$\mathbf{mR_{LWE}}$-CP-ABE: A REVOCABLE CP-ABE FOR POST-QUANTUM CRYPTOGRAPHY

MARCO CIANFRIGLIA(1), ELIA ONOFRI(1),(2), AND MARCO PEDICINI(1)

Abstract. We address the problem of user fast revocation in the lattice based CP-ABE by extending the scheme originally introduced in [*A ciphertext policy attribute-based encryption scheme without pairings.* J. Zhang, Z. Zhang - ICISC 2011]. While a lot of work exists on the construction of revocable schemes for CP-ABE based on pairings, works based on lattices are not so common, and – to the best of our knowledge – we introduce the first server-aided revocation scheme in a lattice based CP-ABE scheme, hence providing post-quantum safety. In particular, we rely on semi-trusted "mediators" to provide a multi-step decryption capable of handling mediation without re-encryption.

We comment on the scheme and its application and we provide performance experiments on a prototype implementation in the ABE spin-off library of Palisade to evaluate the overhead compared with the original scheme.

1. Introduction

In this work we tackle the problem of designing a fast key-revoking system in a Ciphertext Policy Attribute-Based Encryption (CP-ABE) constructed on some presumed post-quantum resistant algebraic setting. The presented approach involves a Dual-Regev CP-ABE scheme, which combines the advantages of attribute-based encryption with the security properties of the Regev encryption scheme [21] and provides a flexible and secure mechanism for access control and data encryption.

The Regev encryption scheme is a lattice-based encryption scheme based on the hardness of the Learning with Errors (LWE) problem, which is considered to be resistant to quantum attacks by the worst case complexity of GapSVP and SIVP on lattices. It represents messages as vectors and encryption is achieved by adding noise to those vectors. Decryption, conversely, can only be efficiently done by the intended recipient who possesses a secret key.

In a Dual-Regev CP-ABE scheme, ciphertexts are associated with access policies represented as pattern strings, where symbols can be 0, 1, or *. Users possess secret keys corresponding to their attributes (represented as bit strings). Decryption

(1) Department of Mathematics and Physics, Roma Tre University, Italy, Rome, RM, 00146.

(2) Institute for Applied Mathematics, National Research Council (CNR–IAC), Italy, Rome, RM, 00185.

E-mail addresses: `marco.cianfriglia@uniroma3.it, elia.onofri@uniroma3.it, marco.pedicini@uniroma3.it`.

2020 *Mathematics Subject Classification.* Primary 94A60, Secondary 68P25 68Q25 81P68.

Key words and phrases. Mediated CP-ABE and Lattice-based cryptography and Learning with Errors and Post quantum cryptography and Cloud cryptography.

succeeds if the user's attribute matches the policy pattern specified in the ciphertext. This allows for fine-grained access control, where access to encrypted data is granted based on attribute matching. Conversely to most of the CP-ABE schemes that are based on bilinear maps, these schemes do not rely on pairings. The absence of pairings in such schemes offers advantages in terms of simplicity and efficiency.

To address the issue of user revocation, we propose $\mathrm{mR}_{\mathrm{LWE}}$-CP-ABE, a novel solution that builds upon the Dual Regev CP-ABE scheme introduced in [31] by enforcing a security mediated public key encryption. In particular, $\mathrm{mR}_{\mathrm{LWE}}$-CP-ABE shares similarities with the ideas introduced in USENIX 2001 Boneh et al.'s paper, [8].

The main idea presented in the paper is the use of a (semi)trusted third party, called the *security mediator*, to check the user whenever she wants to decrypt a ciphertext. The user requires assistance of the security mediator because the user secret key is separated into two (or more) portions during key generation, with one portion given to the user while the remaining parts are given to (possibly multiple) security mediators. The user requires the security mediator's help in order to enable full user secret key and decrypt or sign messages.

We implement the proposed scheme in Palisade, [17]. In particular, building such practical testings on the implementation of the Palisade ABE project spin-off, we implicitly show its effectiveness.

1.1. **Related Works.**

Attribute-Based Encryption (ABE), firstly proposed in [24], is asymmetric cryptographic primitive for one-to-many encryption that, as highlighted by high number of surveys in the last years on it [20, 3, 33, 16], attracted many interests along the years as provides fine grained access control over data. An ABE scheme allows a data owner to encrypt some data once and to share them with many along with a set of required attributes that define an access policy; the set of valid recipients is not required to be known in advance, all we need is that an authorised user must retain a set of valid attributes that satisfy the access policy. Each user is identified by the set of attributes his/her owns. Over the years, two variants of ABE has been proposed in the literature: the Ciphertext Policy Attribute-Based Encryption (CP-ABE) [6] and the Key Policy Attribute-Based Encryption (KP-ABE) [12]. In CP-ABE the access policy is applied to the ciphertext, conversely, in KP-ABE it is associated to the secret key, so usually CP-ABE is preferred as it is more flexible. Differently from classical public key schemes where a user who wants to share encrypted data with many others is required to perform many encryptions, one for each of valid recipient, in ABE schemes the encryption is done only once for many users, for this reason in cloud environments ABE schemes are a common choice. However, in this context, usually the set of users change frequently so the ability to revoke some users is a necessary requirement for any ABE scheme.

In the literature [28], the revocation mechanism was categorised in three classes: direct, indirect and server-aided.

The *direct revocation* follows the approach of conventional public key management systems (PKMS) where a certificate revocation list (CRL) is distributed. Once a user needs to be revoked, the key authority in the PKMS adds the user identifier to the CRL and share the updated list. Some example of ABE schemes that implements direct revocation are [19, 14]. The major drawback of direct revocation is, of course, related to the distribution of the updated CRL. Any data owner must update his/her CRL before encrypting new data to exclude revoked users. Furthermore, as the revoked user set grows, so does the size of the CRL. In [14] authors proposed a solution to overcome both issues by setting expiration dates on keys, by embedding the revocation list along with the ciphertext and by removing revoked keys from the list once expired; however, in such schemes, data owner still needs to update his/her CRL to be sure not to miss any recently revoked-user.

In *indirect revocation*, every time a user is revoked, the key authority generates new keys only for the remaining non-revoked users. The benefit of this approach are that the server only needs to work on the subset of still active users and does not need to periodically share the CRL. A few examples of CP-ABE indirect revocable schemes are [23, 30] and [27]. For instance both in [23] and [30], the authors proposed to update both the keys for still active users and the older ciphertexts, stored on the cloud, to not letting a revoked-user to decrypt them anymore. The approach proposed in [27] is little bit different, they update the keys but each user has two different keys, an individual and a group keys, both needed for the decryption.

Server-aided revocation solutions try to avoid the need for key update and the distribution of the CRL. They required, as the system we propose in this paper, to leverage third-party cooperation to decrypt. Here, following the approach firstly proposed in [8] and then applied also in [29] and [10], we rely on key-splitting feature for the revocation. Differently from the literature, to the best of our knowledge, mR$_{\text{LWE}}$-CP-ABE is the first application of such a revocation technique to a lattice-based ABE scheme; we believe this is an important step as our system, uniquely with respect to all the previous works, provide post-quantum safety.

1.2. **Contributions.** Here in the following we list the main contributions of the present work

- Inspired by [8], we propose mR$_{\text{LWE}}$-CP-ABE the first, to the best of our knowledge, CP-ABE revocation scheme based on lattice, a presumed post-quantum resistant algebraic setting. We start from the CP-ABE scheme presented in [31] and we extend and modify it to support key revocation. We rely on (semi)trusted third party, called the *security mediator*, to perform fast and efficient user key revocation.
- We provide a formal description of the proposed scheme along with the analysis of its parameter and its security proof.
- We implement mR$_{\text{LWE}}$-CP-ABE scheme on Palisade, a well known crypto library, and we experimentally evaluate the overhead introduced by the revocation mechanism in term of performance.
- We will release the implementation of our scheme to let the community independently test and evaluate it.

1.3. **Paper organisation.** The rest of the paper is organised as follows. Section 2 wraps up the notation and the mathematical basics used in what follows. Section 3 formally introduce the definition of CP-ABE and its security model, the system model of the mediated scheme and its threat model. Section 4 reviews the mathematical background used throughout the paper (a confident reader can safely skip this section). Section 5 analyse the scheme presented in [31] by reworking its definition, providing a few small changes in the notation to better prepare the ground for the mediated scheme. Section 6 holds the main contribute of the paper, introducing the mediated scheme (Section 6.1), the parameter analysis (Section 6.2) and the security proofs (Section 6.3). Section 7 introduces the multi-bit variation on the original and mediated scheme, following the build from [31]. Section 8 presents some benchmarks and results on the proposed scheme. Section 9 closes the paper resuming the paper and providing some hints on future works.

2. Notation

Numeric sets of positive integers, integers, and real numbers are denoted with blackboard bold letters $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ respectively. The quotient group modulo q, $q \in \mathbb{N}$, is denoted by $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z} = \{0, \dots, q-1\}$. Probability are defined by capital letter $\mathbb{P}[\cdot]$ and distributions are denoted usually with χ and we say that a is sampled from it by writing $a \leftarrow_{\$} \chi$. In particular, the uniform distribution over a set S is denoted by $U(S)$.

Matrices are usually denoted by upper-case letters $(\mathbf{A}, \mathbf{B}, \dots)$ while vectors are interpreted as single-column matrices and usually denoted by lower-case letters $(\mathbf{a}, \mathbf{b}, \dots)$. Matrices (and vectors) can be transposed $(\mathbf{A}^T)$, concatenated by columns $([\mathbf{A} \| \mathbf{B}])$, or concatenated by rows $(\mathbf{A}; \mathbf{B})$. The scalar product is denoted by $\langle \cdot, \cdot \rangle$ while the euclidean and the infinity norm of a vector are denoted by $\|\mathbf{a}\|$ and $\|\mathbf{a}\|_\infty$ respectively. By abuse of notation, we define the norm of a matrix as the infinity norm over the euclidean norm of its columns, *i.e.* if $\mathbf{A} = [\mathbf{a}_1 \| \dots \| \mathbf{a}_n]$ then $\|\mathbf{A}\| = \max_i \|\mathbf{a}_i\|$. Finally, if the columns of a matrix $\mathbf{A} = [\mathbf{a}_1 \| \dots \| \mathbf{a}_n]$ are linearly independent, we denote with $\tilde{\mathbf{A}} = [\tilde{\mathbf{a}}_1 \| \dots \| \tilde{\mathbf{a}}_n]$ the Gram-Schmidt orthogonalisation of vectors $a_1, \dots, a_n$ taken in that order.

We refer to attributes with calligraphic capital letters; in particular $\mathcal{R}$ denote the admissible attributes, $\mathcal{S}$ denote user attribute specifications, and $\mathcal{W}$ denote ciphertext access structures. If $\mathcal{S}$ is compatible with $\mathcal{W}$ we say that it satisfy the access structure and we write $\mathcal{S} \vdash \mathcal{W}$, otherwise we write $\mathcal{S} \nvdash \mathcal{W}$.

