symmetry

MDPI

Article

Efficient Lattice CP-ABE AC Scheme Supporting Reduced-OBDD Structure for CCN/NDN

Eric Affum, Xiasong Zhang *, Xiaofen Wang and John Bosco Ansuura

School of Computer Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China; affrico23@yahoo.com (E.A.); xfwang@uestc.edu.cn (X.W.); jansuura@gmail.com (J.B.A.)

* Correspondence: johnsonzxs@uestc.edu.cn

Received: 3 December 2019; Accepted: 8 January 2020; Published: 14 January 2020

Abstract: In line with the proposed 5th Generation network, content centric network/named data networking (CCN/NDN) has been offered as one of the promising paradigms to cope with the communication needs of future realistic network communications. CCN/NDN allows network communication based on content names and also allows users to obtain information from any of the nearest intermediary caches on the network. Due to that, the ability of cached content to protect itself is essential since contents can be cached on any node everywhere, and publishers may not have total control over their own published data. The attribute based encryption (ABE) scheme is a preferable approach, identified to enable cached contents to be self-secured since it has a special property of encryption with policies. However, most of the proposed ABE schemes for CCN/NDN suffer from some loopholes. They are not flexible in the expression of access policy, they are inefficient, they are based on bilinear maps with pairings, and they are vulnerable to quantum cryptography algorithms. Hence, we propose the ciphertext policy attribute based encryption access control (CP-ABE AC) scheme from a lightweight ideal lattice based on ring learning with error (R-LWE) problem, and demonstrated its use in practical applications. The proposed scheme is proved to be secure and efficient under the decision ring LWE problem in the selective set model. To achieve an efficient scheme, we used an efficient trapdoor technique and the access tree representation of access structure describing the access policies was modified into a new structure, based on a reduced ordered binary decision diagram (reduce-OBDD). This access structure can support Boolean operations such as AND, NOT, OR, and threshold gates. The final result showed that the proposed scheme was secure and efficient for applications, thereby supporting CCN/NDN as a promising paradigm

Keywords: access policy; CCN/NDN; CP-ABE; Gaussian sampling; lattice; reduced-OBDD

1. Introduction

The rapid growth of the utilization of mobile and network resources has led to an increase in global network traffic every year. This is one of the most apparent concerns for mobile and network operators. To manage this huge network traffic and slow throughput, several architectures have been proposed to accommodate this rapid growth and its associated problems. One of these proposed architectures is called content centric networking/named data networking (CCN/NDN). CCN/NDN is one of the technologies of the information centric network (ICN) based on 5G network architecture. The main basic features in CCN/NDN architectures are interest-based content retrieval, content-aware naming and routing at the network layer, and in-network caching

In the CCN/NDN network layer, the sender does not directly send packets (contents) to the receivers and receivers do not access packets (interests) from the data owner. Data owners rather publish content to all networks without necessarily knowing the interested users of the content. These users of the content then request their content without knowing the publisher. Here, the rule for the transaction is evidence of a match between the publisher and subscribers to be followed by the establishment of a delivery path, to enable the delivery of content. The main advantages of this mechanism are, the network nodes cache the content for a fixed period of time and the same content can be requested multiple times, and satisfied from the node without contacting the content owners.

In adopting this phenomenon, we considered a typical internet of things (IoT)-CCN/NDN scenario depicted in Figure 1. This system consists of publisher, IoT CCN/NDN, and the consumers. The content publishers broadcast content that can be cached in all networks and can be accessed and retrieved from any intermediate node. For example, after Bob retrieves content from the server, the content is cached on each of the intermediate nodes, so Alice and Vic can access the same content from node F, and Oscar can also access the same content from node G.

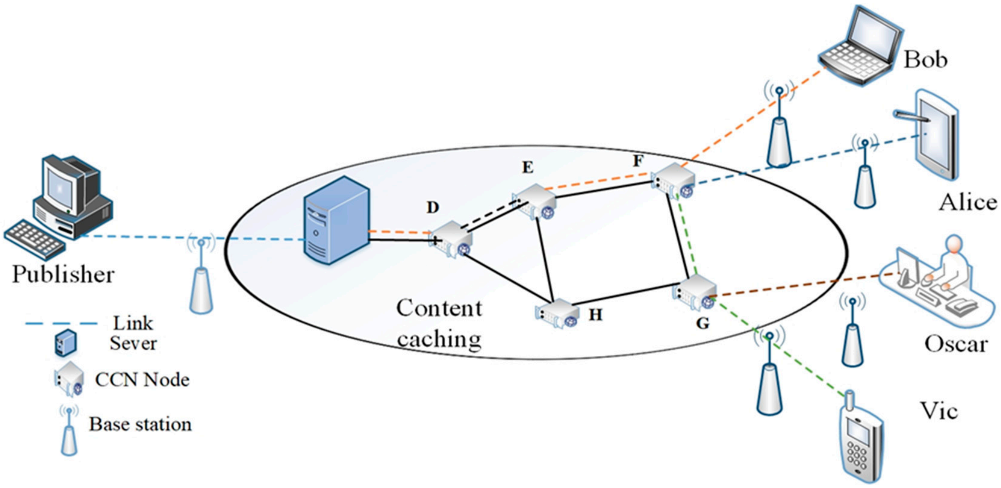

Figure 1. CCN/NDN distribution scenario.

The CCN/NDN has different techniques with regard to its security model. The security component of CCN/NDN modifies the security approach to secure the cached content, instead of the traditional approach of securing network paths for all the networks. The effective way to achieve a required secured data sharing is to provide more scalable and flexible access control for this pervasive and distributed CCN/NDN environment [1]. Fortunately, attribute-based encryption (ABE) cryptosystem has been proposed as a fine-grained access control mechanism for CCN/NDN based on the 5G communication network.

The attribute based encryption scheme comes with two main aspects, namely cipher text-policy ABE (CP-ABE) scheme and key-policy ABE (KP-ABE) scheme. With these schemes, users can recover a message if their attributes fulfill the requirement of the access structure. Ciphertext policy ABE (CP-ABE) has some special properties and advantages, over symmetric, asymmetric and KP-ABE. It also has an impressive property of manufacturing and describing access privileges of users in a more intuitive and scalable way. Further, by using this scheme and without prior knowledge of the receivers of information, data could be shared according to the encrypted policy.

Basically, there are two approaches to designing the algorithms of ABE encryption schemes, and these are bilinear map over elliptical curve and the lattice-based approach. However, several gaps and problems exist in the implementation of these algorithms over the years. By and large, these gaps and problems could be mainly categorized into high communication overhead during cipher text uploading and downloading, high computational cost, the problem of quantum and post-quantum attacks and attacks on the plaintext. There are several access control schemes proposed for CNN/NDN. However, most of these exiting proposed access control schemes are based on a bilinear map over the elliptical curve [2,3]. Some of these works have large computational overhead during encryption and decryption. They also have a high communication overhead during ciphertext uploading and downloading. These massive storage overheads require additional properties of securing cached contents to authenticate each content consumer. Above all, almost all the proposed schemes for CNN/NDN paradigm are susceptible to quantum attacks. The above-mentioned challenges make most of the existing ABE access control schemes unattractive for CCN/NDN.

Herranz et al. [4] and Chen et al. [5] proposed constant ciphertext-policy ABE (CP-ABE) schemes to address the issues of client high computational cost. However, their schemes are inexpressive and based on AND gate and threshold function by the large-scale ciphertext. An outsource computational ABE scheme was proposed by Hohenberger and Waters [6] and Lai et al. [7]. These schemes have high communication cost and most of the encryption and decryption computations are outsourced. In order to reduce the policy scale, Zhou and Huang [8] proposed a minimum sum of product expression and Song et al. [9] proposed minimum linear code, respectively, to minimize the policy scale. A small-scale policy that has less ciphertext redundancy, the reduction of redundancy is limited and unstable. A compact ciphertext-policy ABE (CP-ABE) scheme was proposed by [10] to compact the policy scale and reduce ciphertext redundancy. However, the above-mentioned schemes are based on bilinear maps with high computational complexity and could not address the problem of quantum and post-quantum attacks.

To address the problems of quantum attacks, the researchers of [11] first introduced the idea of the lattice into cryptography. There has been recent progress in the area of quantum cryptography including lattice-based ABE schemes. Zhu et al. [12] proposed KP-ABE scheme using a threshold access policy for the ideal grid based on the R-LWE problem, which proved to be CPA secured. However, this scheme could not satisfy the attack on plaintext security as claimed by the authors. Instead of adopting the preceding approaches, LSSS CP-ABE access control scheme from the lightweight ideal grid was proposed by Tan et al. [13], which can resist collision attacks. Yan et al. [14] used the LSSS access structure to propose the ideal multi-agency CP-ABE scheme. Wang et al. [15] achieved an effective encryption scheme based on R-LWE with high encryption power. The decryption run time and integrity support features are based on chosen cipher-text security. In 2018, authors of [16] proposed the attribute-based encryption scheme supporting tree-access structure from ideal lattices. They used an expressive and flexible access policy by Shamir threshold secret sharing technology, including “and”, “or”, and “threshold” operations. In order to construct more efficient lattice-based ABE to resolve inefficient issues in the lattice ABE cryptosystem, the accessed structures and some components such as the trapdoor design and the matrix dimension which play a significant role in the construction of the lattice based ABE scheme need to optimize. Hence, the main contribution of our work is to propose a flexible and efficient CP-ABE access control scheme based on ring learning with error supporting reduced-OBDD for CCN/NDN.

1.1. Clarification of Problem and Contribution

In spite of the enormous benefits of the CCN/NDN technique, security challenges are some of its major concerns. These security challenges consist of the design of secured, efficient, and flexible schemes to secure cached data and also protecting data from illegal data modification, unauthorized access, as well as impersonated data dissemination and retrieval. The CP-ABE scheme is a newly preferable solution identified to achieve access control in CCN/NDN. This security scheme has special properties of encrypting with access policies. It also allows content to be self-protected when they are cached and can be accessed by many users.

However, most of these proposed CP-ABE AC schemes have some loopholes which make them unappealing. Some of these problems which we address in this paper are: i) They are not flexible, i.e., they cannot support many access policy operations such as AND, OR, NOT, and threshold gates. ii) They are inefficient, i.e., the computation and communication of secrete keys and ciphertext take a long time. iii) They vulnerable quantum attacks (i.e., they are based on bilinear maps with pairing and are not quantum secured for polynomial time quantum algorithms.

Above all, most of the proposed secured CCN/NDN information sharing systems cannot secure cached contents from some entities such as trusted service providers and cache routers. Therefore, cache routers can conspire with some users to act maliciously when the contents are cached.

To address the challenges and limitations described above we CP-ABE AC scheme which has the following characteristics:

(i) The proposed CP-ABE AC scheme from ideal lattice supports a reduced-OBDD access structure. Reduced-OBDD offers a compact and optimized access structure with fewer nodes and paths. Encryption and decryption are performed by waking on the path instead of using nodes. This means that it has a lower encryption and decryption computational time over rings.

(ii) The proposed scheme supports Boolean operations such as AND, OR and threshold gate. Also, it can support multiple subscribers of positive and negative attributes in strategy.

