A symmetric LWE-based Multi-Recipient Cryptosystem

Saikat Gope, Srinivasan Krishnaswamy, Chayan Bhawal

Abstract—This article describes a post-quantum multi-recipient symmetric cryptosystem whose security is based on the hardness of the LWE problem. In this scheme a single sender encrypts multiple messages for multiple recipients generating a single ciphertext which is broadcast to the recipients. Each recipient decrypts the ciphertext with her secret key to recover the message intended for her. In this process, the recipient cannot efficiently extract any information about the other messages. This scheme is intended for messages like images and sound that can tolerate a small amount of noise. This article introduces the scheme and establishes its security based on the LWE problem. Further, an example is given to demonstrate the application of this scheme for encrypting multiple images.

Index Terms—LWE problem, pseudorandom map, multi-recipient cryptosystem.

I. INTRODUCTION

A Multi-Recipient Encryption Scheme (MRES) simultaneously encrypts multiple messages for multiple receivers. The idea of MRES was introduced by Bellare et al. [1]. This scheme was a public key encryption scheme wherein a set of messages intended for different users are simultaneously encrypted using their respective public keys. The encryption algorithm generates a set of ciphertexts, one for each recipient. Further, Kurosawa proposed an MRES design having a shortened ciphertext [2]. The ciphertext size is almost half of the n recipient scheme and showed its security to be almost the same as that of a single-recipient scheme. MRES using randomness re-use was proposed in [3] for reducing transmission load and computational cost. Other notable contributions in this area include [4]–[6].

With the advancement of quantum computation and its applications [7], [8], problems such as the discrete logarithm problem or factorization of primes can be efficiently solved. Hence, encryption schemes whose security is based on the hardness of these problems become vulnerable to quantum attacks. Lattice-based problems serve as promising alternatives to develop schemes that are resistant to quantum attacks. Some hard problems related to lattices are the GapSVP$_\gamma$ problem, GapCVP$_\gamma$ problem and the SIVP problem [9]–[12]. The Learning With Error (LWE) problem [13], [14] involves solving a set of linear equations over a large finite field in the presence of noise. The hardness of the LWE problem reduces to that of the GapSVP$_\gamma$ problem [9]–[11]. This problem has therefore led to the development of numerous post-quantum cryptosystems.

In this paper, we implement a symmetric Multi-Key Multi-Recipient (MKMR) encryption scheme based on the hardness of the LWE problem. In this scheme the sender simultaneously encrypts a set of messages for a set of receivers. each receiver has a secret key shared with the sender. The sender generates **a**

single ciphertext, which each user decrypts using their respective secret key to recover their intended message. We prove that the resulting tuple of ciphertexts is indistinguishable from a random block of data sampled from a uniform distribution of the appropriate size. Further, we demonstrate an application of this scheme for multiple image encryption.

This paper is organized into 4 sections. Section 2 introduces the preliminaries that are needed to understand the rest of the paper. In section 3, we explain the LWE-based multi-recipient encryption scheme along with an example. The conclusion is presented in section 4.

A. Motivation and Contribution

Most multi-recipient encryption schemes available in literature are public key schemes [1]–[6]. Further, the security of these schemes are based on the hardness of problems like the discrete logarithm problem. These problems are efficiently solvable using quantum algorithms. Hence the available multi-recipient schemes are vulnerable in post-quantum scenario. This paper proposes a post-quantum symmetric multi-recipient encryption scheme whose security is based on the hardness of the LWE problem. A unique feature of this scheme is that it generates a single ciphertext for all messages. Each recipient uses their respective key to decrypt the ciphertext and recover the message intended for them. Sending the same ciphertext to multiple recipients introduces redundancy; if a recipient loses the ciphertext, they can recover it from another recipient. The proposed scheme is computationally light, with the encryption process consisting only of repeated matrix vector multiplications.

II. PRELIMINARIES

A. Notation Table

Table 1 shows the set of notations that are used in the paper. We now formally define lattices and some of the hard problems related to lattices include the approximate shortest vector problem i.e. the GapCVP$_\gamma$ problem and Learning With Error (LWE) problem.