The security parameter throughout the paper is n, and all other quantities are implicitly functions it. We use standard notations big-$\mathcal{O}$ and small-ω to denote asymptotic class, we write $poly(n)$ to determine functions $f(n) = O(n^c)$ for some constant c, and we write $negl(n)$ to determine negligible functions $f(n)$, *i.e.* definitively upper bounded by $1/n^c$. Finally, we say a probability is overwhelming if it is $1 - negl(n)$.

3. Scheme, system and threat model

In the following we recall the formal definition of a CP-ABE scheme and of its security model. Then we describe the architecture of mR$_{\text{LWE}}$-CP-ABE, our new ABE encryption scheme, based on lattice, able to efficiently revoke a target user. Finally, we define the threat model and we discuss the security of our solution.

3.1. Ciphertext policy attribute-based encryption.

A ciphertext policy attribute-based encryption (CP-ABE) scheme is a framework to perform secure data sharing where recipients are not specific user – like in classic public key encryption (PKE) schemes – but rather users with specific attributes. A trusted central authority is needed for what concerns user key creation, however data encryption and decryption can be performed without its further collaboration; in particular, also data owners outside the accredited users can encrypt data.

More formally, a CP-ABE scheme consists of four algorithms, namely:

- $\texttt{Setup}(\sigma, \mathbb{R}) \to (\texttt{msk}, \texttt{pk})$ Is the initialisation algorithm executed by a central authority to setup a pair of public key ($\texttt{pk}$) and master secret key ($\texttt{msk}$) starting from a set of security parameters σ and a set of admissible attributes $\mathbb{R}$. $\texttt{msk}$ is used for the creation of users key while $\texttt{pk}$ is employed for message encryption.
- $\texttt{KGen}(\texttt{msk}, \mathcal{S}) \to \texttt{sk}$ Is the algorithm the authority runs to accredit a user with an attribute specification $\mathcal{S}$, hence building a private key $\texttt{sk}$ capable of decrypt ciphertexts only with access structure $\mathcal{W}$ such that $\mathcal{S} \vdash \mathcal{W}$.
- $\texttt{Enc}(\texttt{pk}, \mathcal{W}, M) \to C$ Is the encryption algorithm run by a data owner to encrypt the message M in a ciphertext C with access structure $\mathcal{W}$. Only the public key $\texttt{pk}$ is needed to perform this operation.
- $\texttt{Dec}(\texttt{sk}, C) \to M'$ or $\perp$ Is the decryption algorithm run by a user to retrieve the message M associated to the ciphertext C. The equality $M = M'$ is required with overwhelming probability if the attribute specification $\mathcal{S}$ of the private key $\texttt{pk}$ satisfies the access structure $\mathcal{W}$ of the ciphertext C (*i.e.* $\mathcal{S} \vdash \mathcal{W}$). On the contrary, if $\mathcal{S} \nvdash \mathcal{W}$, the output must be $\perp$.

Following the structure of the original paper [31], we prove the security of the CP-ABE scheme by adopting the selective security model with chosen plaintext (sCPA) where the challenge access structure $\mathcal{W}$ is initially specified by the attacker. In the game, the attacker submits two plaintexts, one of which is randomly chosen and encrypted by the challenger. The attacker is then required to determine which plaintext corresponds to the given ciphertext.

More formally, consider the following indistinguishability game (IND-sCPA) between a challenger $\mathcal{C}$ that acts as central authority and an adversary $\mathcal{A}$ that acts as an attacker:

Init. $\mathcal{A}$ chooses a challenge access structure $\mathcal{W}$ and prompts it to $\mathcal{C}$.

Setup. $\mathcal{C}$ performs all the setup tasks and eventually prompts the public key $\texttt{pk}$ to $\mathcal{A}$.

Key generation queries. $\mathcal{A}$ is allowed to make a polynomial number of adaptive key generation queries on any attribute specification $\mathcal{S}$ such that $\mathcal{S} \nvdash \mathcal{W}$.

Challenge. $\mathcal{A}$ submits two messages of equal length M_0, M_1 to $\mathcal{C}$, who randomly chooses $b \in \{0, 1\}$ and returns to $\mathcal{A}$ the ciphertext associated with M_b, *i.e.* returns $\texttt{Enc}(\texttt{pk}, \mathcal{W}, M_b)$.

Guess. $\mathcal{A}$ is allowed to perform one more round of Key generation queries and eventually outputs a bit b'.

The advantage of an adversary $\mathcal{A}$ *w.r.t.* the previous game is defined as

$$\texttt{Adv}_{\mathcal{A}}^{\text{IND-sCPA}}(\sigma) = |\mathbb{P}[b = b'] - {}^1\!/_2| \ .$$

We can further define a CP-ABE scheme to be secure against sCPA if, for any polynomial time adversary $\mathcal{A}$, the advantage $\texttt{Adv}_{\mathcal{A}}^{\text{IND-sCPA}}(\sigma)$ is a negligible function in the security parameters σ.

3.2. **System model of mR$_{\text{LWE}}$-CP-ABE.** We rely on new server-aided approach to provide fast and reliable solution in order to avoid some inefficiently intrinsically derived by direct and indirect revocation mechanisms. Our system is logically composed by four kinds of entities:

- the Key Generation Server (KGS): a trusted server that is able to generate a public key and, for each user, the corresponding secret keys.
- A set of k *security mediators* (SM): each SM is a semi-trusted entity that has access to the *mediator keys* of a (sub)set of users.
- The data owner: someone who wants to encrypt some data for a set of, possibly unknown, users.
- A set of users that belong to the system: each user has an attribute specification that specifies his/her access rights. The attributes are associated to the secret user key generated by the KGS.

We defined our scheme on top of the one introduced in [31]; namely, for each user the KGS generates a tuple of keys, $(\mathtt{sk}, \mathtt{mk}_1, \ldots, \mathtt{mk}_k)$; the $\mathtt{sk}$ is the user key and it is given to the user while the keys $\mathtt{mk}_j$, with $1 \leq j \leq k$, are the mediator keys which are distributed one for each SM involved. In order for a user to successfully decrypt a ciphertext two conditions are required: first, as usually in CP-ABE, the user must have an attribute specification $\mathcal{S}$ that satisfy the ciphertext policy; secondly, all the k SMs must contribute in the decryption.

More formally, our revocable CP-ABE scheme consists of 5 algorithms:

- $\mathtt{Setup}(\sigma, \mathbb{R}) \to (\mathtt{msk}, \mathtt{pk})$ Is the initialisation algorithm executed by the KGS. It behaves like in regular CP-ABE.
- $\mathtt{MKGen}(\mathtt{msk}, \mathcal{S}, k) \to (\mathtt{sk}, \{\mathtt{mk}_j\}_{j=1}^{k})$ Is the algorithm the KGS runs to accredit a user with an attribute specification $\mathcal{S}$. Conversely to regular CP-ABE, the key is segmented in $k+1$ parts, k of which are provided to k SMs. The specified access structure $\mathcal{W}$ is stored with the user private key $\mathtt{sk}$ only, making mediators unaware of users capabilities.
- $\mathtt{Enc}(\mathtt{pk}, \mathcal{W}, M) \to C$ Is the encryption algorithm the data owner runs to encrypt the message M. It behaves like in regular CP-ABE schemes.
- $\mathtt{MDec}(C, \mathtt{sk}) \to M$ or $\perp$ Is the decryption algorithm a user runs to retrieve the message M associated to the ciphertext C. It requires the cooperation of all the k SMs which should return the result of $\mathtt{PDec}$ (see below) in order to make the user able to evaluate $M' = M$ with overwhelming probability (if $\mathcal{S} \vdash \mathcal{W}$). Like in regular CP-ABE schemes, if $\mathcal{S} \nvdash \mathcal{W}$, the output must be $\perp$ (regardless the possible collusion with SMs).
- $\mathtt{PDec}(\mathbf{y}, \mathtt{mk}) \to a$ Is the algorithm run by SMs that allows them to produce a partial decryption information a from $\mathbf{y}$ and the mediator key $\mathtt{mk}$. Here, $\mathbf{y}$ is derived from the ciphertext C by the user requiring the partial decryption within $\mathtt{MDec}$ function.

If a user is revoked, the KGS only needs to send this information to the SMs that have a mediator key for that user and they will stop to collaborate in the decryption process. In particular, it is sufficient that just one SM refuses to cooperate to defeat the decryption process. This guarantees that if at least one SM follows the protocol, a revoked user cannot decrypt anymore.

Please notice that, differently from previous schemes in the literature, we do not require to update keys or re-encrypt ciphertexts in order to revoke a user, we just need to notify the SMs. Furthermore, already encrypted ciphertexts that have not been decrypt before revoke occurs, are evenly secure against the revoked user. This is also different from direct revocation where the CRL, as this revocation process does, does not involve the encryption process. In order to support fast and secure revocation, our system incurs of course in some overhead compared to [31]. For instance,

- the KGS has to generate $k+1$ keys for each user;
- the decryption process of a ciphertext C requires $k+1$ partial decryption plus k error generation that is added by each SM to protect their mediator keys.

To experimentally evaluate the impact of revocation we report some experiments in Section 8.

It is important to highlight that, despite SM need to be reachable at decryption time, hence making the protocol interactive, the approach preserves the advantages of CP-ABE over classical PKE schemes. In fact, data owners still produce encrypted data off-line and without suffering any overhead w.r.t. non-mediated CP-ABE schemes. Furthermore, access to data is still preserved to data owners and final users only, since SMs have blind-access to data.

3.3. **Threat model to mR$_{\mathbf{LWE}}$-CP-ABE.** We now describe the threat model of our system; the security and correctness proofs are reported in Section 6. In the threat model we define five entities: the KGS, the set of SMs, the data owner, the set of users, and an external attacker. We remember that the KGS is a trusted entity whereas the SMs are semi-trusted. The data owner is also trusted whereas the users and, of course, the external attacker are untrusted. We identify the following possible threats that may affect our system:

- SMs collusion: multiple SMs involved in the decryption of the same ciphertext may collude together to decrypt without the user aid;
- Users collusion: multiple users may collude to decrypt a ciphertext they are not authorised to;
- Ineffective revocation: a revoked-user is still able to decrypt.
- DOS-decryption: an attacker who compromise at least on SM can prevent legitimate users to decrypt

We formally analyse the security of SMs and users collusion and the ineffective revocation in Theorem 1.

The DOS-decryption attack indeed can be mitigated by providing redundant mediated keys to SM.

4. Prerequisites on lattices

A n-dimensional lattice of rank $m \leq n$ is a subset of $\mathbb{R}^n$ given by the span of m linear independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{R}^n$. In formulas, we have

$$\mathbf{\Lambda} = \mathcal{L}(\mathbf{B}) = \left\{ \langle \mathbf{B}, \mathbf{c} \rangle \;\middle|\; \mathbf{c} \in \mathbb{Z}^m \right\} ,$$

where $\mathbf{B} \in \mathbb{R}^{n \times m} = [\mathbf{b}_1 \| \ldots \| \mathbf{b}_m]$ is called *basis* of the lattice.