(iii) Our scheme is quantum secured for polynomial time quantum algorithms based on the assumption of R-LWE. Due to the algebraic construction from the ideal lattice, it is more effective than schemes based on ring learning LWE.

(iv) Our scheme has an improvement over the sample right algorithms with a stronger trapdoor and efficient sampling based on the discrete Gaussian in $O(log^c n)$ instead of $\Omega(n^2 log^2 n)$.

Finally, we integrate the proposed reduced-OBDD CP-ABE over ring LWE with CCN/NDN platform and demonstrate how it could be used to provide an access control scheme to enable content to be self-secured against quantum attack.

1.2. Methods

The attribute based encryption scheme represents a promising proposal for content centric network. However, it has some drawbacks such as computational time and flexible access control expression. To deal with these problems and to ensure efficient a secured data sharing over CCN, the following methodologies were used.

1.2.1. Flexible and Expressive Access Policy

Our scheme supports reduced-OBDD: We constructed our access policy from reduced ordered binary decision diagram. This approach is simple but very efficient and expressive. Based on recursive Shannon theorem, $f(x_1 x_2, \cdots, x_n) = \bar{x}_n \cdot f(0, x_1, x_2, x_n) + x_1 \cdot f(0, x_1, x_2, x_n)$, we constructed a reduced binary decision diagram to represent our access structure. By adopting this approach, a Threshold access structure of five levels with sixty-three (63) nodes can be reduced to six (6) nodes which can perform the same function but in a more efficient way. This structure can support the threshold gate, Boolean operations such as AND, OR, NOT, and also, multiple subscribers of positive and negative attributes in the strategy. To deal with negative attributes, we modified the proposal in [17] by attaching the negative attributes to a default attribute

1.2.2. Optimized Algorithms

Compact and optimized access policy: Reduced-OBDD offers a compact and optimized access structure with fewer nodes and links. However, instead of using the number of nodes for our encryption and decryption, we used the links between the nodes which have a direct positive impact on our encryption and decryption algorithms. The terminal nodes with constant meanings were deleted. This means that our scheme has less encryption and decryption computational time over rings.

Optimized sampling algorithm: Instead of using sample left algorithm used by various construction, we combined the theorem of MP12 [18] to construct an efficient trapdoor. We also design an optimized sampling algorithm to output an invertible matrix m. This is a significant method for delegating trapdoor and sample right algorithm with a trapdoor protocol. The matrix m is obtained from a discrete Gaussian execution time of $O(log^c n)$ with a trapdoor quality approximately $1.6(n \log q)^{1/2}$ and matrix m dimension approximately $2n \log q$. Hence, our scheme has an improved storage capacity as compared with other relevant schemes such as [19]. The performance analysis shows that the size of the master key, secret key, and the ciphertext expansion size is much lower. This is detailed in Table 1.

1.2.3. Efficient Secured Content Sharing Over CCN/NDN

The ABE scheme has a general computation loophole. To ensure an efficient secured content sharing system, we will adopt a hybrid technique by combining our proposed reduced-OBDD based ABE AC with asymmetric key encryption scheme. An asymmetric encryption scheme known to be efficient is used to encrypt the content needed by the consumer and the proposed reduced-OBDD CP-ABE AC scheme from lattice is used to encrypt the content policy which contains the password or the secret key and other relevant information about the content data to decrypt the content. The content policy is issued with a time value and periodic automatic update properties to ensure the management of our system, and also allows user's features to be updated individually

1.3. Organization

The remaining of the paper is organized as follows: In Section 2, we review some relevant related work. The preliminaries are discussed in Section 3. We demonstrate our access structure and our scheme in Section 4. The performance analysis of our scheme is presented in Section 5. The integration of our proposed scheme into CCN/NDN systems is discussed in Section 6, and this paper is concluded in Section 7.

2. Related Works

2.1. Encryption Access Control Schemes from Lattice

Lattice cryptography is considered to be the preferred cryptography system for quantum security due to its wide applicability [20] and its security proof is based on known lattice problems in the worst case of hardness. Lattices have since then achieved a lot of fame for constructing numerous diverse cryptography schemes. An efficient identity-based encryption (IBE) system from lattice was proposed by Agrawal et al. [21]. The authors of [22] proposed CP-ABE scheme lattices. Their scheme is flexible and supports (k, n) threshold access policies on Boolean attributes. Zhao and Gao [23] proposed the KP-ABE mechanism for the subclass circuit using a short size matrix secret key for the OR gate and proved to be secured against the chosen-plaintext attack in the selective model under the assumption of learning with error. Based on full-rank differences function, the authors of [24] proposed a large universe CP-ABE scheme to attain improvement in the expression of attributes and unbounded attribute space.

Unlike previous solutions, Nguyen et al. [25] presented a server-side revocable IBE scheme base on the LWE assumption. The re-encryption approach was used to allow smooth interaction between the server and the user as ensuring messages confidentiality. An efficient revocable ABE scheme was constructed by [26], their revocation of attributes and grants is based on a binary tree approach. A single random vector parameter was selected for nodes corresponding to attributes. To solve some open issues, a bonsai tree, which is a cryptography structure based on lattice, was proposed by David Cash [27]. In reference [28], the ABE scheme from LSSS based on lattices was proposed. This scheme eliminates the ranks and columns of the matrices to merge a preferred structure in the decryption stage. virtual encryption matrix in the key generation phase, which is reasonably dissimilar from the universal techniques in the present ABE schemes from lattice-based cryptography. Based on the LSSS matrix and from the lattice, an ABE mechanism was constructed using a distinct common lattice approach to execute the same task. However, the number of secret keys grows exponentially with the number of inputs which will cause a restriction to the initial parameters [29].

An efficient HIBE scheme with a new delegation mechanism was proposed by Agrawal et al. [19]. This technique does not increase the involved lattice's dimensions. In [30], a flexible ABE from lattice for multi-authority was which support AND, OR, and threshold operations. They used optimized Gaussian sampling and trapdoor algorithms to achieve a remarkable efficiency with less storage capacity. Using a standard model, the authors of [31] proposed a lattice-based threshold hierarchical ABE scheme based on a lattice. Their scheme is secured against a selective attribute set and chosen-plaintext attacks under the LWE problem without random oracle. Meanwhile, they didn't use the same attributes level.

2.2. Secured Content Centric Network (CCN/NDN)

One of the common ways of ensuring a secured content sharing on ICN is by access control approach. Information centric network systems allow inter network caches by a cached router which is presumed to be secured and honest. However, it is not always practical. Since content is cached in anywhere on the internet, content publishers have difficulties to control access to their own published content. A restricted named mechanism that restricts names to only legitimate consumers was proposed by [32]. This approach is not sufficient since the name of the content can be easily identified. To improve upon access control mechanisms in CCN (securing the content and its name) from unauthorized users, several mechanisms have been proposed, such as attribute encryption access, [33–35] proxy re-encryptions, and broadcast encryption access control schemes [36,37].

Attribute based encryption has gained popularity among other cryptographic approaches due to its special encryption properties based on policies. According to [38], the identity of legitimate users is considered as attribute set and base on that, the massage owner encrypts content to be shared based on some selected condition. Here, only users whose attributes match with that condition can extract the content for consumption. However, attribute-based encryption mechanisms need a trusted party to manage the system and regulate users' attributes which are sometimes impractical.

In [39], we proposed an efficient CP-ABE scheme for IoT CCN based on ROBDD for IoT data sharing on CCN. This scheme has a better decryption stage and offers resistance to collision attacks. The efficiency of the proposed scheme is based on the efficiency of the ROBDD structure. From our performance analysis, this scheme achieved high efficiency in terms of key generations, encryption operation and decryption operations as compared to most of the existing CP-ABE schemes proposed for IoT CCN. However, our previous access control scheme is based on bilinear maps with high computational complexity and could not address the problem of quantum and post-quantum attacks.

The proposed proxy re-encryption and broadcast encryption mechanisms hide the data and its name from the nodes of the network which sends the content to the legitimate users. However, securing the name only is not enough since an attacker can pretend to express the same interest. However, a random approach can be used to randomize the original content with some noise so that the attacker cannot find the original content. However, this technique leads to communication overheads [40].

On the whole, the aforementioned mechanisms cannot secure the content from some entities, and cache routers can conspire with the users to act maliciously when the contents are cached. Moreover, all of these access control schemes for CCN/NDN are based on bilinear maps with pairing and are not quantum secured for polynomial time quantum algorithms.

3. Preliminaries

3.1. Lattice

Definition 1. *(Lattice [41]) Given* $\boldsymbol{B} = [b_1|\cdots|b_m] \in \mathbb{R}^{m\times m}$ *as* $m \times m$ *with a linearly independent column vectors* $b_1, \dots, b_m \in \mathbb{R}^m$*. The m-dimensional lattice* Λ *generated by* $\boldsymbol{B}$ *is the set.*

$$\Lambda = \mathcal{L}(\mathbf{B}) = \left\{ y \in \mathbb{R}^m \text{ s.t. } \exists \mathbf{s} \in \mathbb{Z}^m, \qquad \mathrm{y} = \mathbf{Bs} = \sum_{i=1}^{m} s_i b_i \right\}.$$

Now, we consider an integer lattice, where Λ belongs to the set of $\mathbb{Z}^m$. We denote the determinant of Λ as $\det(\Lambda)$.

Definition 2. *([41]): For a prime* $q, A \in \mathbb{Z}_q^{n\times m}$ *and* $A \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{n}}$*, define.*

$$\Lambda_q(A)\sim = \left\{ e \in \mathbb{Z}^m \; s.t. \; \exists \mathbf{s} \; \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{n}} \text{ where } A^{\mathrm{T}} s = e (\mathrm{mod}\; q) \right\}$$

$$\Lambda_q^{\perp}(A)\sim = \{e \in \mathbb{Z}^m \ s.t.\ Ae = 0(\mathrm{mod}\ q)\}$$

$$\Lambda_q^{u}(A)\sim = \{e \in \mathbb{Z}^m \ s.t.\ Ae = u(\mathrm{mod}\ q)\}$$

Note that, if $d \in \Lambda_q^u(A)$, then $\Lambda_q^u(A) = \Lambda_q^{\perp}(A) + d$ and therefore, $d \in \Lambda_q^u(A)$ is a shift of $\Lambda_q^{\perp}(A)$.