B. Lattices

Definition 1. Given n-linearly independent basis vectors $\mathcal{B} = \{b_1, b_2, \ldots, b_n\} \subset \mathbb{R}^n$, the set of all integer linear combination of basis vectors $\mathcal{B}$ is defined as lattice $\mathcal{L} \subset \mathbb{R}^n$. Mathematically, it is represented as:

$$\mathcal{L} := \mathcal{L}(\mathcal{B}) = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z}, 1 \le i \le n \right\} \quad (1)$$

Definition 2 ([11]). Consider an n dimensional lattice $\mathcal{L}$ with basis vectors $\mathcal{B}$ as in Definition 1, the discrete Gaussian

TABLE I
TABLE OF SYMBOLIC NOTATIONS

Symbols Used	Interpretations
$\mathbb{F}_q$	Finite field $\mathbb{F}_q$ with cardinality q
$\mathbb{F}_q^n$	n-dimensional vector space over finite field $\mathbb{F}_q$ with cardinality q
$\|v\|_p$	l_p norm of n-dimensional vector v over field $\mathbb{F}$ with $p \geq 1$
$\|v\|$	2 norm of n-dimensional vector v over field $\mathbb{F}$
$\langle s,v \rangle$	Inner product of vector s and vector v where $s,v \in \mathbb{F}_q^n$
$\lceil v \rfloor$	Round elements of array v to its nearest integer
$v \bmod q$	The integer between $\lfloor \frac{-q}{2} \rfloor$ and $\lfloor \frac{q}{2} \rfloor$ which is equivalent to the integer v modulo q in $\mathbb{F}_q$
$\mathcal{M}_i$	i^{th} column of matrix $\mathcal{M}_{m \times l}$ where $i = 1, 2, \ldots, l$
χ^m	Set of m tuple elements from distribution χ

probability distribution over lattice $\mathcal{L}$ with standard deviation $\sigma > 0$ is defined as

$$\mathcal{D}_{\mathcal{L},\sigma}(v) := \frac{\rho_\sigma(v)}{\rho_\sigma(\mathcal{L})} \qquad (2)$$

where $\rho_\sigma(v) := e^{\left(-\pi\|v\|^2/2\pi\sigma^2\right)}$ for all $v \in \mathcal{L}$ and $\rho_\sigma(\mathcal{L}) := \sum_{y \in \mathcal{L}} e^{\left(-\pi\|y\|^2/2\pi\sigma^2\right)}$.

Definition 3 ([9], [11]). Given n linearly independent basis vectors $\mathcal{B} = \{b_1, b_2, \ldots, b_n\} \subset \mathbb{R}^n$ over an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\mathcal{B})$, the minimum distance of the lattice $\mathcal{L}$ in l_p norm with $p \geq 1$ is defined as,

$$\lambda^{(p)}(\mathcal{L}) := \min_{y \in \mathcal{L} \setminus \{0\}} \|y\|_p \qquad (3)$$

For a distance threshold $s > 0$, the GapSVP$_\gamma$ problem with $\gamma(n) \geq 1$ refers to the problem of determining whether $\lambda^{(p)}(\mathcal{L})$ is a YES instance or NO instance. These instances are defined as follows:

- YES instance: $\lambda^{(p)}(\mathcal{L}) \leq s$
- NO instance: $\lambda^{(p)}(\mathcal{L}) > \gamma s$

C. LWE Problem

The learning with errors problem with parameters n, q, χ namely $\mathcal{LWE}_{n,q,\chi}$, refers to solving a noisy set of linear equations over the finite field $\mathbb{F}_q$ where the noise is sampled from a distribution χ over $\mathbb{F}_q$. We now formally define two variants of $\mathcal{LWE}_{n,q,\chi}$ problem, the search $\mathcal{LWE}_{n,q,\chi}$ and the decision $\mathcal{LWE}_{n,q,\chi}$.

1) Search $\mathcal{LWE}$:

Definition 4. Let, the secret vector $\boldsymbol{s}$ and vectors $a_1, a_2, \ldots, a_m$ be sampled from uniform distribution over $\mathbb{F}_q^n$. Given, the set of samples pairs $(a_1, b_1), (a_2, b_2), \ldots, (a_m, b_m)$, the search $\mathcal{LWE}_{n,q,\chi}$ refers to the problem of finding s from the pair (a_i, b_i) for $i = 1, 2, \ldots, m$ such that $b_i \equiv \langle \boldsymbol{s}, a_i \rangle + e_i \pmod{q}$ where e_i is sampled from discrete Gaussian distribution χ over $\mathbb{F}_q$.

2) Decision $\mathcal{LWE}$:

Definition 5. Let, the secret vector $\boldsymbol{s}$ and vectors $a_1, a_2, \ldots, a_m$ be sampled from uniform distribution over $\mathbb{F}_q^n$.

Consider the set of vectors $(a_1, b_1), (a_2, b_2), \ldots, (a_m, b_m)$, where $b_i \equiv \langle \boldsymbol{s}, a_i \rangle + e_i \pmod{q}$ and e_i is sampled from discrete Gaussian distribution χ over $\mathbb{F}_q$. The decision $\mathcal{LWE}_{n,q,\chi}$ problem refers to the problem of distinguishing this m-tuple from a set of m vectors that are randomly sampled from a uniform distribution over $\mathbb{F}_q^{n+1}$.