The set of linear functionals that take integer values on each point of $\mathbf{\Lambda}$ is called *dual lattice* and it is denoted by

$$\mathbf{\Lambda}^* = \left\{ x \in \mathbb{R}^n \;\middle|\; \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}, \text{for all } v \in \mathbf{\Lambda} \right\} .$$

Given a matrix $\mathbf{A} \in \mathbb{Z}^{n\times m}$, the set of vectors that nullifies $\mathbf{A}$ is a m-dimensional lattice called *orthogonal lattice of* $\mathbf{A}$ and it is denoted by

$$\mathbf{\Lambda}^{\perp}(A) = \left\{ \mathbf{e} \in \mathbb{Z}^m \;\middle|\; \langle \mathbf{A}, \mathbf{e} \rangle = \mathbf{0} \right\} .$$

Orthogonal lattices are particularly useful when working in modular arithmetic; given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, we analogously define

$$\mathbf{\Lambda}_q^{\perp}(\mathbf{A}) = \left\{ \mathbf{e} \in \mathbb{Z}^m \;\middle|\; \langle \mathbf{A}, \mathbf{e} \rangle \equiv_q \mathbf{0} \right\} .$$

We further observe that, for any square matrix $\mathbf{B} \in \mathbb{Z}_q^{n\times n}$ we have $\langle \mathbf{A}, \mathbf{x} \rangle = 0 \iff \langle \mathbf{B}, \langle \mathbf{A}, \mathbf{x} \rangle \rangle = 0$, hence $\mathbf{\Lambda}_q^{\perp}(\mathbf{A}) = \mathbf{\Lambda}_q^{\perp}(\langle \mathbf{B}, \mathbf{A} \rangle)$.

4.1. **Hard problems.** Many cryptographic primitives have been constructed whose security is based on the (worst-case) hardness of SIVP or closely related lattice problems. In particular, the (worst-case) hardness of Shortest Independent Vectors Problem (SIVP) for *poly*(n) approximation factors implies the existence of several fundamental cryptographic primitives. Blömer and Seifert [7] showed that the Shortest Independent Vectors Problem (SIVP) is NP-hard to approximate for any constant approximation factor γ. Their result is shown only for the Euclidean norm, and their proofs were extended to arbitrary norms by [1].

The length of vector $\mathbf{x}$, denoted by $\|\mathbf{x}\|$, is defined with respect to integer p:

$$\|\mathbf{x}\|_p := \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p} .$$

We write SIVP$_p$ as a notation respective of p. Hence, SIVP$_2$ is the case considered in [7].

Hereinafter we suppose fixed $p = 2$ and we omit from explicitly mentioning it in the norm.

A basic parameter of the lattice $\mathbf{\Lambda}$ is the length of the shortest non-zero vector in the lattice. The parameter λ_1 is also indicated as the *first successive* of $\mathbf{\Lambda}$ and denoted by λ_1. It is important to know lower and upper bounds for λ_1, which of course depends on p: a lower bound is given by the length of the shortest vector in the Gram-Schmidt reduced form of the basis: $\lambda_1 \leq \min_i \|\tilde{\mathbf{b}}_i\|$. Similarly, for $i = 1, \ldots, n$, the i-th successive minimum, denoted by $\lambda_i(\mathbf{\Lambda})$, is the smallest l such that there are i non-zero linearly independent lattice vectors that have length at most l.

The (SIVP) consists in finding n independent and "short" vectors: given a basis $\mathbf{B} \in \mathbb{Z}^{n\times n}$ find independent vectors $\mathbf{u}_1, \ldots, \mathbf{u}_n$ such that $||\mathbf{u}_i|| \leq \lambda_n$ for $i = 1, \ldots, n$. [5]

Proposition 1 (Theorem 2 from [1])**.** *Under the (randomised) Gap Exponential Time Hypothesis, for any $p \geq 1$, there exists $\gamma > 1$, $\epsilon > 0$ such that γ-SIVP$_p$ with rank n is not solvable in $2^{\epsilon n}$ time.*

The Gap-Exponential Time Hypothesis (Gap-ETH) is a fine-grained complexity-theoretic hypothesis introduced in [13] and it is required to exclude sub-exponential algorithms.

4.2. **Discrete Gaussians.** We recall the definition of Gaussian function centred in $\mathbf{c}$ and scaled by a factor of s to be

$$\rho_{s,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi\frac{\|\mathbf{x}-\mathbf{c}\|^2}{s^2}\right) \ , \qquad \mathbf{x} \in \mathbb{R}^n .$$

A Gaussian function is typically used to build (continuous) probability distributions as

$$D_{s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{s^N} \ , \qquad \mathbf{x} \in \mathbb{R}^n \ ,$$

being $s^N = \displaystyle\int_{\mathbf{x}\in\mathbb{R}^n} \rho_{s,\mathbf{c}}(\mathbf{x})\, d\mathbf{x}$ the total measure associated to $\rho_{s,\mathbf{c}}$.

Given a lattice $\mathbf{\Lambda} \subset \mathbb{Z}^n$, we can discretise the distributions $D_{s,\mathbf{c}}$ on it by distributing $\mathbf{x} \in \mathbb{R}^n$ according to $D_{s,\mathbf{c}}$ and conditioning $\mathbf{x} \in \mathbf{\Lambda}$, hence obtaining

$$D_{\mathbf{\Lambda},s,\mathbf{c}}(\mathbf{x}) = \frac{D_{s,\mathbf{c}}(\mathbf{x})}{D_{s,\mathbf{c}}(\mathbf{\Lambda})} = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\mathbf{\Lambda})} \ ,$$

where $\rho_{s,\mathbf{c}}(\mathbf{\Lambda})$ is the proper normalisation constant given by $\rho_{s,\mathbf{c}}(\mathbf{\Lambda}) = \sum_{\mathbf{y}\in\mathbf{\Lambda}} \rho_{s,\mathbf{c}}(\mathbf{y})$. We call such distribution a *Discrete Gaussian function* with centre $\mathbf{c}$ and parameter s and we omit the subscripts s and $\mathbf{c}$ if equal respectively to 1 and to the origin $\mathbf{0}$.

Given a parameter $\epsilon \in \mathbb{R}^+$, we further recall from [15] the definition of *smoothing parameter* η_ϵ as

$$\eta_\epsilon = \min\left\{ s \in \mathbb{R}^+ \ \middle|\ \rho_{1/s}(\mathbf{\Lambda}^* \backslash \{\mathbf{0}\}) \leq \epsilon \right\} .$$

In particular, if $s \geq \eta_\epsilon$, we can bound the dispersion of the gaussian as per the following

Lemma 1 (Lemma 4.4 from [15])**.** *For any n-dimensional lattice $\mathbf{\Lambda}$, for any centre $\mathbf{c} \in \mathbb{R}^n$, and for any $\epsilon \in (0,1)$ we have that if $s \geq \eta_\epsilon(\mathbf{\Lambda})$ then*

$$\mathbb{P}_{\mathbf{x}\leftarrow_\$ D_{\mathbf{\Lambda},s,\mathbf{c}}}\left[\|\mathbf{x}-\mathbf{c}\| > s\sqrt{n}\right] \leq \frac{1-\epsilon}{1+\epsilon}\cdot 2^{-n} \ .$$

4.3. **Learning with errors.** Originally presented in [21] and later extended in [22], Learning with Errors (LWE) is a hard lattice problem founding in Fully Homomorphic Encryption. Its hardness has been proven in [21] via a quantum reduction to SIVP and GapSVP and in [18] via a classical reduction to a variation of GapSVP.

Let $q \in \mathbb{N}$ and let χ be a probability distribution on $\mathbb{Z}_q$. For any $\mathbf{s} \in \mathbb{Z}_q^n$, LWE instances with secret $\mathbf{s}$ are defined as samples from

$$A_{\mathbf{s},\chi} = \left\{ (\mathbf{a},\mathbf{y}) \in \mathbb{Z}_q^n \times \mathbb{Z}_q \ \middle|\ \mathbf{y} = \mathbf{a}^T\mathbf{s} + x, \text{ with } \mathbf{a} \leftarrow_\$ U(\mathbb{Z}_q)^n, x \leftarrow_\$ \chi \right\} .$$

LWE can be either formulated as search or decision problem, being the first to recover $\mathbf{s}$ given multiple samples of $A_{\mathbf{s},\chi}$ and the second to distinguish between $A_{\mathbf{s},\chi}$ and $U(\mathbb{Z}_q)^n \times U(\mathbb{Z}_q)$. In particular, if $q = \mathrm{poly}(n)$ the two problems are polynomially equivalent (see [22]).

Let us denote by Ψ_α, a periodisation of the normal distribution with mean 0 and variance $\frac{\beta^2}{2\pi}$ and by $\bar{\Psi}_\alpha$ its discretisation, then we have:

Proposition 2 (Theorem 1.1 from [22])**.** *Let $\alpha = \alpha(n) \in (0,1)$ and let $q \in \mathbb{N}$ be such that $\alpha q > 2\sqrt{n}$ holds. Assuming we have access to an oracle that solves*

LWE$_{q,\bar{\Psi}_\alpha}$ *given a polynomial number of samples, then there exists an efficient quantum algorithm for solving SIVP and GapSVP. The decision version of GapSVP and SIVP to within* $\tilde{\mathcal{O}}({}^{n}\!/\!{}_{\alpha})$ *in the worst case.*

More formally, for $r \in [0, 1)$ we have

$$\Psi_\alpha(r) = \sum_{k=-\infty}^{\infty} \frac{1}{\alpha} \cdot \exp\left(-\pi\left(\frac{r-k}{\alpha}\right)^2\right) \mod 1$$

and

$$\bar{\Psi}_\alpha(r) = \lfloor q \cdot \Psi_\alpha(r) \rceil \mod q \ .$$

In particular, we can characterise the distribution $\bar{\Psi}^m_\alpha$ as follows:

Lemma 2 (Lemma 12 from [2])**.** *Let* $\mathbf{e} \in \mathbb{Z}^m$ *and* $\mathbf{y} \leftarrow_\$ \bar{\Psi}^m_\alpha$*. Then the following relation in* $\mathbb{Z}_q$ *holds (but for negligible probability in* m*)*

$$|\mathbf{e}^T\mathbf{y}| \le \|\mathbf{e}\| \cdot q\alpha \cdot \omega(\sqrt{\log m}) + \|\mathbf{e}\|{}^{\sqrt{m}}\!/\!{}_{2} \ .$$

In particular, for $x \leftarrow_\$ \bar{\Psi}_\alpha$*, it holds in* $\mathbb{Z}_q$ *(but for negligible probability in* m*)*

$$|x| \le q\alpha \cdot \omega(\sqrt{\log m}) + {}^{1}\!/\!{}_{2} \ .$$

4.4. **Literature algorithms on lattices.** In the following we recall four algorithms from literature that are later used both in the original CP-ABE scheme and in mR$_{\text{LWE}}$-CP-ABE.

