \mathscr{O}_\$] = 1/2$ and $Pr[\mathscr{O}' = \mathscr{O} \mid \mathscr{O} = \mathscr{O}_\$] = 1/2$

Then, the advantage of simulator $\mathscr{B}$ in this selective game model under the decision R-LWE problem thereby is as follows.

$$\begin{aligned}
&\frac{1}{2}Pr[\mathscr{O}' = \mathscr{O} \mid \mathscr{O} = \mathscr{O}_s] + \frac{1}{2}Pr[\mathscr{O}' = \mathscr{O} \mid \mathscr{O} = \mathscr{O}_\$] - \frac{1}{2} \\
&= \frac{1}{2}(\frac{1}{2} + \varepsilon) + \frac{1}{2}(\frac{1}{2}) - \frac{1}{2} \\
&= \frac{\varepsilon}{2}
\end{aligned}$$

This concludes the security reduction proving that there exists a PPT algorithm simulator $\mathscr{B}$ that decides the decision R-LWE problem with advantage $\frac{\varepsilon}{2}$. □

4.2 Efficiency

The proposed DCP-ABE scheme is constructed based on the hardness of R-LWE problem. The n samples $(a,b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from the standard LWE distribution is replaced with the single sample $(a,b) \in R_q \times R_q$ from the R-LWE distribution, thus reducing the generated public key size by a factor of n. This subsequently reduces computation time and resulting a smaller ciphertext size.

4.3 Comparison With Previous Work

We compare our proposed protocol with some of the related works. Our work is fully decentralized where any party can act as an authority by creating a public key and issuing private keys to different users without requiring to contact with other authorities. Also, it is post-quantum and supports any monotone access structure without relying on central trusted authority. Although the scheme in [18] achieves similar properties as our scheme, it is not quantum-safe. Schemes in [34] and [33] are secure against quantum cryptanalysis. But they rely on trusted central authority and do not support monotone access structure. We summarize the comparison in Table 1.

5 Conclusion

In this paper, we have proposed a post-quantum decentralized CP-ABE protocol. The protocol is chosen-plaintext secure in selective-set model under decisional learning with errors over rings (R-LWE) assumption and it supports any monotone access structure. We have shown that the scheme allows any party to

	[18]	**[33]**	**[34]**	**Our Work**
Post-Quantum	No	Yes	Yes	Yes
Trusted Authority	No	Yes	Yes	No
Hardness	Bilinear Group	LWE	R-LWE	R-LWE
Decentralized	Yes	Yes	No	Yes
Access Policy	‘AND’, ‘OR’	‘AND’	‘AND’	‘AND’, ‘OR’

Table 1. Comparison with related schemes

become an authority, thus removing any dependency on a trusted centralized authority. As for the future work, we plan to extend our protocol to an IND-CCA secure post-quantum decentralized CP-ABE that supports any non-monotone access structure.

References

[1] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (h)ibe in the standard model. In *Proc. of the Annual International Conference on the Theory and Applications of Cryptographic Techniquyes (EUROCRYPT’10), Monaco and Nice, France*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, Berlin, Heidelberg, June 2010.

[2] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee. Functional encryption for threshold functions (or fuzzy ibe) from lattices. In *Proc. of the 15th International Workshop on Public Key Cryptography (PKC’12), Darmstadt, Germany*, volume 7293 of *Lecture Notes in Computer Science*, pages 280–297. Springer, Berlin, Heidelberg, May 2012.

[3] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. of the 29th annual ACM symposium on Theory of computing (STOC’97), El Paso, Texas, USA*, pages 284–293. ACM, May 1997.

[4] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Israel Institute of Technology, 1996.

[5] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Proc. of the 2007 IEEE Symposium on Security and Privacy (SP’07), Berkeley, California, USA*, pages 321–334. IEEE, May 2007.

[6] X. Boyen. Attribute-based functional encryption on lattices. In *Proc. of the 10th Theory of Cryptography Conference (TCC’13), Tokyo, Japan*, volume 7785 of *Lecture Notes in Computer Science*, pages 122–142. Springer, Berlin, Heidelberg, March 2013.

[7] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of cryptology*, 25(4):601–639, October 2012.

[8] M. Chase. Multi-authority attribute based encryption. In *Proc. of the 4th Conference on Theory of Cryptography (TCC’07), Amsterdam, The Netherlands*, volume 4392 of *Lecture Notes in Computer Science*, pages 515–534. Springer, Berlin, Heidelberg, February 2007.

[9] M. Chase and S. S. M. Chow. Improving privacy and security in multi-authority attribute-based encryption. In *Proc. of the 16th ACM Conference on Computer and Communications Security (CCS’09), Chicago, Illinois, USA*, pages 121–130. ACM, November 2009.

[10] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange. Provably weak instances of ring-lwe. In *Proc. of the Annual Cryptology Conference (CRYPTO’15), Santa Barbara, CA, USA*, volume 9215 of *Lecture Notes in Computer Science*, pages 63–92. Springer, Berlin, Heidelberg, August 2015.

[11] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proc. of the 41st annual ACM symposium on Theory of computing (STOC’09), Bethesda, Maryland, USA*, volume 9, pages 169–178. ACM, May 2009.

[12] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proc. of the 40th annual ACM symposium on Theory of computing (STOC’08), Victoria, British*

Columbia, Canada, pages 197–206. ACM, May 2008.