Definition 3. *(An m-dimensional lattice Λ [41]): An m-dimensional lattice is both an additive subgroup: ($o \in \Lambda$, and $x, x + y \in \Lambda$ for every, $y \in \Lambda$) and discrete (every $x \in \mathcal{L}$ has a neighbor in $\mathbb{R}^m$ where x is the only lattice point). The minimum distance of lattice Λ is the length of a shortest non-zero lattice vector $\lambda_1(\Lambda) := min_{v \in \mathcal{L}\setminus\{0\}} \parallel v \parallel$, where $\parallel v \parallel$ denote Euclidian norm. Generally, $i - th$ successive minimum $\lambda_i\,(\mathcal{L})$ is the smallest r such that Λ has i linearly independent vectors of the norm at most r.*

Definition 4. *(Ideal lattice [41]): A lattice $\Lambda \in Z^n$ is an ideal lattice if there exists a ring $R = [x]/< f >$ and ideal $I \subseteq R$ such that Λ is associated with I.*

Definition 5. *(Gram-Schmidt norm of a basis [41]): Given $G = (g_i)_{i \in I}$ as a finite basis and $\hat{\mathrm{G}} = (\hat{\mathrm{g}}_i)_{i \in I}$ as Gram-Schmidt orthogonalization. The Gram–Schmidt norm G is the value of*

$$\|\hat{\mathrm{G}}\|\sim = \mathrm{max}_{\mathrm{i}\in\mathrm{I}}\|\hat{\mathrm{g}}_i\|.$$

There are two relevant properties of Gram Schmidt dorm and its bases which are beneficial to the construction lattices. These are: (1) They are quick to compute (The *Gram-Schmidt norm* for a general lattice is obtained by conducting the *Gram–Schmidt process to the basis of the lattice and compute the maximum length of the resultant vector*). (2) Their size can be small (The size of the lattice which we compute Gaussian sampling and the sample of the private key size should be proportional to $\|\hat{\mathrm{G}}\|$, where G is lattice basis). Therefore, it is significant that $\|\hat{\mathrm{G}}\|\sim = \mathrm{max}_{\mathrm{i}\in\mathrm{I}}\|\ \hat{\mathrm{g}}_i\|$ should be small as possible. According to [18], a full rank set G in a lattice can be converted into T with an equally low Gram–Shmidt norm $\|\hat{\mathrm{G}}\|$ of G

Lamma 1. *([18], Lemma 7.1): Given Λ as an m-dimensional lattice, there is a deterministic polynomial-time algorithm that gives an arbitrary basis of $\mathcal{L}$ and a full rank set of $G = \{g_1, \cdots, g_m\}$ in $\mathcal{L}$, outputs a basis of T of $\mathcal{L}$ satisfying $\|\hat{T}\| \leq \|\hat{\mathrm{G}}\|$ and $\|T\| \leq \|G\|\sqrt{m/2}$.*

3.2. Gaussian Sampling for a Ring

Definition 6. *(Gaussian function): Given $m \in \mathbb{Z}$ and $\mathcal{L} \subset \mathbb{R}^m$ as a positive integer greater than zero and m dimensional matrix. Let $\sigma \in \mathbb{R}$ greater than zero and $c \subset \mathbb{R}^m$. A Gaussian-shape function $\rho_{\sigma,c}(x)$ on $\mathbb{R}^m$is defined as $\rho_{\sigma,c}(x) = exp(-\pi[(\parallel x - c \parallel^2)/\sigma^2])$. For a matrix $\mathcal{L}$, we define the discrete of $\rho_{\sigma,c}$ as $\rho_{\sigma,c}(\mathcal{L}) = \sum_{x \in \mathcal{L}} \rho_{\sigma,c}(x)$. The discrete Gaussian distribution over $\mathcal{L}$ set as $\mathcal{D}_{\mathcal{L},\sigma,c}$ and then $\forall y \in \mathcal{L}$, the discrete Gaussian distribution over $\mathcal{L}$ is defined as:*

$$\mathcal{D}_{\mathcal{L},\sigma,c}\,(\mathcal{L}\,) = \rho_{\sigma,c}(y)/\rho_{\sigma,c}(\mathcal{L}).$$

3.3. Some Significant Algorithms

3.3.1. Algorithm Generation of Trapdoor

Theorem 1. *$LatticeTrapGenAlg\ (R, D) \rightarrow (\hat{e}, T_{\hat{e}})$. A probabilistic polynomial-time (PPT) algorithm in an existence accepts inputs of $R \in Z_q^{n\times m}$, $D \in Z_q^{n\times n}$, parameters $q, n \geq 1$, $m = O(log\ q), w = nt$, where t=$\lceil log_2\ q \rceil$. $\rho \in Z\lfloor \mathcal{X} \rfloor$ is a polynomial with n degree. The algorithm outputs $(\hat{e}, T_{\hat{e}})$. $\hat{e} = (\hat{e}_1, \hat{e}_2 \cdots, \hat{e}_u)^T =\in Z_q^{n\times m}$, statistically close to uniform. $\hat{e} = [R|DP - RT_{\hat{e}}]$, Where $\in Z_q^{n\times w}$, $T_{\hat{e}} \in Z_q^{m\times w}$ and a small trapdoor bases for lattice $\Lambda_q^{\perp}({A'}_{\rho}^{T})$ which satisfies $L\|T_{\hat{e}}\| \leq (\sqrt[\hat{O}]{n})$.*

3.3.2. Algorithm for Preimage Sampling

Theorem 2. $PreimSampAlg(\hat{e}, T_{\hat{e}}, P, \alpha, \sigma) \rightarrow \hat{a} \in Z^m$. *A PPT algorithm accepts inputs of* $e \in Z_q^{n \times m}$ *as a matrix, where* $q \geq 2$ *and* $m \geq 2n\ log\ q$, $T_e \in Z_q^{m \times m}$ *as the basis of a trapdoor for* $\Lambda_q^{\perp}(M)$*, expected image and parameter for Gaussian is* $\sigma \geq\ O(\sqrt{n\ log\ q})$ *and output* $\hat{a} \in Z^m$ *that satisfies* $A\hat{a} = \alpha\ mod\ q$*. Based on* $PreimSampAlg(M, T_M, \alpha, \sigma)$*, a new preimage sampling algorithm over rings for* $GenIdealSamPreimAlg()$ *is constructed.*

GenIdealSamPreimAlg($\hat{e}, T_{\hat{e}}$, α, σ) → ($\hat{g} \in R$). The algorithm takes an input of $\hat{e} \in R_q^m$ as a vector, $T_{\hat{e}} \in Z_q^{mn \times mn}$ trapdoor of $\Lambda_q^{\perp}\left(A'^{T}_{\rho}(\hat{e})\right)$, α ∈ R_q as expected image and a parameter of Gaussian σ > $\|T_{\hat{e}}\|.\,\omega(\sqrt{\log m})$ and output $\hat{g} \in R_q^m$ that satisfies $\hat{e} \otimes \hat{g} = \alpha$. Here, we have:

a Encode:

$$E = \Lambda_q^{\perp}\left(A'^{T}_{\rho}(\hat{e})\right) \in Z_q^{n \times mn}$$

b

$$t =\ PreimSampAlg(E, T_{\hat{e}}, P, \alpha, \sigma) \in Z_q^{n \times mn}$$

c

$$\hat{g} = Map^1(t) \in R_q^m,\ \hat{g} \sim D_{Z^{mn}, \sigma}$$

3.4. Decision R-LWE Problem

Init*:* The adversary chooses a specific access structure and sends to the Challenger

Given n as security parameter, let d and q be an integer that depends on n. Where $f(x) = (x^n + 1)$ and $R_q = R/qR$, let $R = Z[x]/(f)$. Given a distribution χ over R_q depending on n, the Decision learning with error problem instance consist of access to an unspecified challenge oracle o, either a noisy pseudo-random sampler O_s, for random secrete key $S \leftarrow R_q$; or a truly random sampler $O_\$$. The Decision R-LWE problem is to distinguish the sampling between O_s and $O_\$$, which perform respectively as follows;

O_s: Given a uniform distribution constant invariant value across invocation as $S \in Z_q^n$, a new sample $x_i \in Z_q$ from χ and a uniform sample $u \in Z_q^n$. Output a sample of form as $(u_{i,} v_i = u_i . u_i^T S + x_i) \in Z_q^n \times Z_q$.

$O_\$$: An exact uniform output sample (u, v) drawn from $Z_q^n \times Z_q$.

The aim of the decision ring-LWE problems is to allow repeated quarries to be sent to the challenge oracle O. The Attacker's algorithm decides the decision ring-learning with error problem if $|\Pr[Attacker^{O_s} = 1] - \Pr[Attacker^{O_\$} = 1]|$ is non-negligible random value for $s \in Z_q^n$. Given $\lfloor x \rceil$ defining

3.5. Access Structure

Assuming $P = \{p_1, p_2, \ldots p_n\}$ is a set of parties. Let 2^p represent subsets contained in $\{p_1, p_2, \ldots p_n\}$ and $\in 2^p$. The collection of $ST \in 2^{P=\{p_1, p_2, \ldots p_n\}}$ is known as an access structure. The set contains in $ST \in 2^{P=\{p_1, p_2, \ldots p_n\}}$ are called authorize sets and sets $ST \notin 2^{P=\{p_1, p_2, \ldots p_n\}}$ are called unauthorized sets. The access is monotone if $for\ all\ Q, A\text{:}\ if\ A \in ST$ and $A \subseteq Q$ then $Q \in ST$.

3.6. Reduced Ordered Decision Diagram (Reduced-OBDD)

Reduced-OBDD is based on a fixed ordering of variables and has the additional property of being reduced. This means that it is irredundant, unique, and recovers the important canonicity property. Thus, for a fixed variable ordering, each Boolean function has a canonical (unique) representation as a Reduce-OBDD and checking if they are of equal or the same successors. If there are two distinct nodes u and v have the same variable name and low and high successor, i.e., if

$var(u) = var(v), low(u) = low(v)$ and $high(u) = high(v)$, implies $u = v$ and no variable node u has identical low and high successor, i.e., $low(u)$ and $high(u)$.

3.7. Ciphertext-Policy Attribute Base Encryption Model

The CP-ABE basic algorithms include the following four fundamental operations (Setup, Encrypt, KeyGen, Decrypt).

Setup (λ): This algorithm takes security parameter λ as input and outputs the public key PK and master key MK.

Encrypt (PK, MK, A): This algorithm takes public parameter PK, plaintext M, and access policy A, to output Ciphertext CT

KeyGen (MK, S): The algorithm takes masters key MK and attribute set S as input and outputs the secret key SK.

Decrypt (PK, CT, SP): This algorithm takes in public parameter PK, ciphertext CT, and a secret key SK as input and outputs the message M

3.8. Selective Set Model

A CP-ABE is secured in a selective -set model if the PP adversary has at most a negligible advantage in the game below.

Initial: The adversary Adv. declares the attribute set AS which he wants to challenge.

Setup: The setup algorithm is run by the challenger and sends the Pk to the Adv.

Phase 1: The Adv. is allowed to make a private request of its choice as long as $\mathrm{AS} \in \mathrm{A}$

Challenge: The Adv. sends two messages of equal length, M_0 and M_1 the challenger.

The challenger randomly selects b and encrypt M_b using A. The ciphertext is sent to the Adv.

Phase 2: Repeat Phase 1.

Guess: Adv. output a guesses $b^1$of b. The advantage in the security game is defined as $Adv = |\Pr[b = b^1] - 1/2$

4. Our Construction

4.1. Constructing Boolean Function of an Access Policy

We suppose the access policy of a Boolean function is $f(u_0, u_1, \cdots u_{n-1})$. Where $(0 \le i \le n-1)$ and n as the whole number of attributes, denotes a sequential predefined access policy number which is represented as $u(0 \le i \le n-1)$. The function $f(u_0, u_1 u_{n-1})$ is converted between fundamental logical operations such as AND, OR, and NOT

An operation is considered as threshold gate $T(t, n)$ if and only if t attributes of a subset n can complete the operation successfully. To be able to decrypt a message in a security system, a user must be able to complete some specific threshold operations. To construct a Boolean function of a given $T(t, n \in N)$, Where N is the attribute set, extract all the subset of N with t attributes and separately compute the whole number of subsets $C(n, t) = Com1, Com2 \cdots Com_{C(n,t)}$ by using permutation and combination. This is followed by the construction of a separate set level conjugate for each subset $C(n, t) = Con1, Con2 \cdots Con_{(n,t)}$. Finally, obtain the Boolean function of $f(t, n) = \vee_{i=1}^{C(n,t)} Con_i$ by a disjunctive operation on $C(n, t)$.