Function 1 (`SampleGaussian`, Theorem 4.1 from [11])**.** *Let* $\mathbf{\Lambda} = \mathcal{L}(\mathbf{B}) \subset \mathbb{R}^m$ *be a* m*-dimensional lattice with basis* $\mathbf{B}$*. Given a gaussian parameter* $s \in \mathbb{R}^+$ *such that* $s \ge \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log m})$ *and for any centre* $\mathbf{c} \in \mathbb{R}^m$*, there exists a probabilistic polynomial-time algorithm* `SampleGaussian` *(*$\mathbf{B}, s, \mathbf{c}$*) that samples a vector* $\mathbf{x} \in \mathbf{\Lambda}$ *with a distribution statistically close to the discrete gaussian* $D_{\mathbf{\Lambda},s,\mathbf{c}}$*.*

Function 2 (`TrapGen`, Algorithm 1 from [4])**.** *Let* $q \in \mathbb{N}$ *be an odd prime associated with a security parameter* n *and let* $m \in \mathbb{N}$ *be a dimension such that* $m \ge (5 + 3\delta_0)n \log q$*, for any* $\delta_0 \in \mathbb{R}^+$*. There exists a probabilistic polynomial-time algorithm* `TrapGen` *(*n, m, q*) that generates a statistically* $(mq^{-\delta_0 n/2})$*-close to uniform matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *and a with-overwhelming-probability-short basis* $\mathbf{T_A}$ *of the orthogonal lattice* $\mathbf{\Lambda}_q^\perp(\mathbf{A})$*, i.e. such that* $\|\mathbf{T_A}\| \le \mathcal{O}(n \log q)$ *and* $\|\tilde{\mathbf{T}}_\mathbf{A}\| \le \mathcal{O}(\sqrt{n \log q})$*.*

In the following we choose $\delta_0 = {}^{1}\!/\!{}_{3}$ *so that we obtain* $m \ge \lceil 6n \log q\rceil$*.*

Function 3 (`SamplePre`, Section 5.2 from [11])**.** *Let* $q \in \mathbb{N}$ *be an odd prime associated with a security parameter* n*, let* $m \in \mathbb{N}$ *be a dimension such that* $m \ge 2n \log q$*, and let* $s \in \mathbb{R}$ *be a gaussian parameter such that* $s \ge \omega(\sqrt{\log m})$*. In general, for all (but a* $2q^{-n}$ *fraction of)* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$*, the distribution of the syndrome* $\mathbf{u} = \mathbf{A}\mathbf{e} \mod q$ *yielded by* $\mathbf{e} \leftarrow_\$ D_{\mathbb{Z}^m,s}$ *is statistically close to* $U(\mathbb{Z}_q^n)$*. In particular, for such values, there exists a probabilistic polynomial time algorithm* `SamplePre` *(*$\mathbf{A}, \mathbf{T_A}, s, \mathbf{u}$*) that samples* $\mathbf{e}$ *given a short basis* $\mathbf{T_A}$ *of the orthogonal lattice* $\mathbf{\Lambda}_q^\perp(\mathbf{A})$*, conditioned on* s *being such that* $s \ge \|\tilde{\mathbf{T}}_\mathbf{A}\| \cdot \omega(\sqrt{\log m})$*.*

Function 4 (`GenSamplePre`, Theorem 3.4 from [9])**.** *Let* $q \in \mathbb{N}$ *be an odd prime associated with a security parameter* n *and let* $m \in \mathbb{N}$ *be a dimension such that* $m \ge 2n \log q$*. Assume* $\mathbf{A} = [\mathbf{A}_1\| \dots \|\mathbf{A}_k] \in \mathbb{Z}_q^{n\times mk}$ *and consider* $J = \{j_1, \dots j_{|J|}\} \subset \{1, \dots, k\}$ *be a set of indices of the* $\mathbf{A}_i$ *matrices*[1]*. Let* $\mathbf{A}_J = [\mathbf{A}_{j_1}\| \dots \|\mathbf{A}_{j_{|J|}}]$ *and let*

[1] More in general, at least n columns of the matrix $\mathbf{A}$ are required, however, for the sake of simplicity, we consider only blocks $\mathbf{A}_i$

$\mathbf{T}_{\mathbf{A}_J}$ *be a basis of the orthogonal lattice* $\mathbf{\Lambda}_q^{\perp}(\mathbf{A}_J)$*. There exists a probabilistic polynomial time algorithm* `GenSamplePre` $(\mathbf{A}, \mathbf{T}_{\mathbf{A}_J}, J, s, \mathbf{u})$ *that samples* $\mathbf{e} \leftarrow_{\$} D_{\mathbb{Z}^{mk},s}$ *condition on* $\langle \mathbf{A}, \mathbf{e} \rangle = \mathbf{u}$*, with* $s \geq \|\tilde{\mathbf{T}}_{\mathbf{A}_J}\| \cdot \omega(\sqrt{\log km})$ *(hence independent on the choice and size of* J*).*

In particular, to build such an algorithm, consider $\bar{J} = \{1, \ldots, k\} \backslash J$*. We can retrieve* $\mathbf{e}_i$ *for* $i \in \bar{J}$ *directly from* $\mathbf{e}_{\bar{J}} \leftarrow_{\$} D_{\mathbb{Z}^{m \cdot (k - \|J\|)},s}$ *while* $\mathbf{e}_j$ *for* $j \in J$ *can be retrieved from* $\mathbf{e}_J = \texttt{SamplePre}(\mathbf{B}, \mathbf{T}_{\mathbf{B}}, s, \mathbf{u} - \langle \mathbf{A}, \mathbf{e}_{\bar{J}} \rangle)$*, so building* $\mathbf{e}$ *such that* $\langle \mathbf{A}, \mathbf{e} \rangle = \mathbf{u}$*.*

5. CP-ABE scheme on lattices

In this section we review the CP-ABE scheme presented in [31] we extend later in Section 6. The scheme is somehow inspired by Shamir Secret Sharing [26] technique, where a randomly chosen shared secret $\mathbf{s} \leftarrow_{\$} \mathbb{Z}_q^n$ is hidden trough multiple LWE samples and it is used in a LWE-PKE [11] fashion to build a ciphertext.

The main idea is to provide a given user with a fixed attribute (say 0) and a set of variable attributes $\mathcal{R} = \{1, \ldots, |\mathcal{R}|\}$ that can either be assigned (say i^+) or not (say i^-) for a total of $r = |\mathcal{R}| + 1$ attributes. Then, access structures W can either specify a given attribute (both in a positive or a negative way) or not (actually providing them both).

More formally, a user attribute specification is a 2-partition $\mathcal{S} = (S^+, S^-)$ of $\mathcal{R}$ (*i.e.*, $S^+ \cup S^- = \mathcal{R}$ and $S^+ \cap S^- = \emptyset$) while an access structure is a 2-covering $\mathcal{W} = (W^+, W^-)$ of $\mathcal{R}$ (*i.e.* $W^+ \cup W^- = \mathcal{R}$, but $W^+ \cap W^- = \emptyset$ is not required) where S^+ and W^+ represent sets of positive attributes, moreover, S^- and W^- are sets of negative attributes. In particular, we say that user attributes $\mathcal{S}$ *satisfies* the access structure $\mathcal{W}$ if $S^+ \subseteq W^+$ and $S^- \subseteq W^-$: in such case we write $\mathcal{S} \vdash \mathcal{W}$, otherwise we write $\mathcal{S} \nvdash \mathcal{W}$.

The advantage of providing user-attribute specifications as 2-partition consists in always having the same number of attributes, hence being able to build a matrix $\mathbf{D} \in \mathbb{Z}_q^{n \times mr}$ to be used in `GenSamplePre`. At the same time, the fixed attribute 0, provides an excellent point to evaluate the short basis needed by `GenSamplePre` (hence assuming $J = \{0\}$): in fact, it is fixed amongst all the possible user attribute specifications and it can be pre-evaluated efficiently via `TrapGen` algorithm.

5.1. The scheme.

The scheme is parametrised on the modulus q, the dimension m, the security parameter n, the gaussian parameter s and the error distribution χ with parameter α. Requirements on these parameters are analysed later in the next section.

The definition of the four functions defining the CP-ABE scheme followsin Algorithms 1–4.

5.2. Parameters requirements and security.

We can analyse the scheme parameters considering the requirement for a correct decryption (Algorithm 4) to the condition required by Proposition 2 and from Functions 1–4; we obtain:

(*i*) $m \geq \lceil 6n \log q \rceil$ as required by `TrapGen` (see Function 2);
(*ii*) $s \geq \|\tilde{\mathbf{T}}_{\mathbf{B}_0}\| \cdot \omega(\sqrt{\log(mr)})$ as required by `GenSamplePre` (see Function 4) and by the security proof;
(*iii*) $|x_z - x'| \leq q/\ell$, with $\ell > 4$, for correct decryption (see Algorithm 4).
(*iv*) $\alpha q \geq 2\sqrt{n}$ for LWE hardness (see Proposition 2);

Algorithm 1: $\texttt{Setup}(n, m, q, \mathcal{R}) \to (\texttt{pk}, \texttt{msk})$

```
Input: the parameters $n, m, q \in \mathbb{N}$ and the set of attributes
       $\mathcal{R} = \{1, \dots, r-1\}$
Output: the public key pk and the master secret key msk
$(\mathbf{B}_0, \mathbf{T}_{\mathbf{B}_0}) \leftarrow \texttt{TrapGen}(n, m, q)$;
for each $i \in \mathcal{R}$ do
    $\mathbf{B}_i^+, \mathbf{B}_i^- \leftarrow_\$ U(\mathbb{Z}_q^{n \times m})$;
$\mathbf{u} \leftarrow_\$ U(\mathbb{Z}_q^n)$;
$\texttt{pk} \leftarrow (\mathbf{B}_0, \{\mathbf{B}_i^+, \mathbf{B}_i^-\}_{i \in \mathcal{R}}, \mathbf{u})$;
$\texttt{msk} \leftarrow (\texttt{pk}, \mathbf{T}_{\mathbf{B}_0})$
```

Algorithm 2: $\texttt{KGen}(\texttt{msk}, \mathcal{S}) \to \texttt{sk}$

```
Input: the master secret key msk and a user attribute spec. $\mathcal{S} = (S^+, S^-)$
Output: the user secret key sk holding the attribute specification $\mathcal{S}$ and
        the private secret $\mathbf{e} \leftarrow_\$ D_{\mathbb{Z}^{mr}, s}$
for each $i \in \mathcal{R}$ do
    $\mathbf{A}_i \leftarrow \begin{cases} \mathbf{B}_i^+ & \text{if } i \in S^+ \\ \mathbf{B}_i^- & \text{if } i \in S^- \end{cases}$;
$\mathbf{A} \leftarrow [\mathbf{B}_0 \| \mathbf{A}_1 \| \dots \| \mathbf{A}_{|\mathcal{R}|}]$;
$\mathbf{e} \leftarrow \texttt{GenSamplePre}(\mathbf{A}, \mathbf{T}_{\mathbf{B}_0}, \{0\}, s, \mathbf{u})$;
$\texttt{sk} \leftarrow (\mathcal{S}, \mathbf{e})$;
```