[13] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proc. of the 40th Annual ACM Symposium on Theory of Computing (STOC'08), Victoria, British Columbia, Canada*, pages 197–206. ACM, May 2008.

[14] V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded ciphertext policy attribute based encryption. In *Proc. of the 35th International Colloquium on Automata, Languages, and Programming (ICALP'08), Reykjavik, Iceland*, volume 5126 of *Lecture Notes in Computer Science*, pages 579–591. Springer, Berlin, Heidelberg, July 2008.

[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of the 13th ACM Conference on Computer and Communications Security (CCS'06), Alexandria, Virginia, USA*, pages 89–98. ACM, October 2006.

[16] C.-C. Lee, P.-S. Chung, and M.-S. Hwang. A survey on attribute-based encryption schemes of access control in cloud environments. *International Journal of Network Security*, 15(4):231–240, January 2013.

[17] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Proc. of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), French Riviera, France*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer, Berlin, Heidelberg, June 2010.

[18] A. Lewko and B. Waters. Decentralizing attribute-based encryption. In *Proc. of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'11),Tallinn, Estonia*, volume 6632 of *Lecture Notes in Computer Science*, pages 568–588. Springer, Berlin, Heidelberg, May 2011.

[19] H. Lin, Z. Cao, X. Liang, and J. Shao. Secure threshold multi authority attribute based encryption without a central authority. *Information Sciences*, 180(13):2618 – 2632, July 2010.

[20] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Proc. of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), French Riviera, France*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, Berlin, Heidelberg, June 2010.

[21] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-lwe cryptography. Cryptology ePrint Archive, Report 2013/293, 2013. `http://eprint.iacr.org/2013/293` [Online; Accessed on August 1, 2017].

[22] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity*, 16(4):365 – 411, December 2007.

[23] S. Müller, S. Katzenbeisser, and C. Eckert. On multi-authority ciphertext-policy attribute-based encryption. *Bulletin of the Korean Mathematical Society*, 46(4):803 – 819, 2009.

[24] J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. *IEEE Transaction on Information Forensics and Security*, 10(6):1274–1288, June 2015.

[25] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07), Alexandria, Virginia, USA*, pages 195–203. ACM, October 2007.

[26] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09), Bethesda, MD, USA*, pages 333–342. ACM, May 2009.

[27] C. Peikert. A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939, 2015. `http://eprint.iacr.org/2015/939` [Online; Accessed on August 1, 2017].

[28] C. Peikert. How (not) to instantiate ring-lwe. In *Proc. of the International Conference on Security and Cryptography for Networks (SCN'16), Amalfi, Italy*, volume 9841 of *Lecture Notes in Computer Science*, pages 411–430. Springer, Cham, August 2016.

[29] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, September 2009.

[30] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Proc. of the 24th Annual International Con-*

ference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer-Verlag, May 2005.

[31] Y. Shi, Q. Zheng, J. Liu, and Z. Han. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation. *Information Sciences*, 295(C):221–231, February 2015.

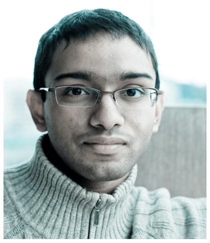
[32] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Proc. of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography (PKC'11), Taormina, Italy*, volume 6571 of *Lecture Notes in Computer Science*, pages 53–70. Springer, Berlin, Heidelberg, March 2011.

[33] G. Zhang, J. Qin, and S. Qazi. Multi-authority attribute-based encryption scheme from lattices. *Journal of Universal Computer Science*, 21(3):483–5001, March 2015.

[34] W. ZHU, J. YU, T. WANG, P. ZHANG, and W. XIE. Efficient attribute-based encryption from r-lwe. *Chinese Journal of Electronics*, 23:778–782, October 2014.

Author Biography

Mohammad Shahriar Rahman is currently an associate professor at the University of Asia Pacific, Bangladesh. Earlier, he worked as a senior researcher at the Information Security group of KDDI Research, Japan. He received his Ph.D. and M.S. degrees in information science from Japan Advanced Institute of Science and Technology (JAIST), in 2012 and 2009 respectively, and B.Sc. in computer science and engineering from University of Dhaka, Bangladesh, in 2006. His research interests include secure protocol construction, privacy-preserving computation and security modeling. He is a member of International Association for Cryptologic Research (IACR).



Anirban Basu is a Senior Researcher at KDDI Research in Japan. He is also a Visiting Research Fellow at the University of Sussex and a Visiting Research Fellow at Rutgers University. He holds a Ph.D. in Computer Science (2010) and a Bachelor of Engineering (Hons.) in Computer Systems Engineering (2004) from the University of Sussex. His research interests are in computational trust, privacy and security and peer-to-peer networks. He is particularly active within the IFIPTM computational trust management community.

Shinsaku Kiyomoto received his B.E. in engineering sciences and his M.E. in Materials Science from Tsukuba University, Japan, in 1998 and 2000, respectively. He joined KDD(now KDDI) and has been engaged in research on stream ciphers, cryptographic protocols, mobile security, and privacy protection. He is currently a senior manager at the Information Security Laboratory of KDDI R&D Laboratories Inc. He was a visiting researcher of the Information Security Group, Royal Holloway University of London from 2008 to 2009. He received his doctorate in engineering from Kyushu University in 2006. He received the IEICE Young Engineer Award and IEICE Achievement Award in 2004 and 2016 respectively. He is a member of JPS and IEICE.