4.2. Reduced- OBDD Access Structure Construction

To construct reduced-OBDD for Boolean function $f(x_1 x_2 \cdots x_n)$, we use the recursive algorithm (Algorithms 1 and 2) based on the expansion theorem of Shannon. To obtain a specific and unique reduced-OBDD, the definition of the variable ordering must be specified since different ordering results to different kinds of diagrams. Given a logic function in terms of selected inputs and the required input for logic synthesis using a multiplexer. For any Boolean function $f(x_1 x_2 \cdots x_n)$ can be expressed as $f(x_1 x_2, \cdots, x_n) = \bar{x}_n \cdot f(0, x_1, x_2, x_n) + x_1 \cdot f(0, x_1, x_2, x_n)$. The process based on Shannon's expansion theorem is described as follows: Let $N = \{0, 1, 2, \cdots n\}$ be node numbers where the low terminal node is 0 and the high terminal node is 1. However, the terminal nodes have specific meanings and their attributes may not be considered. The variable ordering Ω related to N is $\Omega = (x_0 <, x_2 < x_3 < \cdots < x_n)$. The table, Table 1 is the inverse of the table Table 2 which stores the reduced-OBDD. In Algorithm 1, Table 1 is initialized to be ones (1) and zeros (0) lookup function Table 1: $(w, id, low, high)$ maps node w to its attributes $var(w) \longrightarrow id$, $low(w) \longrightarrow low$ and $high(w) \longrightarrow high$. To construct an ordered binary decision diagram from the *id, low,* and *high* if there must be an existence of the node w with variable key $var(w) \longrightarrow id$, $low(w) \longrightarrow low$, and $high(w) \longrightarrow high$. In Algorithm 2, Table 2 is initialized to be empty and find out if there exist of id, low and high in.

Algorithm 1 Build Redeuced-OBDD

```
function BUILD[Table 1, Table 2](id, low, high)
    if  low== high then
        return low
    end if
    If element (TABLE2, id, low, high) then
        return lookup(TABLE2, id, low, high)
    end if
    If low<> high then
        w=insert(TABLE1, ID, low, high)
        return insert(TABLE2, id, low, high)
    end if
end function
```

Algorithm 2 Construct Reduced-OBDD

```
Function CONSTRUCT [TABLE1, TABLE2](t, i)
    if i > n then
        if t== false then
            return 0
        end if
        if t == true then
            return 1
        end if
    end if
    if i ! > n then
        return q0= CONSTRUCT(t[0/xi], i+1)
        return q1= CONSTRUCT (t[1/xi], i+1)
        return BUILD(t, i)
    end if
end function
```

Use the lookup function to find Table 2 (id, low, high) and use insert function to map (id, low, high) to w and assign node serial w with attributes id, high, and low. The algorithm references the attributes of serial w in Table 1 with in Table 2 by recalling the BUILD function in Algorithm 1. Let Table 2: $(id, low, high) \longrightarrow w$ maps attributes $(id, low, high)$ to w such that for all variables nodes w, Table 1 $(w) \longrightarrow (id, low, high)$ *if* Table 2 (id, low, high)⟶ w. After the construction of all nodes Nd of the reduced-OBDD, the final expression is obtained as $Reduced - OBDD = Nd^i_{id}$, where i denote all the attributes in the structure and id is the set containing the serial numbers of non-leaf nodes. The final table of Nd^i_{id} $(w, id, high, low)$ contains the id of the current node id, the id of the attribute in the current node i, the id of the high branch $high$ and the id of the low branch low. Hence, the access structure $\tau_s = \{Nd^f_{V1}, Nd^e_{V2}, Nd^d_{V3,}Nd^c_4, Nd^b_{V5}, Nd^a_{V6}\}$

4.3. Satisfying Reduced-OBDD Structure

Let $\mathcal{T}$ be access structure, attributes set be A_s and let the valid path be the path from the root node to the terminal (1) be $Vx \longrightarrow Vx \longrightarrow Vx \cdots, \rightarrow (1)$ as shown in Figure 2. Based on node values, a recursive comparison is conducted, starting from the root nodes to the leaf nodes. Thus, for a non-leaf node with an attribute of $i \in A_s$ is 1, send to the high branch node, otherwise send to the low branch node. This process is repeated until it reaches the leaf node. The set A_s satisfied τ if the terminal node is (1). Otherwise, outputs fail. The attributes set A_s must satisfy the access structure $\mathcal{T}$ (i.e., $A_s \vDash \mathcal{T}$) when the leaf node is lastly reached.

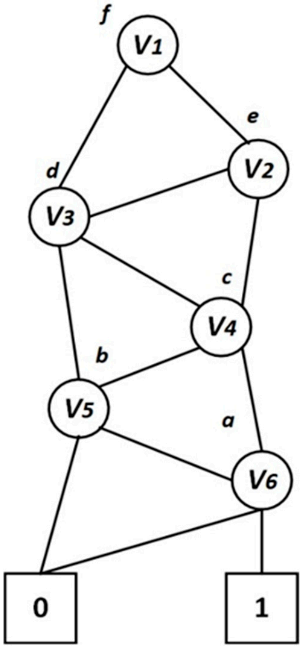

Figure 2. Reduced-OBDD representation of Ω.

4.4. Construction Of Reduced-OBDD ABE AC From Lattice

Our proposed CP-ABE scheme supports positive a_i and negative $\neg a_i$ attributes. In a brief statement, we have $a_{\underline{i}}.(a_i \text{ or } \neg a_i)$ where $a_{\underline{i}}$is a default value. Let U represent attribute sent with serial numbers, our algorithms are described below.

Setup (γ, U): The algorithm is given an input of γ and U as security parameter and attributes set respectively. Denoting $\mathrm{P} \in \mathrm{Z}_{\mathrm{q}}^{\mathrm{n}\times\mathrm{w}}$ as a public parameter, let $\mathrm{D} \in \mathrm{Z}_{\mathrm{q}}^{\mathrm{n}\times\mathrm{n}}$ be matrix. Randomly select $R \in Z_q^{n\times\overline{m}}$ and trapdoor $\mathrm{T_A} \in \mathrm{Z}_{\mathrm{q}}^{\overline{\mathrm{m}}\times\widehat{w}}$ with a size of less than or equal to $\sqrt{m}.w(\sqrt{\log q})$. Execute the LatticeTrapGenAlg Algorithm to generate a random matrix $\mathrm{A}_i = \left[\mathrm{R}\middle|\mathrm{DP} - \mathrm{RT}_{\mathrm{A}_i}\right] = A_i^0 R_{i,j}$, where $\mathrm{A}_i{}' = A_i R_{i,j}^{-1}$ is inverse of A_i. Randomly choose a uniform vector $\boldsymbol{\alpha}^{\mathrm{T}} \in \mathrm{Z}_{\mathrm{q}}^{\mathrm{n}}$ and finally, output the public parameter and the masters key as:

$$PP = \{\boldsymbol{\alpha}, \{\mathbf{A_i},\}_{i=1}^{U}\} \tag{1}$$

$$MK = \{\mathbf{T_{A_i}}\}_{i=1}^{U} \tag{2}$$

KeyGen $(MK, A_s) \rightarrow (SK)$: Given master key MK and the set of users attribute $A_s = \{a_0, a_1, a_2, \cdots, a_i\}$. Set any a_i which doesn't belong to A_s as a default value $\neg a_i$ and execute the key generation process is as follows:

Define $y_{a_{\underline{i}}}$ for any $a_i \in A_s$; if $a_i \in A_s \wedge a_{\underline{i}} = a_i$ and let $y_{a_{\underline{i}}} = y_a$ else, set $y_{a_{\underline{i}}} = y'_a$

Generate $A'_{i,j} = A_i R_{ij}^{-1}$ and a trapdoor matrix $T_A \in Z_q^{\overline{m}+w}$ for $\Lambda\frac{1}{q}(A'_{i,j})$ and a secrete share $\boldsymbol{\alpha_i}$ for each a_i.

Execute GenIdealSamPreimAlg $(A, T_{A_{ij}}, \mathrm{P}, \boldsymbol{\alpha}_i, \sigma,)$ to output $\mathfrak{d}_{i,j} \in Z_q^{\bar{m}+v} = Z_q^m$, where $\boldsymbol{\alpha_i} = A'_{i,j}\mathfrak{d}_{i,j}$.

Set the private key as

$$SK_u = \left\{ \left(\mathfrak{d}_{i,j}\right)_{ai,j \in A_S} \right\} \tag{3}$$

$Encryption(PP, M, \mathcal{T}) \rightarrow (CT)$: The algorithm is given public parameter PP, the message M, and the access structure $\mathcal{T} = Node_{id}^{i}$ $|\mathrm{id} \in \mathrm{ID}, \mathrm{i} \in \mathrm{I}$. Let (Y, Y') be a valid and invalid path. Denote the valid paths as $V_p = V_1, V_2, \cdots, \rightarrow V_y$. The information of the attributes in the path V_y is $\sum_{y_i}$ and the ciphertext of y is denoted as $C_{V_y} = \sum_{i \in I} y_i . s = s_i$. Where s is a random parameter and y_i is associated with the set of attributes i in $\mathcal{T}$ and s_i is the secret to be shared. The relationship between i and (Y, Y') is shown in Figure 3.

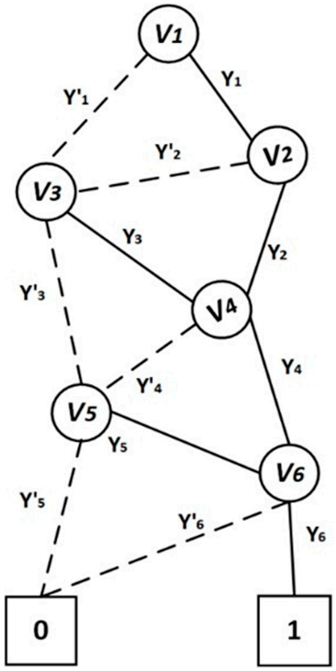

Figure 3. The relationship between paths (Y_i, Y_i') and i.

Randomly generate parameter $s \in R_q$ and error terms $\theta, \theta_{i,j} \in \mathcal{X}$.

The encryption algorithm follows the following steps:

$$\mathrm{C}_{\mathrm{i,j}}^{(\mathrm{l})} = \mathrm{A'}_{\mathrm{i,j}}^{\mathrm{T}} . \mathrm{s_i} + \theta_{\mathrm{i,j}} \bmod \mathrm{q} \tag{4}$$

Set

$$\mathrm{C} = \boldsymbol{\alpha}^{\mathrm{T}}\mathrm{s} + \theta + \mathrm{m}\left\lfloor \frac{\mathrm{q}}{2} \right\rfloor \bmod \mathrm{q} \tag{5}$$

Then, output ciphertext as $CT = \left(C, \left\{\mathrm{C}_{\mathrm{i,j}}^{(\mathrm{l})}\right\}_{i,j \in \mathcal{T}}\right)$.