Algorithm 3: $\texttt{Enc}(\texttt{pk}, W, M) \to C$

```
Input: the public key pk, an access structure $\mathcal{W} = (W^+, W^-)$ and a
       message $M \in \{0, 1\}$
Output: the ciphertext structure $C$ holding the LWE-PKE encrypted
        message $z \in \mathbb{Z}_q$ and the coefficients $\mathbf{c}_i^\pm$ to allow the random secret
        retrieval (if the access structure is satisfied)
$\mathbf{s} \leftarrow_\$ U(\mathbb{Z}_q^n)$;
$x_z \leftarrow_\$ \chi$;
$z \leftarrow \langle \mathbf{u}^T, \mathbf{s} \rangle + x_z + M \lfloor q/2 \rfloor$;
$\mathbf{x} \leftarrow_\$ \chi^m$;
$\mathbf{c}_0 \leftarrow \langle \mathbf{B}_0^T, \mathbf{s} \rangle + \mathbf{x}$;
for each $i \in W^+$ do
    $\mathbf{x} \leftarrow_\$ \chi^m$;
    $\mathbf{c}_i^+ \leftarrow \langle {\mathbf{B}_i^+}^T, \mathbf{s} \rangle + \mathbf{x}$;
for each $i \in W^-$ do
    $\mathbf{x} \leftarrow_\$ \chi^m$;
    $\mathbf{c}_i^- \leftarrow \langle {\mathbf{B}_i^-}^T, \mathbf{s} \rangle + \mathbf{x}$;
$C \leftarrow (W, z, \mathbf{c_0}, \{\mathbf{c}_i^+\}_{i \in W^+}, \{\mathbf{c}_i^-\}_{i \in W^-})$;
```

```
Algorithm 4: $\mathtt{Dec}(C, \mathtt{sk}) \to M$ or $\perp$
  Input: a ciphertext structure $C$ and a secret key $\mathtt{sk}$
  Output: the message $M' \in \{0,1\}$ which corresponds to the original
          message $M$ if $|x_z - x'| < q/4$ (say $\leq q/\ell$ for each $\ell > 4$)
  if $\mathcal{S} \nvdash \mathcal{W}$
      return $\perp$;
  for each $i \in \mathcal{R}$ do
      $\mathbf{y}_i \leftarrow \begin{cases} \mathbf{c}_i^+ & \text{if } i \in S^+ \\ \mathbf{c}_i^- & \text{if } i \in S^- \end{cases}$;
  $\mathbf{y} \leftarrow [\mathbf{c}_0; \mathbf{y}_1; \ldots; \mathbf{y}_{|\mathcal{R}|}]$;
  $a \leftarrow \langle \mathbf{e}^T, \mathbf{y} \rangle$;   // $\langle \mathbf{e}^T, \mathbf{y} \rangle = \langle \mathbf{e}^T, \langle \mathbf{A}^T, \mathbf{s} \rangle \rangle + \langle \mathbf{e}^T, \mathbf{x} \rangle = \langle \mathbf{u}^T, \mathbf{s} \rangle + x'$
  $b \leftarrow z - a$;   // $z - a = x_z - x' + M\lfloor q/2 \rfloor$
  $M' \leftarrow \begin{cases} 1 & \text{if } \lfloor q/4 \rfloor \leq b \leq \lfloor 3q/4 \rfloor \\ 0 & \text{otherwise} \end{cases}$;
```

(i) suggests us to parametrise m over a value $\delta \in \mathbb{R}$ being such that $n^\delta > \lceil \log q \rceil$, hence obtaining

$$m = 6n^{1+\delta} \ .$$

Furthermore, we know from Function 2 that $\|\tilde{\mathbf{T}}_{\mathbf{B}_0}\| \leq \mathcal{O}(\sqrt{n \log q})$, or, in other terms, that$\|\tilde{\mathbf{T}}_{\mathbf{B}_0}\| \leq \mathcal{O}(\sqrt{m})$; hence, from the second condition, we obtain

$$s = \sqrt{m} \cdot \omega\left(\sqrt{\log(mr)}\right) \ .$$

In order to tackle (iii), we recall from Lemma 2 that $|x_z| \leq q\alpha \cdot \omega(\sqrt{\log m}) + 1/2$ and $|x'| = |\langle \mathbf{e}^T, \mathbf{x} \rangle| \leq \|\mathbf{e}\| \cdot q\alpha \cdot \omega(\sqrt{\log m}) + \|\mathbf{e}\|\sqrt{m}/2$ and from Lemma 1 that $\|\mathbf{e}\| \leq s\sqrt{mr}$; hence, due to triangular inequality, we obtain

$$\begin{aligned} |x_z - x'| &= |x_z| + |x'| \\ &\leq q\alpha \cdot \left(\omega\left(\sqrt{\log m}\right) + \|\mathbf{e}\| \cdot \omega\left(\sqrt{\log(mr)}\right)\right) + \frac{1}{2}\left(1 + \|\mathbf{e}\|\sqrt{m}\right) \\ &\leq q\alpha \cdot s\sqrt{mr} \cdot \omega\left(\sqrt{\log(mr)}\right) + \frac{1}{2}(1 + sm\sqrt{r}) \\ &\leq sq\alpha\sqrt{mr} \cdot \omega\left(\sqrt{\log(mr)}\right) + smr \ . \end{aligned}$$

Plugging the inequality in (iii) and letting $\hat{\omega} = \omega\left(\sqrt{\log(mr)}\right)$ we obtain

$$\begin{gathered} \ell sq\alpha \cdot \sqrt{mr} \cdot \hat{\omega} + \ell smr \leq q \\ q \cdot (\ell s\alpha \cdot \sqrt{mr} \cdot \hat{\omega} - 1) \leq \ell smr \end{gathered}$$

which suggests us to require

$$\alpha = \left(s \cdot \sqrt{mr} \cdot \omega\left(\sqrt{\log(mr)}\right)\right)^{-1}$$

hence obtaining from the previous inequality that

$$q \cdot (\ell \cdot \omega(1) - 1) \leq \ell smr \ .$$

Furthermore, in order to satisfy (iv) and recalling we obtain

$$q > 2\sqrt{n} \cdot \alpha^{-1} = s \cdot \sqrt{4nmr} \cdot \hat{\omega} \ .$$

Recalling from (i) that $m > 4n$, a suitable solution is given by

$$q = smr \cdot \omega\left(\sqrt{\log(mr)}\right) \ ,$$

solution yet still satisfying the sequence of inequalities we built for (iii).

We can resume the above stated conditions as follows

$$(\dagger) \qquad \begin{aligned} m &= 6n^{1+\delta}, \quad \text{with } \delta \in \mathbb{R} \mid n^{\delta} > \lceil \log q \rceil \\ s &= \sqrt{m} \cdot \omega\left(\sqrt{\log(mr)}\right) \\ q &= smr \cdot \omega\left(\sqrt{\log(mr)}\right) \\ \alpha &= \left(s \cdot \sqrt{mr} \cdot \omega\left(\sqrt{\log(mr)}\right)\right)^{-1} \end{aligned}$$

in order to provide the scheme security claim

Proposition 3 (Theorem 1 from [31])**.** *Let $\chi = \bar{\Psi}_\alpha$ and let m, s, q, and α be as from $(\dagger)$. The, if LWE$_{q,\chi}$ is hard, the CP-ABE scheme (*`Setup`*,* `KGen`*,* `Enc`*,* `Dec`*) defined by Algorithms 1, 2, 3, and 4 is secure against selective chosen plaintext attack (sCPA).*

In particular, if there exists an adversary $\mathcal{A}$ that breaks its sCPA security with advantage ϵ, then there exists an algorithm $\mathcal{B}$ solving LWE$_{q,\chi}$ with probability ϵ.

6. mR$_{\text{LWE}}$-CP-ABE

In this section we formally describe the mediated scheme mR$_{\text{LWE}}$-CP-ABE, the analysis of its parameter and the security proofs.

6.1. **The scheme.**

mR$_{\text{LWE}}$-CP-ABE shares the same parameter structure with regular CP-ABE scheme presented in Section 5. Requirements on these parameters are very similar too and are discussed in the next section. For this reason, `Setup` function is defined as in Algorithm 1 without any particular changes.

Concurrently, as described in Section 3.2, encryption procedure is not modified by the mediation process, hence `Enc` function is defined as in Algorithm 3.

The definition of the three remaining functions defining a revocable CP-ABE scheme follows in Algorithm 5–7.

6.2. **Parameter requirements.**

Requirements introduced in Section 5.2 still hold. However, error grows higher in `MDec` if compared to the lattice based CP-ABE scheme `Dec`. In fact, the requirement for a correct decryption is

$$|x_z - \sum_{j=0}^{k} x'_j - \sum_{j=1}^{k} x_j| \leq \frac{q}{\hat{\ell}} \ .$$

Do note that $\{x_j\}_{j=1}^{k}$ are sampled from the same distribution as x_z and $\{x'_j\}_{j=1}^{k}$ are obtained as it was for x' in the original algorithm, hence Lemma 2 still applies.

```
Algorithm 5: $\texttt{MKGen}(\texttt{msk}, \mathcal{S}, k) \rightarrow (\texttt{sk}, \{\texttt{mk}_j\}_{j=1}^{k})$
Input: the master secret key $\texttt{msk}$, a user attribute specification
       $\mathcal{S} = (S^+, S^-)$, and the number of mediators $k$
Output: the user secret key $\texttt{sk}$ holding the attribute specification $\mathcal{S}$ and
        the private secret $\mathbf{e} \leftarrow_\$ D_{\mathbb{Z}^{mr},s}$
Output: the mediator secret key $\texttt{mk}_j$ holding the private secret
        $\mathbf{mk}_j \leftarrow_\$ D_{\mathbb{Z}^{mr},s}$, for each $0 < j \leq k$

for each $i \in \mathcal{R}$ do
    $\mathbf{A}_i \leftarrow \begin{cases} \mathbf{B}_i^+ & \text{if } i \in S^+ \\ \mathbf{B}_i^- & \text{if } i \in S^- \end{cases}$;
$\mathbf{A} \leftarrow [\mathbf{B}_0 \| \mathbf{A}_1 \| \ldots \| \mathbf{A}_{|\mathcal{R}|}]$;
for $j = 1, \ldots, k$
    $\mathbf{u}_j \leftarrow_\$ U(\mathbb{Z}_q^n)$;
$\mathbf{mk}_j \leftarrow \texttt{GenSamplePre}(\mathbf{A}, \mathbf{T}_{\mathbf{B}_0}, \{0\}, s, \mathbf{u}_j)$;
$\mathbf{u}_0 \leftarrow \mathbf{u} - \sum_{j=1}^{k} \mathbf{u}_j$;
$\mathbf{e} \leftarrow \texttt{GenSamplePre}(\mathbf{A}, \mathbf{T}_{\mathbf{B}_0}, \{0\}, s, \mathbf{u}_0)$;
$\texttt{sk} \leftarrow (\mathcal{S}, \mathbf{e})$;
$\texttt{mk}_j \leftarrow (\mathbf{mk}_j)$;
```

```
Algorithm 6: $\texttt{PDec}(\mathbf{y}, \texttt{mk}_j) \rightarrow a_j$
Input: a vector $\mathbf{y}$ holding the information about the shared secret of a
       ciphertext and a mediator key $\texttt{mk}_j$
Output: the decryption information $a_j$

$x_j \leftarrow_\$ \chi$;
$a_j \leftarrow \langle \mathbf{mk}_j^T, \mathbf{y} \rangle + x_j$ ;
  // $\langle \mathbf{mk}_j^T, \mathbf{y} \rangle + x_j = \langle \mathbf{mk}_j^T, \langle \mathbf{A}^T, \mathbf{s} \rangle \rangle + \langle \mathbf{mk}_j^T, \mathbf{x} \rangle + x_j = \langle \mathbf{u}_j^T, \mathbf{s} \rangle + x'_j + x_j$
```