$Decryption\ (CT, PP, SK) \rightarrow (M)$: The decryption algorithm takes an input of ciphertext (CT), public parameter (PP), and secret key (SK). Perform recursive Algorithm 3. The algorithm defines the root node as the current node and extracts the current id and the $index$. The algorithm conducts recursive operations based on a high branch node and the low branch node. If any node is a non-leaf node, the algorithm sets it as a current node. The process continues until it reaches the leaf nodes. Based on the high branch node: if the $high\ branch\ node\ is\ a\ non - leaf\ node$, set it as a current node; else if the high branch of the node is the $low\ leaf\ node$ (0), the algorithm is aborted. Otherwise, the algorithm stores the information in the path next to the leaf *node 1*. Based on the low branch node, if the low branch node is a non-leaf node, set it as current node; else if the

$low\ branch\ node\ is\ leaf\ node\ (0)$, the algorithm is aborted; else if the node on the high branch node Based on the high branch node low branch is the high leaf node, the algorithm stores the path to the leaf node (1). Define $\bar{\sigma}_{i,j} = \sigma_{i,j}\widehat{w}(\sqrt{\log m})$ as Gaussian parameter and continue with the below computation recursively.

Algorithm 3 Decryption Process

```
1:  look for the node with serial number 2
2:  Define it as the new node
3:  Extract the node details $Node_{id}^{i}$ include in the node
4:      if $i \in set \wedge i = i$ then
5:              seek the high-branch-node of the new node based on the high order
6:          if high-branch -= = 0 then
7:                  end the process
8:          end if
9:              if high-branch = = 1 then
10:                 store the root $\rightarrow 1$ path
11:             end if
12:             if high-branch ==non-leaf-node then
13:                 go to line 2
14:             end if
15:     end if
16:     if $i \in set \wedge = \neg i \vee i \notin set$ then
17:         Seek the low-branch-node of the new node based on the low order
18:             if low-branch == 0 then
19                  end the process
20:             end if
21:                 if low-branch = =1 then
22:                     store the root $\rightarrow$1 then
23:                 end if
24:                 if low-branch = = non-leaf-node then
25:                     go to line 2
26:                 end if
27:     end if
```

Compute Lagrange coefficients L_I, as $\sum_{ai,j\in A_s'} L_I s_I = s(mod\ q)$ and set

$$M = C - \sum_{ai,j\in A_s'} L_I \mathfrak{d}_{i,j}^{T} c_{i,j}^{(l)} \tag{6}$$

If $|M' = \lfloor q/2 \rfloor| < \lfloor q/4 \rfloor$, the system output 1, else output 0

4.5. Correctness and Security Proof

In this section, we provide the security proof and the performance achieved by this work.

4.5.1. Correctness

In order to decrypt $CT = (C, \{C_i\}_{i\in\tau})$ we have

$$\begin{aligned} M = C - \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T c_{i,j}^{(l)} &= \boldsymbol{\alpha}^{\mathrm{T}}\mathrm{s} + \theta + \mathrm{m}\left\lfloor\frac{\mathrm{q}}{2}\right\rfloor - \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T.\,(\mathrm{A'}^{\mathrm{T}}_{\mathrm{i,j}}.\,\mathrm{s_i} + \theta_{\mathrm{i,j}}) \\ &= \boldsymbol{\alpha}^{\mathrm{T}}\mathrm{s} + \theta + \mathrm{m}\left\lfloor\frac{\mathrm{q}}{2}\right\rfloor - \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T.\,(\mathrm{A'}^{\mathrm{T}}_{\mathrm{i,j}}.\,\mathrm{s_i}) \\ &+ \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T.\,\theta_{\mathrm{i,j}}) \\ &= A'_{i,j}\mathfrak{d}_{i,j}.\,\mathrm{s} + \theta + \mathrm{m}\left\lfloor\frac{\mathrm{q}}{2}\right\rfloor - \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T.\,(\mathrm{A'}^{\mathrm{T}}_{\mathrm{i,j}}.\,\mathrm{s_i}) \\ &+ \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T.\,\theta_{\mathrm{i,j}}) \ = M\lfloor q/2\rfloor + \left(\theta - \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T \theta_{i,j}\right) \end{aligned} \tag{7}$$

where the error term is: $\left(\theta - \sum_{ai,j\in A'_s} L_l\left|\mathfrak{d}_{i,j}^T\theta_{i,j}\right|\right)$.

It is required to choose the parameters such that considering the overwhelming probability (w.h.p) of

$$|\ \theta - \textstyle\sum_{i=1}^{I} L_i \sum_{ai,j\in A'_s} L_l \mathfrak{d}_{i,j}^T \theta_{i,j}\ | \le |\theta| + \sum_{i=1}^{I} L_i \sum_{ai,j\in A'_s} L_l \left|\mathfrak{d}_{i,j}^T\theta_{i,j}\right|. \tag{8}$$

$\left|\mathfrak{d}_{i,j}^T\right| \le \bar{\sigma}_{i,j} m \widehat{w}(\sqrt{\log m})$ with w.h.p, we have by PreimSampAlg $(\hat{\mathrm{e}}, \mathrm{T}_{\hat{\mathrm{e}}}, \mathrm{P}, \alpha, \sigma) \rightarrow \hat{\mathrm{a}}$ such that, $\left|\mathfrak{d}_{i,j}^T x_{i,j}\right|$ is bounded by w.h.p by $\left|\mathfrak{d}_{i,j}^T x_{i,j}\right| \le q\alpha_{i,j}\sigma_i m v(\log m) + \sigma_{i,j} m^{\frac{3}{2}} \widehat{w}(\sqrt{\log m})$.

For our trapdoor operation, we choose $m \approx 2n\log q$ to ensure correctness which is less than $\frac{q}{5}$ w.h.p and set $\alpha_{i,j} <\ qv\left(\sqrt{\log m}\right) +\ q\sigma_{i,j} m \widehat{w}(log\ m)]^{-1}$

$$\mathrm{q} > \sigma_{\mathrm{i,j}}\mathrm{m}^{\frac{3}{2}}\,\widehat{w}(\sqrt{\log \mathrm{m}}) \tag{9}$$

4.5.2. Security Proof

Theorem 3. *If the $\left(Z_q, n, \psi_\alpha\right) - LWE$ notion holds, then with a negligible advantage of ε, there is no polynomial-time adversary $\mathcal{A}$. that can selectively win the security game of our system.*

Proof: Assuming there is PPT $\mathcal{A}$ attack on the proposed efficiently secured scheme with an advantage of $\varepsilon > 0$, then there exists an algorithm that can distinguish $\left(Z_q, n, \psi_\alpha\right) - LWE$ problem with an advantage of ε. The problem of LWE is provided as sample oracle O, which can be really random $O\$$ or noisy pseudo-random for some secret key $S \in Z_p^n$. The challenger's algorithm Sim simulates attack environment and exploits $\mathcal{A}$ to which oracle O is given.

Initialize: Adversary $\mathcal{A}$, sends the access structure $\tau^* = \{Nd_{id\in ID}^{i\in I}\}$ to the challenger's Simulator $\mathcal{B}$.

Instance: $\mathcal{B}$ makes a request to the oracle and the oracle responds by sending new pairs of $(\varpi_1, \upsilon_1) \in Z_q^n \times Z_q$, where $i \in \{\,1,2,\cdots,I\}$ to obtain $m\sum_1^I s_i + 1$. Thus

$$\{(\varpi_1, \upsilon_1)\}$$

$$\{(\varpi_1^1, \upsilon_1^1), (\varpi_1^2, \upsilon_1^2), \cdots, (\varpi_1^m, \upsilon_1^m)\}$$

$$\{(\varpi_2^1, \upsilon_2^1), (\varpi_2^2, \upsilon_2^2), \cdots, (\varpi_2^m, \upsilon_2^m)\}$$

$$\Big\{\Big(\varpi^1_{\sum_1^I s_i+1.}, \upsilon^1_{\sum_1^I s_i+1.}\Big), \Big(\varpi^2_{\sum_1^I s_i+1.}, \upsilon^2_{\sum_1^I s_i+1.}\Big), \cdots,$$

$$\Big(\varpi^m_{\sum_1^I s_i+1.}, \upsilon^m_{\sum_1^I s_i+1.}\Big)\Big\}$$

Target: $\mathcal{A}$ makes an announcement of the set of attributes that it is intended to challenge

Setup: The public parameters are generated by $\mathcal{B}$. Let's denote υ as ϖ_1.

For $A_{i,j} \in {A_s}^*$, generate

$A_{i,j} = (\varpi^1_{\sum_{p=1}^I s_p + j}, \varpi^2_{\sum_{p=1}^I s_p + j}, \cdots,\ \varpi^m_{\sum_{p=1}^I s_p + j})$ where $i = (1, \cdots, I)$ and $j = (1, \cdots, s_I)$

From

$$\left\{\left(\varpi^{1}_{\sum_{p=1}^{i} s_p+j}, \mathcal{v}^{1}_{\sum_{p=1}^{i} s_p+j}\right), \left(\varpi^{2}_{\sum_{p=1}^{i} s_p+j}, \mathcal{v}^{2}_{\sum_{p=1}^{i} s_p+j}\right), \cdots,\right.$$
$$\left.\left(\varpi^{m}_{\sum_{p=1}^{i} s_p+j}, \mathcal{v}^{m}_{\sum_{p=1}^{i} s_p+j}\right)\right\}$$

Obtain

$$A_i^0 = \sum_{j=1}^{s_i} A_{i,j} \tag{10}$$

$\mathcal{B}$ outputs a matrix for each $a_{i,j}$ where attributes $a_{i,j} \notin A_s{}^*$, by running a trapdoor algorithm to generate a random matrix $R^*_{i,j} \in Z_q^{m\times m}$ and the computes

$$A'^*_{i,j} = A_i R^*_{i,j}$$

Using $A_{i,j}$ as an input, $\mathcal{B}$ generates a random matrix $R^*_{i,j} \in Z_q^{m\times m}$ and a trapdoor $T_{A^*_{i\prime j}} \in Z_q^{\bar{m}\times u}$ for $\Lambda_q^{\perp}(A'^*_{i,j})$

Finally, $\mathcal{B}$ outputs $A_i = A_i^0 R_{i,j}$ and set $PP = \{(A_i)_{i\in A_s,}\boldsymbol{\alpha}\}$ to the $\mathcal{A}$.

Phase 1: $\mathcal{A}$ sends a private key request for a set of attributes $\mathrm{A_G}^* = \{\mathrm{a}_{\mathrm{s}_1}^*, \mathrm{a}_2^*, \cdots, \mathrm{a}_\mathrm{j}^*\}$, where $\mathrm{A_s}^* \Vdash\neq \mathcal{T}\ \forall$ ai.

$\mathcal{B}$ computes $\boldsymbol{\alpha}_\mathbf{i}$ share of α for each $\mathrm{a_i}$. For any legitimate path, there must exist an attributes $\mathrm{a_j} \in \mathrm{A_I}$ satisfying $\mathrm{a_j} \in \mathrm{A_s}^* \wedge \mathrm{a}_{\underline{\mathrm{j}}} = \neg\mathrm{a_j}$or $\mathrm{a_j} \notin \mathrm{A_s}^* \wedge \mathrm{a}_{\underline{\mathrm{j}}} = \mathrm{a_j}$. Generally, $\mathcal{A}$ attributes satisfy the condition $\mathrm{a_j} \notin \mathrm{AS}^* \wedge \mathrm{a}_{\underline{\mathrm{j}}} = \mathrm{a_j}$ and each attribute is apportioned as follows: $\mathrm{a_j} \notin \mathrm{A_s}^* \wedge \mathrm{a_j} = \mathrm{a_j}, \underline{\mathrm{y}}_{\mathrm{a_j}} = \mathrm{m}\cdot \mathrm{y}'_{\mathrm{a_j}}$; for $\mathrm{a_i} \neq \mathrm{a_j}$.

$\mathcal{B}$ runs the key generation algorithm to generate $\mathrm{A'_{ij}} = \mathrm{A_i R_{ij}^{-1}}$ and a trapdoor matrix $\mathrm{T_A} \in \mathrm{Z_q^{\bar{m}+w}}$ for $\Lambda\frac{1}{\mathrm{q}}(\mathrm{A'^*{}_{ij}})$ and invokes $\mathrm{GenIdealSamPreimAlg}(\mathrm{A}, \mathrm{T_{A_{ij}}}, \mathrm{P}, \boldsymbol{\alpha}_\mathrm{i}, \sigma,)$ function to output $\partial_{\mathrm{i,j}} \in \mathrm{Z_q^{\bar{m}+v}} = \mathrm{Z_q^m}$ and set the private key of $\mathrm{a_j}^*$ as $\mathrm{SK_u} = \left\{\left(\partial_{\mathrm{i,j}}\right)_{\mathrm{ai,j} \in \mathrm{A_s}}\right\}$ to the $\mathcal{A}$

Challenge: $\mathcal{A}$ agrees to accept the challenge and submits challenge message $(m_0, m_1) \in \{0,1\}$ with the attribute set $a_j{}^*$ and flips a coin to generate randomly $m \in (0,1)$. $\mathcal{B}$ generates a ciphertext as $CT^* = (C_0^*, \left\{C_{i,j}^{(i)*}\right\}, \tau)$ to $\mathcal{A}$ where:

$$C_0^* = \alpha^T s + \theta + m\left\lfloor\frac{q}{2}\right\rfloor \bmod q \tag{11}$$

$$C_{i,j}^{(i)*} = A'^T_{i,j}.s_i + \theta_{i,j} \bmod q. \tag{12}$$

It is clear that the encrypted message CT^* is valid encryption of m under the access policy of A_s if $O = O_\$$. The encrypted message is uniform in (Z_p, Z_q^m) and $O = O'_\$(\mathcal{v}, \mathcal{v}_{i,j})$ is uniform in (Z_p, Z_q^m).

Phase 2: $\mathcal{A}$ continues by repeating Phase 1

Decision: $\mathcal{A}$ outputs a guess m' for m. If $m = m'$. The challenger considered the samples O' to be O_s sample, else it guesses them as $O_\$$ samples.

Assuming the adversary $\mathcal{A}$ can correctly guess m with a probability of at least $1/2 + \varepsilon$. Then $\mathcal{A}$ can make a decision of the decision ring-LWE problem with an advantage of

$$\left(\frac{1}{2}\right) Prob.[m' = m|(w,u) \leftarrow O_s] + \left(\frac{1}{2}\right) Prob.[m' = m|(w,u) \leftarrow O_\$]$$

$$= \left(\frac{1}{2}\right) \times \left(\frac{1}{2} + \varepsilon\right) + \left(\frac{1}{2}\right) \times \left(\frac{1}{2}\right) = \frac{1}{2}\varepsilon$$

5. Performance Analysis

5.1. Complexity Analysis

The complexity analysis of our scheme is based on the performance of the Boolean operations, the factors that affect the communication time and the factors affecting the execution time. The complexity of the Boolean operations depends on the size of the reduced-OBDD. For a Boolean circuit of $1- out - of - n$ input bit (OR gates) or $n - out - of - n$ input bit (AND gates,) designed as an output gate, the circuit size of the Boolean function f is the same as the size of the reduced-OBDD structure. Also, the complexity of the reduced-OBDD Boolean function is equal to the reduced depth of Boolean function f. For the function $f_1(w_0, w_1, w_{2,} w_3) = w_0 + w_1 w_2 + w_1 w_3 + w_2 w_3$ with ordering $\pi: w_0 < w_1 < w_2 < w_3$, the size of the reduced-OBDD is $2n$. This could either be linear or exponential depending on the variable ordering. The complexity of the Boolean function operations also depends on the number of nodes in the reduced-OBDD. That is to say, for the AND gate, the various operations of our scheme are expressed as $n - out - of - n$ threshold while the OR gate and NOT gate are expressed as $1 - out - of - n$ threshold. The Boolean operation considers all the nodes of the reduced-OBDD with the complexity of $O(n)$, where n is the number of nodes in the reduced-OBDD. To achieve a better runtime, we deleted the leaf nodes which have specific meanings.

We also improved on the execution and communication time, by reducing some parameters of our scheme such as the size of the trapdoor, the public parameters, the master key size, the secret key size, and the ciphertext. The size of the matrix m is reduced to $m \approx 2n \log q$ to output a reduced and better trapdoor. This implies a reduction in storage and communication cost. The size of the secret key depends on the end user's attributes and the size of the matrix column. The size of our public parameter is smaller due to the small lattice size.

Hence, the complexity of our key generation and decryption algorithm is $O(1)$,. The execution time of the encryption, decryption, and the resulting ciphertext relates to the number of the legitimate paths in the reduced-OBDD instead of the nodes which directly improve the execution, storage and sharing times

5.2. Discussion of Simulated Result

In this section, we compare our scheme with some relevant existing schemes. The implementation of this work was conducted on an Intel i7-8700 processor at 2.53 GHz and 8GB memory running Windows 10 operating system of 64 bits. Our scheme was simulated with PALISADE library 1.3 on C++ [42].

The factors considered in the implementation result are execution time and storage capacity of ciphertext, key generation, encryption, and decryption.

Table 1 summarizes the comparison analysis of our proposed scheme with other schemes in terms of key generation, encryption and decryption operation times. The parameters were set as follows: lattice base 1024, 80-bit security, modulus as $log_2 q = 24$, the attribute universe, U was set as 100, and the sample of attributes used in our encryption was set as $l = 10, 20, 30, 40$ and 50. In our scheme, for a ciphertext with 50 attributes, the key generation, and the encryption and decryption operations were completed at $89.8, 33.59$ and 1.29 $milliseconds$ respectively. Although our key generation was a bit slower, the execution time of our scheme had a better performance in encryption and decryption operations than the schemes in [28], [31] and [24].

Table 1. Comparing the execution time of some related works (ms).

Scheme	KeyGen	Encryption	Decryption
	$\boldsymbol{l} =$ **(10 / 20 / 30/40 / 50)**	$\boldsymbol{l} =$ **(10 / 20 / 30 / 40/ 50/)**	$\boldsymbol{l} =$ **(10 / 20 / 30/ 40 / 50)**
[28]	(57.6/69.7/78.9/ 91.1/99.8)	(16.13/21.32/27.39/33.91/36.12)	(0.79/0.90/1.38/1.58/1.79)
[31]	(73.6/82.5/91.8/102.8/119.8)	(21.78/27.58/33.84/37.12/47.86)	(1.66/1.71/1.98/2.15/2.41)
[24]	(65.6/74.1/87.3/101.8/111.9)	(18.98/24.58/29.47/31.22/41.99)	(0.80/1.543/1.69/ 1.81/1.90)
ours	(51.6/62.7/ 70.8/82.08/89.8)	(14.51/19.81/24.81/29.99/33.59)	(0.51/0.82/1.11/1.17/1.29)

The efficiency of our encryption and decryption operations is mainly due to the efficiency of our access structure, the choice of our trapdoor and the discrete Gaussian sampling approach. Our discrete sampling is based on the sample performance in $O(log^c n)$ times but not $\Omega(n^2 log^2 n)$ times which applied in most schemes. Also, the trapdoor algorithm used to generate the matrix $R \in Z^{m\times m}$ is efficient which directly improves the system execution time.

Table 2 compares the storage capacity, supported access structures and their operations. The above criteria were used to compare our scheme with three other related schemes in [28], [31] and [24]. Our storage capacity analysis was based on the size of the public parameters PP, secrete key size SK, and the expansion of the ciphertext.

Table 2. Relevant related schemes in terms of their access structures, operations and capacity analysis.

Scheme	Access Structures	Operation	PP size	MK Size	SK Size	Ciphertext Size
[28]	LSSS matrix	AND, OR, Threshold	$(snm + nm + n)\ log\ q$	$sm^2 logq$	$[(s + 1)m]^2$	$(s + 1)m\ logq$
[31]	Threshold gate	Threshold	$(2nm + n)$ log$q$	$2snm^2 \log q$	$m^2\ d^2\log\ q + mU$	$(dmA_s + 1) \log q$
[24]	Threshold gate	Threshold, AND	$3nm + n + sn) \log q$	$m^2 logq$	$2mU$	$(2mA_s + 1)logq$
ours	Reduce-OBDD	AND, OR,Threshold	$(smn + n) \log q$	$m^2 \log q$	mU	$(mA_s + 1)logq$

The following notations were used in this work: U is the initial or universe attributes, A_s is the number of attributes in the ciphertext, $n \times m$ matrix which relates to A_s, s secrete share for each A_s and d is the depth of the attributes. The public parameters PP of [24], [28] and [31] are very long as compared to ours of $(smn + n)\log q$. The public parameters of the other schemes are not linearly related to the system's number of attributes. However, they are related to the parameters of the lattice which results in the high storage size. The master key MK and the secrete key sizes of [28] and [31] are longer than the other schemes. The schemes in [28] and [31] are based on the sample left approach therefore, their secret keys are related to the number of users' attributes and the cascaded matrix column. In [31], the ciphertext and the key size relate to the number of users, matrix column, and the depth of the attribute hierarchy.

In terms of access structures and their operations, the policies of the schemes in [24] and [31] are not flexible and therefore do not support a flexible and fine-grain access policy. They are based on threshold gates. The scheme in [31] supports only threshold operation, [24] supports threshold and AND operations whilst the scheme in [28] supports AND, OR and threshold operation which a bit flexible in terms of an access policy expression. In addition to supporting AND, OR, and threshold operations, our scheme also supports negative and positive attributes making it more flexible as compared to the others. Whilst our scheme is based on a reduced ordered binary decision diagram access structure which gives an efficient access policy expression without redundancy, [28] is based on the LSSS matrix without a detailed explanation of how the expression of access policy was conducted.