Due to triangular inequality and following the same reductions as before, we obtain

$$\begin{aligned} |x_z - \sum_{j=0}^{k} x'_j - \sum_{j=1}^{k} x_j| &\leq |x_z| - \sum_{j=0}^{k} |x'_j| - \sum_{j=1}^{k} |x_j| \\ &\leq (k+1)sq\alpha\sqrt{mr} \cdot \hat{\omega} + (k+1)smr \ . \end{aligned}$$

Plugging the inequality in the requirement for decryption we obtain

$$\begin{gathered} (k+1)\hat{\ell}sq\alpha \cdot \sqrt{mr} \cdot \hat{\omega} + (k+1)\hat{\ell}smr \leq q \\ q \cdot ((k+1)\hat{\ell}s\alpha \cdot \sqrt{mr} \cdot \hat{\omega} - 1) \leq (k+1)\hat{\ell}smr \ , \end{gathered}$$

whose solution is comparable to the one of the original scheme if we consider $\ell = \hat{\ell} \cdot (k+1)$ since the only requirement imposed on ℓ is $\ell > 4$ which still holds.

6.3. **Security of mR$_{\text{LWE}}$-CP-ABE.** The here presented mediated scheme is equivalent to the original scheme from the point of view of an external attacker. In fact, the encryption and decryption functions behaves the same as in the original scheme but for the addition of more noise (the more the mediators, the higher the

```
Algorithm 7: MDec(C, sk) → M or ⊥
Input: a ciphertext structure $C$ and a user secret key sk
Output: the message $M' \in \{0,1\}$ which corresponds to the original
        message $M$ if $|x_z - \sum_{j=0}^{k} x'_j - \sum_{j=1}^{k} x_j| < q/4$ (say $\leq q/\hat{\ell}$ for each
        $\hat{\ell} > 4$)
if $\mathcal{S} \nvdash \mathcal{W}$
    return $\perp$;
for each $i \in \mathcal{R}$ do
    $\mathbf{y}_i \leftarrow \begin{cases} \mathbf{c}_i^+ & \text{if } i \in S^+ \\ \mathbf{c}_i^- & \text{if } i \in S^- \end{cases}$;
$\mathbf{y} \leftarrow [\mathbf{c}_0 \| \mathbf{y}_1 \| \dots \| \mathbf{y}_{|\mathcal{R}|}]$;
$a_0 \leftarrow \langle \mathbf{e}^T, \mathbf{y} \rangle$;    // $\langle \mathbf{e}^T, \mathbf{y} \rangle = \langle \mathbf{e}^T, \langle \mathbf{A}^T, \mathbf{s} \rangle \rangle + \langle \mathbf{e}^T, \mathbf{x} \rangle = \langle \mathbf{u}_0^T, \mathbf{s} \rangle + x'_0$
for $j = 1, \dots, k$
    Request to the $j$-th mediator $a_j \leftarrow$ PDec$(\mathbf{y}, \circ)$;
$a \leftarrow \sum_{j=0}^{k} a_j$;    // $\sum_{j=0}^{k} a_j = \sum_{j=0}^{k} \left( \langle \mathbf{u}_j^T, \mathbf{s} \rangle + x'_j \right) + \sum_{j=1}^{k} x_j =$
    $\langle \mathbf{u}^T, \mathbf{s} \rangle + \sum_{j=0}^{k} x'_j + \sum_{j=1}^{k} x_j$
$b \leftarrow z - a$;    // $z - a = x_z - \sum_{j=0}^{k} x'_j - \sum_{j=1}^{k} x_j + M\lfloor q/2 \rfloor$
$M' \leftarrow \begin{cases} 1 & \text{if } \lfloor q/4 \rfloor \leq b \leq \lfloor 3q/4 \rfloor \\ 0 & \text{otherwise} \end{cases}$;
```

noise). We can further claim, analogously to Proposition 3, the security of the scheme under sCPA:

Theorem 1 (Security of mR$_{\text{LWE}}$-CP-ABE (external)). *Let $\chi = \bar{\Psi}_\alpha$ and let m, s, q, and α be as from (†). Then, if LWE$_{q,\chi}$ is hard, the revocable CP-ABE scheme (*Setup*,* MKGen*,* Enc*,* PDec*,* MDec*) defined by Algorithms 1, 5, 3, 6, and 7 is secure against selective chosen plaintext attack (sCPA).*

In particular, if there exists an adversary $\mathcal{A}$ that breaks its sCPA security, then there exists an adversary $\mathcal{B}$ that solves the LWE$_{q,\chi}$ decision problem.

The proof of the theorem is analogous to the one from [31]; however, we report it for completeness.

Proof. Assume there exists a polynomial-time adversary $\mathcal{A}$ capable of breaking IND-sCPA for the mediated scheme with advantage ϵ by using at most q key generation queries by obtaining both user and mediator keys.

Let $\mathcal{O}(\circ)$ be an oracle that either samples always from $A_{\mathbf{s},\chi}$ or from uniform distribution $U(\mathbb{Z}_q)$. Let $\mathcal{B}$ be an attacker who cooperate with $\mathcal{A}$ and wants to decide whether of the two distributions $\mathcal{O}(\circ)$ is sampling from.

The idea of the cooperation is to build a CP-ABE game – with $\mathcal{A}$ as the attacker and $\mathcal{B}$ as the challenger – that can be won with probability noticeably grater than $1/2$ if and only if $\mathcal{O}(\circ)$ is sampling from $_{\mathbf{s},\chi}$. Assuming such a game exists, then $\mathcal{B}$ can discriminate between the two distributions.

We recall that, in order to run the game, the challenger $\mathcal{B}$ is only required to be able to (i) provide a public key to $\mathcal{A}$, (ii) encrypt a message and (iii) make q

generations of valid keys (with respect to the provided public key) on attribute specifications that does not satisfies the challenged access structure; decryption is hence not required as well as being able to generate secret keys for attribute specification satisfying the challenged access structure.

Let us formally define the game:

Init. $\mathcal{A}$ chooses a challenge $\mathcal{W} = (W^+, W^-)$ and prompts it to $\mathcal{B}$.

Setup. $\mathcal{B}$ samples $(\mathbf{a}, y) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ pairs multiple times from $\mathcal{O}(\circ)$ in order to build the matrices $\mathbf{B}_0$ and $\mathbf{B}_i^{\pm}$ needed by the chosen access structure (out of the vectors $\mathbf{a}_i$) and to save (potentially) LWE-valid vectors $\mathbf{c}_i$ for the ciphertext creation. The total number of samples required are $(|S^+| + |S^-| + 1) \cdot m + 1$ and they are used to build the following couples:

- $(\mathbf{B}_0, \mathbf{v}_0) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$;
- $(\mathbf{u}, v_u) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$;
- $(\mathbf{B}_i^+, \mathbf{v}_i^+) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ for each $i \in S^+$;
- $(\mathbf{B}_i^-, \mathbf{v}_i^-) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ for each $i \in S^-$.

Then, in order to create the missing matrices $\mathbf{B}_i^+$ and $\mathbf{B}_i^-$ (respectively for $i \notin S^+$ and $i \notin S^-$) and coherently being able to run `MKGen` algorithm on $\mathcal{S}$ such that $\mathcal{S} \nvdash \mathcal{W}$, the challenger $\mathcal{B}$ computes:

- $(\mathbf{B}_i^+, \mathbf{T}_{\mathbf{B}_i^+}) \leftarrow \texttt{TrapGen}(n, m, q)$ for each $i \notin S^+$;
- $(\mathbf{B}_i^-, \mathbf{T}_{\mathbf{B}_i^-}) \leftarrow \texttt{TrapGen}(n, m, q)$ for each $i \notin S^-$.

Finally, the challenger stores $(\{\mathbf{T}_{\mathbf{B}_i^+}\}_{i \in S^+}, \{\mathbf{T}_{\mathbf{B}_i^+}\}_{i \in S^+})$ for the key generation, stores $(\mathbf{v}_0, v_u, \{\mathbf{v}_\mathbf{i}^+\}_{i \in S^+}, \{\mathbf{v}_\mathbf{i}^-\}_{i \in S^-})$ for the ciphertext creation, and outputs the public key $\texttt{pk} = (\mathbf{B}_0, \{\mathbf{B}_i^+, \mathbf{B}_i^-\}_{i \in \mathcal{R}}, \mathbf{u})$ to the attacker $\mathcal{A}$.

Keygen query. Upon receiving a user attribute specification $\mathcal{S}$ from $\mathcal{A}$, if $\mathcal{S} \vdash \mathcal{W}$ then $\mathcal{B}$ outputs $\perp$. Otherwise, there exists at least one attribute $i \in S^+$ such that $i \notin W^+$ or $i \in S^-$ such that $i \notin W^-$; let $\hat{\mathbf{T}}$ be the short basis generated by `TrapGen` during setup associated to such an attribute. $\mathcal{B}$ finally runs and outputs $\texttt{MKGen}((\texttt{pk}, \hat{\mathbf{T}}), \mathcal{S})$ to $\mathcal{A}$. Do note that the so-formed master secret key is valid for $\mathcal{S}$ (and for all the user specifications containing i as does $\mathcal{S}$) since, according Function 4, `GenSamplePre` requires whatever short basis generated from a subset of m linearly independent vectors of $\mathbf{A}$ (the matrix in $\mathbb{Z}_q^{n \times mk}$ defined in Algorithm 5).

Challenge. The attacker $\mathcal{A}$ submits $M_0, M_1 \in \{0, 1\}$ to the challenger $\mathcal{B}$, who randomly chooses $b \in \{0, 1\}$ and returns the (possibly valid) ciphertext associated with M_b. However, since $\mathcal{B}$ wants to output a valid ciphertext only if $\mathcal{O}(\circ)$ is sampling from $A_{\mathbf{c},s}$, the idea is to use the stored values from the setup in order to emulate the LWE instances of the `Enc` function. Therefore $\mathcal{B}$ computes and outputs $C = (W, z, \mathbf{c_0}, \{\mathbf{c}_i^+\}_{i \in W^+}, \{\mathbf{c}_i^-\}_{i \in W^-})$ with:

- $z \leftarrow v_u + M_b \lfloor q/2 \rfloor$, where v_u emulates $\langle \mathbf{u}^T, \mathbf{s} \rangle + x_z$;
- $\mathbf{c}_0 \leftarrow \mathbf{v}_0$ to emulate $\langle \mathbf{B}_0^T, \mathbf{s} \rangle + \mathbf{x}$;
- $\mathbf{c}_i^+ \leftarrow \mathbf{v}_i^+$ to emulate $\langle {\mathbf{B}_i^+}^T, \mathbf{s} \rangle + \mathbf{x}$, for each $i \in W^+$;
- $\mathbf{c}_i^- \leftarrow \mathbf{c}_i^-$ to emulate $\langle {\mathbf{B}_i^-}^T, \mathbf{s} \rangle + \mathbf{x}$, for each $i \in W^-$.