Our scheme is practical with respect to storage capacity, execution time and is secured against quantum attacks due to the choice of an optimized access structure for our access policy expression, lower dimensional size of lattice, and efficient trapdoor approach used.

6. Integrating Lattice Based CP-ABE AC with CCN/NDN

This section entails details of the key exchange and the content sharing protocols. To ensure an efficient content sharing system, a hybrid technique is used. An asymmetric encryption scheme, known to be efficient is used to encrypt the content to be shared whiles the lattice CP-ABE AC scheme is used to encrypt the manifest or policy that contains the password or the key to decrypt the content.

6.1. System Model

The entities of our system and their description are introduced below:

Content Data Publisher (CDP): This can be the owner of the content or a trusted person on behalf of the data owner. He designs access policies, encrypts data and publishes them on the cloud in the ICN approach.

Content Centric Server (CCS): This is the cloud server responsible for content storage and user authentication. The content and the content policy are stored on the CCS in the CCN approach.

Content Data (CD): This is the private information encrypted by the owner and can only be accessed and used by legitimate users. This is stored in the CCN approach and can be accessed by legitimate users from any location

A trusted service provider (TSP): The service provider is a trusted authority responsible for key generation encryption and decryption keys for the publisher and the user. This authority runs two main algorithms:

(i) Asymmetric encryption algorithm, which is used for the encryption and the decryption of the content
(ii) Lattice CP-ABE AC algorithm, which is used to encrypt the content policy which contains the password used to decrypt the content data

Content users (CU): These are prospective authorized content users who can access content from anywhere.

Content Policy (CP): We describe the data manifest which stores the information about the content as content policy. This stores the decryption key of the content. It is encrypted with the key which is associated with the user's attribute. The user can obtain the decryption key if his attributes match with the policy enforced on the content.

6.2. Our Proposed Secured Information Sharing Scenario

Figure 4 demonstrates a secured information sharing system. In this system, communication is based on one to many information sharing; that is, a publisher and many content users of the same interest and subscription. The main aim of the system is to protect and enforce access control policy on sharing content in the CCN approach so that only users whose properties match with the policy can effectively access and use the content.

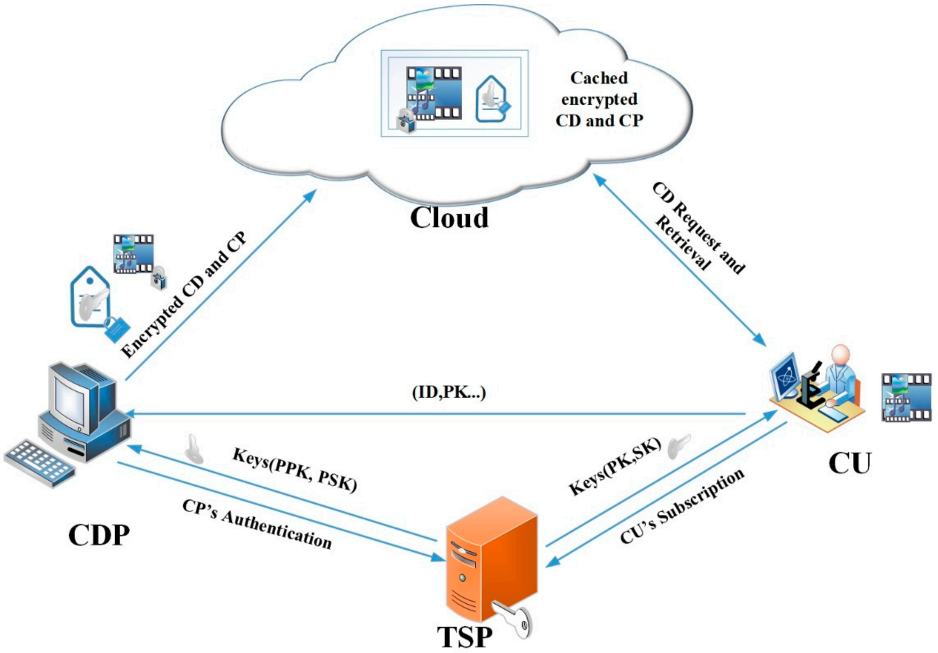

Figure 4. CCN/NDN content dissemination setup.

TSP generates two pairs of keys to the CU and CDP as follows:

(i) The TSP generates a pair of keys $\{PK, SK\}$ by running $KeyGen()$ in Section 4 to the user upon registration. The user installs the secrete key SK on his device and sends $\{PK, ID\}$ to the Publisher.

(ii) TSP runs $KeyGen(a)$ to generate a pair of keys $\{PPK, PSK\}$, and a hashed code of one of the users $ID = \{H(ID)\}$ to the CDP. Let $a \in R_q$ be a uniformly random value and $r_1, r_2 \in R_q$ be a sample from distribution $\mathcal{X}$. The TSP generates $p = r_1 - a.r_2 \in R_q$ and outputs the public key PPK and secret keys PSK as (a, p) and r_2 respectively.The keys generated to users have time validation and automatic key update property, so users will not receive any update once their keys expire or compromised. When the CDP recieves $\{PPK, PSK, H(ID)\}$ from the TSP and $\{PK, ID\}$ from the CU, he authentics the CU by running a hash function of the ID and compares it with the hash codes, $ID = \{H(ID)\}$ received from the TSP.

The CP then performs two main encryption processes.

(i) CDP selects key pairs, $\{PPK, PSK\}$ and parameters, $\theta_0, \theta_1, \theta_2 \in R_q$. He runs the encryption algorithm $Enc(PPK, E(CD))$, where $E(CD)$ is the encoded CD and set $C_{CD} = (C^1, C^2) = (a.\theta_0 + \theta_1, p\theta_1 + \theta_2 + E(CD))$.

(ii) The CDP runs the encryption algorithm $Encryption(PP, M = PSK, AS) \rightarrow (CT)$ in Section 4 and the broadcasts (C_{CD}) and CT to the cloud server. Note that (C_{CD}) is the encrypted content data CD which CUs are interested and CT is the encrypted content policy which contains some relevant information about the CD and secrete key to or password to decrypt (C_{CD}).

The CU on the other side conduct the following processes:

(i) The CU runs the decryption $(CT, PP, SK) \rightarrow (PSK)$ algorithm in Section 4 to obtain the secret key PSK. To obtain PSK, the user's attributes (SK) must satisfy (PP).

(ii) The CU runs $Dec(C_{CD}, PSK)$ to output $m' = C^1 \cdot r_1 + C^2 \in R_q$ to obtain m from m'.

6.3. Key Exchange Protocol, Encryption and Decryption Model

Figure 5 shows the key exchange process of our and Figure 6 represents content dissemination and retrieval process of our system. In Figure 5, the TSP generates (PSK, PPK) based on an asymmetric encryption scheme and sends it to the CDP through a secured key exchange protocol.

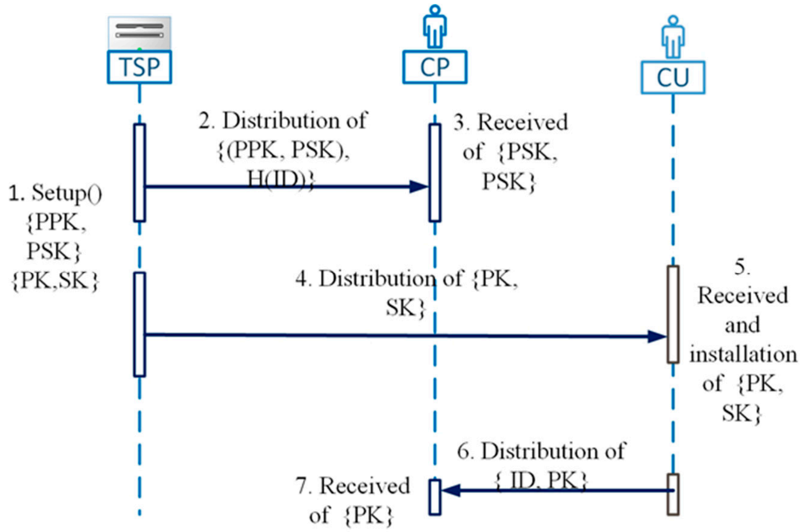
TSP
CP
CU
2. Distribution of {(PPK, PSK), H(ID)}
3. Received of {PSK, PSK}
1. Setup() {PPK, PSK} {PK,SK}
4. Distribution of {PK, SK}
5. Received and installation of {PK, SK}
6. Distribution of { ID, PK}
7. Received of {PK}

Figure 5. Represents the key exchange protocol.

To the CU, the TSP generates a pair of keys (PK, SK) based on CU's attributes. When CU receives (PK, SK), he installs SK on his device and sends PK to the content data publisher. At the end of the key exchange protocol, the user holds a pair of keys which reflects his attributes and the

CDP holds three keys which consist of the public key of users (PK) and a pair of asymmetric keys (PPK, PSK).

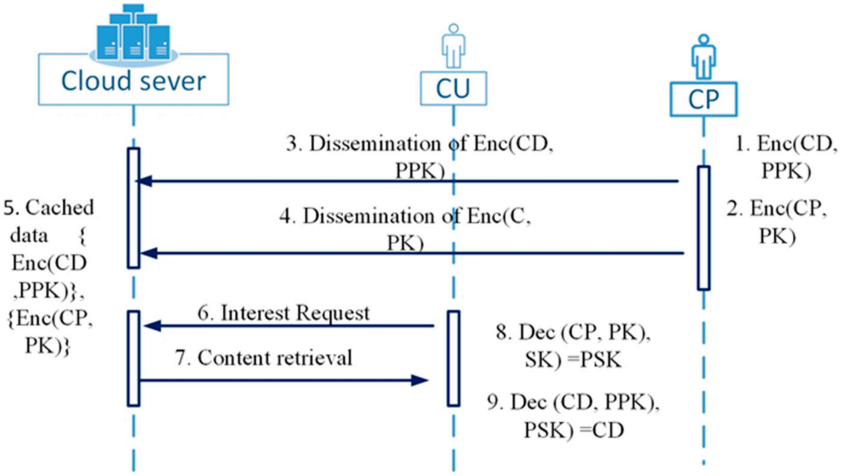
Cloud sever
CU
CP
1. Enc(CD, PPK)
2. Enc(CP, PK)
3. Dissemination of Enc(CD, PPK)
4. Dissemination of Enc(C, PK)
5. Cached data {Enc(CD ,PPK)}, {Enc(CP, PK)}
6. Interest Request
7. Content retrieval
8. Dec (CP, PK), SK) =PSK
9. Dec (CD, PPK), PSK) =CD

Figure 6. Represents content dissemination and retrieval.

The encryption and decryption process in Figure 6 consists of the following steps:

The content data publisher firstly selects (PPK, PSK) pair of keys and encrypt the content $Enc(CD, PPK)$

Secondly, the CDP encrypts the content policy $Enc(CP, PK)$ by taking into consideration the attribute set and the updated policy. The content policy contains the secrete key and some information about the content data, including the hash code of the content data. The CDP encrypts content data $Enc(CD)$ and content policy $Enc(CP)$ and disseminates them unto the cloud server

When the CU sends for request, the server verifies him and when there is a match between his subscription and the policy, the server replies with the content policy $Enc(CP)$ and the content data $C_{CD} = Enc(CD)$ sequentially. The CU runs two main decryption algorithm which consists of the following.