$\mathcal{A}$ is allowed to make more key generation queries after the challenge has been set. Eventually, it outputs a guess b' for b that is correct either with probability $1/2 + \epsilon$ if $\mathcal{O}(\circ)$ is sampling from $A_{\mathbf{c},s}$ or with probability $1/2$ if it is sampling from

$U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$. Hence $\mathcal{B}$ guesses $A_{\mathbf{c},s}$ if $b = b'$ (*i.e.* $\mathcal{A}$ is correct) or guesses $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$ if $b \neq b'$ (*i.e.* $\mathcal{A}$ is wrong).

Do note that if $\mathcal{O}(\circ)$ is sampling from $A_{\mathbf{c},s}$, then $\mathcal{B}$ guesses right with the same non-negligible advantage as $\mathcal{A}$ does. So, if such $\mathcal{A}$ do exists, $\mathcal{B}$ can solve LWE problems, which yields the claim. □

However, due to the revocation requirement, security must be also ensured if the attacker is one or more users, in the sense that

(i-u) a user is not able to decrypt as far as at least a SM denies its cooperation;
(ii-u) a user can not reject a revocation in polynomial time, even after a polynomial number of correct decryptions (meaning that he can neither break nor forge a SM key);
(iii-u) multiple user can not collude to retrieve a SM key or to decrypt a message;

and if the attacker is one or more SMs, in the sense that:

(i-m) one or more SM can not collude to decrypt a message, even upon receiving many mediator keys from different users;
(ii-m) one or more SM can not collude to retrieve a user secret $\mathbf{e}$.

We do note that mediator keys and user keys are complementary in decryption phase and they are generated all starting from $\mathbf{u}_i$ distributed uniformly at random: $\mathbf{u}_0$ is given by the difference of vector distributed uniformly at random, hence it is still distributed uniformly at random. Since $\mathbf{u}_i$ are generated randomly for each user, it follows that different users $\mathbf{e}$ are independent one from the other, hence combining information from different keys ensure no further knowledge, ensuring (iii-u).

A similar outcome can be derived for SMs holding mediator keys related to different users. Moreover SM and users receive no information about mutual keys by-design and mediator keys, if equipped with $\mathcal{S}$, are equivalent to the user ones (*i.e.* SM keys are weaker than user ones), we have that (i-u) implies (i-m) (*i.e.* if user is not able to decrypt without even a single SM, then decryption can not occur without the collaboration of k parties out of the $k+1$, no matters which one is missing).

We claim the following theorem to prove (i-u):

Theorem 2 (Security of PDec algorithm (break))**.** *Let $\chi = \bar{\Psi}_\alpha$ and let m, s, q, and α be as from (†). Then, if $LWE_{q,\chi}$ is hard, the CP-ABE scheme (*`Setup`*,* `MKGen`*,* `Enc`*,* `PDec`*,* `MDec`*) defined by Algorithms 1, 5, 3, 6, and 7 is secure against selective chosen plaintext attack (sCPA) carried out by a user if at least one mediator does not participate in the decryption.*

In particular, if there exists an adversary $\mathcal{A}$ that breaks its sCPA security, then there exists an adversary $\mathcal{B}$ that solves the $LWE_{q,\chi}$ decision problem.

Proof. If at least a mediator (say $\hat{j}$) does not take part to the decryption procedure, from the client perspective the problem resemble to solve the non-mediated version of the scheme with higher noise on z. In fact, he can compute $z' \leftarrow z - \sum_{j=0,j\neq\hat{j}}^{k} a_j$ and $C' = (W, z', \mathbf{c_0}, \{\mathbf{c}_i^+\}_{i\in W^+}, \{\mathbf{c}_i^-\}_{i\in W^-})$ is a valid ciphertext (apart from the potentially higher noise) for the non-mediated scheme with public key $\mathtt{pk} = (\mathbf{B}_0, \{\mathbf{B}_i^+, \mathbf{B}_i^-\}_{i\in\mathcal{R}}, \mathbf{u}_{\hat{\mathbf{j}}})$.

The only advantage the client has is the knowledge of its $\mathbf{e}$ that, however, does not reveal further information neither about the short basis $\mathbf{T}_{\mathbf{B}_0}$ nor about other keys[2] since they are obtained from `GenSamplePre` applied to uniformly random $\mathbf{u}$.

It follows that if there exists an adversary $\mathcal{A}$ that breaks sCPA for the mediated scheme under these assumptions, then there exists an adversary $\mathcal{A}'$ that breaks sCPA for the non-mediated scheme and hence, by Proposition 3, there exists an adversary $\mathcal{B}$ that solves the LWE$_{q,\chi}$ decision problem. □

Furthermore, by design, SMs receive no information about the decryption procedure when a request is submitted by a user; hence, they can not learn anything about the user secret neither from the query itself nor from other sources. Analogously, (ii-m) follows.

Do also consider that mediators receive no information about the attribute specification $\mathcal{S}$ as well; however, if mediator do have access to the database of ciphertexts and can guess which ciphertext was delivered by the user, they can guess the attribute specification by matching vector $\mathbf{y}$ with the allowed $\mathbf{c}_i^{\pm}$. In particular, guessing the correct match between delivered $\mathbf{y}$ and ciphertext is mainly a combinatorial matter that has not received many attention in literature. However, we point out that, whenever it would get important to preserve the privacy between which users required which ciphertext (*e.g.* to prevent user profiling), a possible solution for the user would be to protect $\mathbf{y}$ by adding a noise $\mathbf{x} \leftarrow_{\$} \chi^{mr}$. It is out of the scope of this paper showing the complete proof of correctness, however do note that $\mathbf{y} + \mathbf{x}$ would still be considered as a valid LWE sample (see also later the proof of Theorem 3) with higher noise and decryption would still be correct with some correction on total noise size.

Finally we claim the following theorem that tackles (ii-u):

Theorem 3 (Security of `PDec` algorithm)**.** *Let $\chi = \bar{\Psi}_\alpha$ and let m, s, q, and α be as from (†). Then, if LWE$_{q,\chi}$ is hard, the function* `PDec` *defined by Algorithm 6 is hard to*

- *break, in the sense that there exists no polynomial-time algorithm to retrieve* `mk` *from a polynomially bounded number of pair $(\mathbf{y}, a)$, where $a \leftarrow$* `PDec`$(\mathbf{y}, \texttt{mk})$.
- *forge, in the sense that there exists no polynomial-time algorithm to evaluate a^* from an arbitrary $\mathbf{y}^*$, where $a^* \leftarrow$* `PDec`$(\mathbf{y}^*, \texttt{mk})$*, without knowing* `mk` *from a priorly obtained polynomially bounded number of pair $(\mathbf{y}_i, a_i)$, where $a_i \leftarrow$* `PDec`$(\mathbf{y_i}, \texttt{mk})$.

In particular, if there exists an adversary $\mathcal{A}$ that breaks (forges) `PDec`*, then there exists an adversary $\mathcal{B}$ that breaks the LWE$_{q,\chi}$ search (decision) problem.*

Proof. We recall $\mathbf{y} \leftarrow_{\$} A_{\mathbf{s},\chi}$ since $\mathbf{y} = \langle \mathbf{A}, \mathbf{s} \rangle + \mathbf{x}$, hence $\mathbf{y}$ is indistinguishable from the uniform distribution for the LWE$_{q,\chi}$ hardness.

It is easy to see that $a \in A_{\mathbf{mk},s}$, in fact $a = \langle \mathbf{mk}^T, \mathbf{y} \rangle + x$ where $\mathbf{y}$ is statistically uniform to random and $x \leftarrow_{\$} \chi$. It follows that `PDec` is an actual instance of LWE$_{q,\chi}$, hence proving the claim. □

[2] If this was the case, do note also that users could forge other users keys at first glance

7. Multiple bit encryption

The original CP-ABE scheme introduced in Section 5 was also proposed as a N-bit encryption scheme (with $N \in \mathbb{N}$), where the same shared secret $\mathbf{s}$ was used to encrypt a vector of message bits $\mathbf{M} \in \{0,1\}^N$.

The authors introduced a public matrix $\mathbf{U} \in \mathbb{Z}_q^{n\times N}$ and a user secret matrix $\mathbf{E}$ of size $mr \times N$, where each of the N columns is generated by applying `GenSamplePre` to a different column of $\mathbf{U}$. Here, encryption works analogously, with the only difference within the evaluation of z, now being a vector $\mathbf{z}$:

$$\mathbf{z} \leftarrow \langle \mathbf{U}^T, \mathbf{s}\rangle + \mathbf{x}_z + \mathbf{M}\lfloor q/2 \rfloor, \qquad \text{with } \mathbf{x}_z \leftarrow_{\$} \chi^N \ .$$

Decryption, at the same glance, does not require any further care; in fact, once retrieved the suitable $\mathbf{y}$ vector, we can perform:

$$\begin{aligned}&\mathbf{a} \leftarrow \langle \mathbf{E}^T, \mathbf{y}\rangle = \langle \mathbf{E}^T, \langle \mathbf{A}^T, \mathbf{s}\rangle\rangle + \langle \mathbf{E}^T, \mathbf{x}\rangle = \langle \mathbf{U}^T, \mathbf{s}\rangle + \mathbf{x}'\\ &\mathbf{b} \leftarrow \mathbf{z} - \mathbf{a} = \mathbf{x}_z - \mathbf{x}' + \mathbf{M}\lfloor q/2 \rfloor\end{aligned}$$

and, finally, by identifying $\mathbf{M} = (M_1, \dots, M_N)$ and $\mathbf{b} = (b_1, \dots, b_N)$:

$$M_i \leftarrow \begin{cases} 1 & \text{if } \lfloor q/4 \rfloor \le b_i \le \lfloor 3q/4 \rfloor \\ 0 & \text{otherwise} \end{cases} \qquad \text{for } i = 1, \dots, N \ .$$

A notable advantage of this approach is given by the size of the ciphertext, since only a single copy of $\mathbf{c}_0$, $\mathbf{c}_i^+$ (for each $i \in W^+$) and $\mathbf{c}_i^-$ (for each $i \in W^-$) is needed regardless of the number N of encrypted bits. Therefore, C is made of $N + m \cdot |W^+| \cdot |W^-| \le N + 2mr$ values in $\mathbb{Z}_q$, compared with the $2Nmr$ generated by N different single-bit encryptions.

Clearly, the mediated scheme introduced in this paper can benefit from the same approach, where mediators and user both receive a matrix $\mathbf{MK}_j$ and $\mathbf{E}$ of size $mr \times N$, built upon random matrices $\mathbf{U}_j \leftarrow_{\$} U(\mathbb{Z}_q^{n\times N})$ and upon $\mathbf{U}_0 = \mathbf{U} - \sum_{j=1}^k \mathbf{U}_j$ respectively.

Furthermore, security is ensured with the same claims as per the original paper.

8. Experiments with mR$_{\text{LWE}}$-CP-ABE

Here we report the results of the performance experiments we carry out to evaluate the overhead introduced by the generation of the mediator keys and by their application in the decryption phase. In order to do that we implement mR$_{\text{LWE}}$-CP-ABE on top of the Palisade-ABE implementation [3] of [31] and we compare the execution time of `KGen` vs `MKGen` and of `Dec` vs (`PDec` + `MDec`) vs `Enc`. We compare the time for (`PDec` + `MDec`) also against the time needed for `Enc` algorithm as the procedure `PDec` when generates and adds the error x_j to protect the mediator key, actually is performing a LWE scheme. We carry out the following performance experiments on a Nvidia DGX-1 equipped with 512 GB of memory; for each experiment we report in Table 1 the average execution time over 20 repetitions for the three different security levels, namely HEStd_128_classic, HEStd_192_classic and HEStd_256_classic, and for five values for the number of attributes, for instance 6,8,16,20,34. We conduct experiments fixing the number of encrypted bits to 10000 and by setting $k = 1$.

[3] Last access time 02 -12-2022`https://gitlab.com/palisade/palisade-abe`

As mentioned before, by seeing Table 1, it is clear that the decryption in our system (`PDec` + `MDec`) requires almost the time of the encryption. For what concern the `KGen` vs `MKGen`, the latter requires to double the time of the former; the behaviour is what we expect as `MKGen` needs to generate both the user key and the mediator keys and in the experiments setup, as mentioned, $k = 1$ so actually it generates two keys.

Parameters		**Time (ms)**				
Security-Level	**#Attributes**	`KGen`	`MKGen`	`Dec`	`PDec` + `MDec`	`Enc`
HEStd_128_classic	6	179	354	1	54	47
HEStd_128_classic	8	223	451	2	75	73
HEStd_128_classic	16	386	769	3	141	129
HEStd_128_classic	20	465	938	4	185	174
HEStd_128_classic	32	725	1463	7	309	276
HEStd_192_classic	6	108	212	0	23	21
HEStd_192_classic	8	125	248	1	32	31
HEStd_192_classic	16	195	387	1	59	56
HEStd_192_classic	20	227	454	2	80	73
HEStd_192_classic	32	336	657	3	117	112
HEStd_256_classic	6	341	681	3	103	99
HEStd_256_classic	8	435	864	4	149	147
HEStd_256_classic	16	771	1550	8	282	272
HEStd_256_classic	20	929	1869	9	381	363
HEStd_256_classic	32	1470	2947	16	687	574

Table 1. Average execution time (ms) of `KGen`, `MKGen`, `Dec`, `PDec`, `MDec` and `Enc` algorithms. We run experiments by varying the security level and the values for attributes. We fix the number of security mediators to $k = 1$ and the size of plaintext to 10000 bits.

9. Conclusions and further work

In this paper, we have presented – to the best of our knowledge – the first post-quantum safety scheme for revocable CP-ABE based on LWE problem over lattices. The scheme takes advantage of the lattice based CP-ABE scheme firstly presented in [31] by building upon it a server-aided fine-grained revoking system (mR$_{\text{LWE}}$-CP-ABE). Server involved are considered semi-trusted, hence the security proofs are given against different threat models. Security and applications are discussed both in the single-bit and in the multi-bit approach.

To conclude, the here proposed scheme mR$_{\text{LWE}}$-CP-ABE is implemented on the ABE spin-off of the well-established open-source library Palisade to experimentally validate and provide some early performances estimation with particular attention to the overhead with respect to the original scheme. The implementation will be released open source to let the community independently test and evaluate it.

In future implementation, we will develop a similar approach on the further scheme proposed in [32]. Furthermore, we also plan to provide support to other libraries, including *e.g.* Microsoft SEAL ([25]) and Pyfhel as well as to carry out a more in-depth performance analysis of the system.

Acknowledgements

E. Onofri acknowledges the Gruppo Nazionale per il Calcolo Scientifico (GNCS) of Istituto Nazionale di Alta Matematica (INdAM).

M. Pedicini acknowledges the Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA) of Istituto Nazionale di Alta Matematica (INdAM).

References

[1] Divesh Aggarwal and Eldon Chung. A note on the concrete hardness of the shortest independent vector in lattices. *Information Processing Letters*, 167:106065, 2021. [DOI:10.1016/j.ipl.2020.106065].

[2] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H) IBE in the standard model. *Eurocrypt'10 and PKC'10 joint work*, 2010. [Author's website].

[3] Ruqayah R Al-Dahhan, Qi Shi, Gyu Myoung Lee, and Kashif Kifayat. Survey on revocation in Ciphertext-Policy Attribute-Based encryption. *Sensors (Basel)*, 19(7):1695, April 2019. [DOI:10.3390/s19071695].

[4] Joël Alwen and Chris Peikert. Generating Shorter Bases for Hard Random Lattices. In Susanne Albers and Jean-Yves Marion, editors, *26th International Symposium on Theoretical Aspects of Computer Science STACS 2009*, Proceedings of the 26th Annual Symposium on the Theoretical Aspects of Computer Science, pages 75–86, Freiburg, Germany, February 2009. IBFI Schloss Dagstuhl. [inria:00359718].

[5] Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. On the quantitative hardness of cvp. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 13–24, 2017. [DOI:10.1109/FOCS.2017.11].

[6] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 321–334, May 2007. [DOI:10.1109/SP.2007.11].

[7] Johannes Blömer and Jean-Pierre Seifert. On the complexity of computing short linearly independent vectors and short bases in a lattice. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, STOC '99, pages 711–720, New York, NY, USA, 1999. Association for Computing Machinery. [DOI:10.1145/301250.301441].

[8] Dan Boneh, Xuhua Ding, Gene Tsudik, and Chi-Ming Wong. A method for fast revocation of public key certificates and security capabilities. In Dan S. Wallach, editor, *10th USENIX Security Symposium, August 13-17, 2001, Washington, D.C., USA*. USENIX, 2001. usenix.org/publications/library/proceedings/sec01/boneh.html.

[9] David Cash, Dennis Hofheinz, and Eike Kiltz. How to delegate a lattice basis. Cryptology ePrint Archive, Paper 2009/351, 2009. [eprint:2009/351].

[10] Hui Cui, Robert H. Deng, Xuhua Ding, and Yingjiu Li. Attribute-based encryption with granular revocation. In Robert Deng, Jian Weng, Kui Ren, and Vinod Yegneswaran, editors, *Security and Privacy in Communication Networks*, pages 165–181, Cham, 2017. Springer International Publishing. [DOI:10.1007/978-3-319-59608-2_9].

[11] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206, 2008. [DOI:10.1145/1374376.1374407].

[12] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 89–98, New York, NY, USA, 2006. Association for Computing Machinery. [DOI:10.1145/1180405.1180418].

[13] Russell Impagliazzo and Ramamohan Paturi. On the complexity of k-sat. *Journal of Computer and System Sciences*, 62(2):367–375, 2001. [DOI:10.1006/jcss.2000.1727].

[14] Joseph K. Liu, Tsz Hon Yuen, Peng Zhang, and Kaitai Liang. Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list. In Bart Preneel and

Frederik Vercauteren, editors, *Applied Cryptography and Network Security*, pages 516–534, Cham, 2018. Springer International Publishing. [DOI:10.1007/978-3-319-93387-0_27].

[15] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007. [DOI:10.1137/S0097539705447360].

[16] Steve Moffat, Mohammad Hammoudeh, and Robert Hegarty. A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, ICFNDS '17, New York, NY, USA, 2017. Association for Computing Machinery. [DOI:10.1145/3102304.3102338].

[17] PALISADE Lattice Cryptography Library (release 1.11.2). [Palisade Crypto], May 2021.

[18] Chris Peikert. Some recent progress in lattice-based cryptography. In *Theory of Cryptography*, pages 72–72. Springer Berlin Heidelberg, 2009. [DOI:10.1007/978-3-642-00457-5_5].

[19] Tran Viet Xuan Phuong, Guomin Yang, Willy Susilo, and Xiaofeng Chen. Attribute based broadcast encryption with short ciphertext and decryption key. In Günther Pernul, Peter Y A Ryan, and Edgar Weippl, editors, *Computer Security – ESORICS 2015*, pages 252–269, Cham, 2015. Springer International Publishing. [DOI:10.1007/978-3-319-24177-7_13].

[20] Marco Rasori, Michele La Manna, Pericle Perazzo, and Gianluca Dini. A survey on attribute-based encryption schemes suitable for the internet of things. *IEEE Internet of Things Journal*, 9(11):8269–8290, June 2022. [DOI:10.1109/JIOT.2022.3154039].

[21] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC'05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 84–93. ACM, New York, 2005. [DOI:10.1145/1060590.1060603].

[22] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009. [DOI:10.1145/1568318.1568324].

[23] Amit Sahai, Hakan Seyalioglu, and Brent Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, pages 199–217, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. [DOI:10.1007/978-3-642-32009-5].

[24] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, pages 457–473, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. [DOI:10.1007/11426639_27].

[25] Microsoft SEAL (release 4.0). `https://github.com/Microsoft/SEAL`, March 2022. Microsoft Research, Redmond, WA.

[26] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, nov 1979. [DOI:10.1145/359168.359176].

[27] Xingxing Xie, Hua Ma, Jin Li, and Xiaofeng Chen. An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing. *JUCS - Journal of Universal Computer Science*, 19(16):2349–2367, 2013. [DOI:10.3217/jucs-019-16-2349].

[28] Shengmin Xu, Guomin Yang, and Yi Mu. Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. *Information Sciences*, 479:116–134, 2019. [DOI:10.1016/j.ins.2018.11.031].

[29] Yanjiang Yang, Xuhua Ding, Haibing Lu, Zhiguo Wan, and Jianying Zhou. Achieving revocable fine-grained cryptographic access control over cloud data. In Yvo Desmedt, editor, *Information Security*, pages 293–308, Cham, 2015. Springer International Publishing. [DOI:10.1007/978-3-319-27659-5_21].

[30] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Attribute based data sharing with attribute revocation. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '10, page 261–270, New York, NY, USA, 2010. Association for Computing Machinery. [DOI:10.1145/1755688.1755720].

[31] Jiang Zhang and Zhenfeng Zhang. A ciphertext policy attribute-based encryption scheme without pairings. In *International Conference on Information Security and Cryptology*, pages 324–340. Springer, 2011. [DOI:10.1007/978-3-642-34704-7_23].

[32] Jiang Zhang, Zhenfeng Zhang, and Aijun Ge. Ciphertext policy attribute-based encryption from lattices. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pages 16–17, 2012. [DOI:10.1145/2414456.2414464].

[33] Yinghui Zhang, Robert H. Deng, Shengmin Xu, Jianfei Sun, Qi Li, and Dong Zheng. Attribute-based encryption for cloud computing access control: A survey. *ACM Comput. Surv.*, 53(4), aug 2020. [DOI:10.1109/JIOT.2022.3154039].