(i) Firstly, the user runs the decryption algorithm $Decrypt((CT = Enc(CP), SK)$ in Section 4 to extract the secrete kay PSK using the secret key SK associated with his attribute.

(ii) Finally, using PSK, the user extracts his interested content data CD by running the decryption $Dec((CD, PPK)PSK) \rightarrow CD$. The user can obtain and utilize the message if and only if his attributes match with the policy enforced on the content policy to obtain the secret key PSK for decryption of the Content data.

6.4. Security Analysis of our System

This section looks at the security analysis of our proposed system. This is based on the privacy of the content and users' authentication

6.4.1. Privacy

The proposed system consists of four actors, CU, CP, cloud sever and TSP. After the CU receives his pair of keys (PK, SK) from the TSP, he/she sends PK and one of his $IDs = H(ID)$, to the CP. The CP authenticates the CU and encrypts the content CD with the public key PPK and then lock up the secret key PSK with the public key PKreceived from the CU. The CP publishes the encrypted content and the encrypted secret key to the cloud server in a content centric approach without leaking any information about the CD and PSK. Here, the cloud server cannot learn anything about the CD and PSK except the encrypted content and the encrypted manifest which contains the key PSK. The CU also sends the public key to the CP without disclosing his private keys. So, if the server or any of the users are malicious, none of them can collude to decrypt the content policy to obtain PSK to decrypt the content. Moreover, an attacker cannot eavesdrop the $CU's$ credentials or pretends to be

CP due to the security primitives of the basic scheme described in section 4.4. However, *CP* conspiring with the *TSP* can obtain users' credentials.

6.4.2. Authentication

The content policy or manifest contains the hash code of the content. This enables the user to verify the authenticity of the message and the CP. Hence, the integrity of the content and the legitimacy of the content publisher is assured.

7. Conclusions

We constructed an efficient and secured latticed based reduced-OBDD CP-ABE access control scheme for content cached on CCN/NDN. Our scheme is based on the lattice and resistant to quantum attacks without exponential and pairing costs. An optimized access structure was employed to improve on the efficiency of the access control and can support Boolean operations such as AND, OR, NOT, and threshold gates. Our proposed scheme also used an optimized trapdoor and Gaussian sampling algorithm for the generation of matrices for public parameters. This resulted in a reduced key and ciphertext size, as well as a better execution time for key generation, encryption and decryption operations. Our implementation results show that our scheme is practical and more efficient than most of the existing CP-ABE AC schemes and also resistant to quantum attacks. This makes our scheme suitable for real-life, user-oriented CCN/NDN applications.

In the future, we will conduct further research on how to reduce key generation, run time, and user revocation.

Author Contributions: Conceptualization, E.A. and X.W.; Methodology, E.A. and J.B.A.; Project administration, X.Z.; Supervision, X.Z. and X.W.; Writing—original draft, E.A.; Writing—review & editing, X.W. and J.B.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China under Grant 61502086, the foundation from the State Key Laboratory of Integrated Services Networks, Xidian University (No. ISN18-09).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Anggorojati, B.; Mahalle, P.N.; Prasad, N.R.; Prasad, R. Capability-based access control delegation model on the federated IoT network. In Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, 15 July 2012.
2. Grusho, A. Five SDN-Oriented Directions in Information Security. In Proceedings of the 2014 International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC), Moscow, Russia, 28–29 October 2014; Volume 1, pp. 1–4.
3. Cao, Z. *New Directions of Modern Cryptography*; CRC Press Inc: Boca Raton, FL, USA, 2012; pp. 1–400.
4. Herranz, J.; Laguillaumie, F.; Ràfols, C. Constant size ciphertexts in threshold attribute-based encryption. In Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, 26–28 May 2010.
5. Chen, C. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. *Comput. Sci.* **2013**, *7779*, 50–67.
6. Hohenberger, S.; Waters, B. Online/offline attribute-based encryption. In *Public-Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 293–310.
7. Lai, J.; Deng, R.H.; Guan, C.; Weng, J. Attribute-based encryption with verifiable outsourced decryption. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1343–1354.
8. Zhou, Z.; Huang, D. On efficient ciphertext-policy attribute based encryption and broadcast encryption Extended abstract. *IEEE Trans. Comput.* **2010**, *395*, 753–755.
9. Song, Y.; Li, Z.; Li, Y.; Li, J. A new multi-use multi-secret sharing scheme based on the duals of minimal linear codes, Secure. *Commun. Netw.* **2015**, *8*, 202–211.
10. Wang, J.; Xiong, N.N.; Wang, J.; Yeh, W.C. A compact ciphertext-policy attribute-based encryption scheme for the information-centric Internet of Things. *IEEE Access* **2018**, *6*, 63513–63526.

11. Ajtai, M. Generating hard instances of lattice problems (extend abstract). In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, New York, NY, USA, 1 July 1996.
12. Zhu, W.; Yu, J.; Wang, T.; Xie, W. Efficient attribute-based encryption from R-LWE. *Chin. J. Electron.* **2014**, *23*, 778–782.
13. Tan, S.F.; Samsudin, A. Lattice ciphertext-policy attribute-based encryption from RingLWE. In Proceedings of the IEEE International Symposium on Technology Management and Emerging Technologies, Langkawi, Malaysia, 25 August 2015.
14. Yan, X.; Liu, Y.; Li, Z.; Huang, Q. A privacy-preserving multi-authority attribute-based encryption scheme on ideal lattices in the cloud environment. *Netinfo Secur.* **2017**, *8*, 19–25.
15. Wang, T.; Han, G.; Yu, J.; Zhang, P.; Sun, X. Efficient chosen-ciphertext secure encryption from R-LWE. *Wirel. Pers. Commun.* **2017**, *95*, 1–16.
16. Yu, J.; Yang, C.; Tang, Y.; Yan, X. Attribute-Based Encryption Scheme Supporting Tree-Access Structure on Ideal Lattices. In Proceedings of the International Conference on Cloud Computing and Security, Haikou, China, 8 June 2018.
17. Ostrovsky, R.; Sahai, A.; Waters, B. Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 8 May 2007.
18. Micciancio, D.; Peikert, C. Trapdoors for lattices: Simpler, tighter, faster, smaller, In *Advances in Cryptology—EUROCRYPt*; Springer: Berlin/Heidelberg, Germany, 2012.
19. Agrawal, S.; Boneh, D.; Boyen, X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In Proceedings of the Advances in Cryptology-CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2010.
20. Kirchner, P.; Fouque, P. An improved BKW algorithm for LWE with applications to cryptography and lattices. In Proceedings of the Advances in Cryptology-CRYPTO 2015-35th Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015.
21. Agrawal, S.; Boyen, X.; Vaikunthanathan, V.; Voulgaris, P.; Wee, H. Functional Encryption for Threshold Functions (or, Fuzzy IBE) from Lattices in Public Key Cryptography-PKC. Available online: https://www.iacr.org/cryptodb/data/paper.php?pubkey=24341 (accessed on 8 January 2020).
22. Zhang, J.; Zhang, Z.; Ge, A. Ciphertext policy attribute-based encryption from lattices. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2012.
23. Jian, Z.; Haiying, G. Attribute-Based Encryption for Restricted Circuits from Lattices. In Proceedings of the IEEE Tenth International Conference on Computational Intelligence and Security, Kunming, China, 15 November 2014.
24. Wang, Y.T. Lattice ciphertext policy attribute-based encryption in the standard model. *Int. J. Netw. Sec.* **2014**, *16*, 444–451.
25. Nguyen, K.; Wang, H.; Zhang, J. Server-aided revocable identity-based encryption from lattices. In Proceedings of the International Conference on Cryptology and Network Security, Milan, Italy, 14–16 November 2016.
26. Wang, S.; Zhang, X.; Zhang, Y. Efficient revocable and grantable attribute-based encryption from lattices with fine-grained access control. *IET Inf. Secur.* **2018**, *12*, 141–149.
27. Agrawal, S.; Boneh, D.; Boyen, X. Efficient lattice (H) IBE in the standard model. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 2010.
28. Boyen, X. Attribute-based functional encryption on lattices. In Proceedings of the Theory of Cryptography. 10th Theory of Cryptography Conference TCC, Tokyo, Japan, 3–6 March 2013.
29. Zhao, J.; Gao, H. LSSS Matrix-Based Attribute-Based Encryption on Lattices. In Proceedings of the 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, China, 15–18 December 2017.
30. Liu, Y.; Wang, L.; Li, L.; Yan, X. Secure and Efficient Multi-Authority Attribute-Based Encryption Scheme from Lattices. *IEEE Access* **2018**, *7*, 3665–3674.
31. Liu, X.; Ma, J.; Xiong, J.; Li, Q.; Zhang, T.; Zhu, H. Threshold attribute-based encryption with attribute hierarchy for lattices in the standard model. *IET Inf. Secur.* **2014**, *8*, 217–223.

32. Ion, M.; Zhang, J.; Schooler, E.M. Toward content-centric privacy in ICN: Attribute-based encryption and routing. In Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM, Hong Kong, China, 12 August 2013.
33. Jacobson, V.; Smetters, D.K.; Thornton, J.D.; Plass, M.F.; Briggs, N.H.; Braynard, R.L. Networking named content. *Commun. ACM* **2012**, *55*, 117–124.
34. Papanis, J.P.; Papapanagiotou, S.I.; Mousas, A.S.; Lioudakis, G.V.; Kaklamani, D.I.; Venieris, I.S. On the use of attribute-based encryption for multimedia content protection over information-centric networks. *Trans. Emerg. Telecommun. Technol.* **2014**, *25*, 422–435.
35. Li, B.; Huang, D.; Wang, Z.; Zhu, Y. Attribute-based access control for ICN naming scheme. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 194–206.
36. Mannes, E.; Maziero, C.; Lassance, L.; Borges, F. Optimized access control enforcement over encrypted content in information-centric networks. In Proceedings of the 20th IEEE Symposium on Computers and Communications-ISCC 2015, Larnaca, Cyprus, 6–9 July 2015.
37. Misra, S.; Tourani, R.; Majd, N.E. Secure content delivery in information-centric networks: Design, implementation, and analyses. In Proceedings of the 3rd ACM SIGCOMM Workshop on Information-Centric Networking, Hong Kong, China, 12 August 2013.
38. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October−3 November 2006.
39. Affum, E.; Zhang, X.; Wang, X.; Ansuura, J.B. Efficient CP-ABE Scheme for IoT CCN Based on ROBDD. In *Advances in Computer Communication and Computational Sciences*; Springer: Berlin/Heidelberg, Germany, 2019.
40. Zhao, X.; Li, H. Privacy preserving data-sharing scheme in content centric networks against collusion name guessing attacks. *IEEE Access* **2017**, *5*, 23182–23189.
41. Agrawal, S.; Dan, B.; Boyen, X. Lattice basis delegation in fixed dimension and short-ciphertext hierarchical IBE. In *Advances in Cryptology-CRYPTO*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 98–115.
42. The PALISADE. Lattice Cryptography Library. Available online: https://git.njit.edu/palisade/ PALISADE (accessed on 2 December 2019).