The decision $\mathcal{LWE}_{n,q,\chi}$ is as hard as the search $\mathcal{LWE}_{n,q,\chi}$ [13], and the search $\mathcal{LWE}_{n,q,\chi}$ problem is equivalent to GapSVP$_\gamma$ problem for large $q \geq 2^{n/2}$ [11]. The distribution of the m-tuple $(a_1, b_1), (a_2, b_2), \ldots, (a_m, b_m)$ is called the $\mathcal{LWE}_{n,q,\chi}$ distribution and the assumption that the $\mathcal{LWE}_{n,q,\chi}$ is hard is referred to as the $\mathcal{LWE}_{n,q,\chi}$ assumption.

The LWE problem can be used to design a cryptosystem having multiple keys for multiple participants. It is explained in section III.

III. LWE BASED MULTI RECIPIENT CRYPTOSYSTEMS

In this section, we propose an LWE-based multi recipient encryption scheme. The proposed scheme considers a configuration with a single sender and multiple receivers. Each receiver has a secret key shared with the sender. Here, when the number of receivers is m, an m-tuple of message streams is encrypted using an m-tuple of secret keys (one corresponding to each receiver) to produce a single ciphertext. Each recipient can recover their intended message using their secret key.

We start by defining a pseudorandom map, which is the building block for the multi-recipient scheme.

Definition 6. A function $f_{s,\chi} : \mathbb{F}_q^m \to \mathbb{F}_q$ indexed by an arbitrary chosen vector $s \xleftarrow{\$} \mathbb{F}_q^m$ and a distribution χ is a function-generated map defined as

$$f_{s,\chi}(v) := (\langle \boldsymbol{s}, v \rangle + e) \pmod{q} \qquad (4)$$

where $v \xleftarrow{\$} \mathbb{F}_q^m$, $e \in \mathbb{F}_q$ is sampled from distribution χ.

Definition 7. A map $f : S \times \mathbb{F}_q^m \to \mathbb{F}_q^m$ indexed by elements of set S and distribution χ is said to be pseudorandom map (*PRM*) if the following properties hold:

1) The map f is efficiently computable.
2) For an element $s \xleftarrow{\$} S$ the output of $f(s, \bullet)$ is computationally indistinguishable from a randomly sampled element from $\mathbb{F}_q^m$. In other words, the advantage of an adversary algorithm $\mathcal{A}$ with oracle access to f, in distinguishing the output of f from a randomly sampled element of $\mathbb{F}_q^m$ is bounded by a negligible function ϵ of m.

$$Adv(\mathcal{A}) = \left| Pr\left[\mathcal{A}\left(f(s,.) \right) = 1 \right] - Pr\left[\mathcal{A}\left(U(\mathbb{F}_q^m) \right) = 1 \right] \right|$$
$$\leq \epsilon(m) \qquad (5)$$

The only difference between a *PRM* and a pseudorandom function (*PRF*) is that, in a *PRM* each input can potentially have multiple outputs.

The following theorem demonstrates how a *PRM* $f : S \times \mathbb{F}_q^m \to \mathbb{F}_q^m$ can be used recursively to construct a *PRM* $\mathcal{F} : S \times \mathbb{F}_q^m \to \mathbb{F}_q^{m \times l}$. In the theorem below, we are introducing an arbitrary matrix M which corresponds to the message in the encryption scheme described in Section III-B.

Theorem 1. *Consider a PRM $f : S \times \mathbb{F}_q^m \to \mathbb{F}_q^m$. Let $M = [m_1, m_2, \ldots, m_l] \in \mathbb{F}_q^{m \times l}$, be an arbitrary matrix. Define $\mathcal{F}_{M,S} : \mathbb{F}_q^m \to \mathbb{F}_q^{m \times l}$ as*

$$\begin{aligned} \mathcal{F}_{M,S}(s, g_0) &= (g_1, g_2, \ldots, g_l), \\ \text{and } g_i &= f(s, g_{i-1}) + m_i, \end{aligned} \quad (6)$$

where $g_0 \xleftarrow{\$} \mathbb{F}_q^m$ and s is randomly sampled from uniform distributions over S, independent of each other and the columns of M. Then $\mathcal{F}_{M,S}$ is indistinguishable from a randomly sampled map from $\mathbb{F}_q^m \to \mathbb{F}_q^{m \times l}$.

Proof. Construct a series of hybrid experiments $H_0, H_1, \ldots, H_l$ where in the experiment H_k, the vectors $(g_0, g_1, \ldots, g_k) \in \mathbb{F}_q^{m \times (k+1)}$ are randomly sampled from uniform distribution over $\mathbb{F}_q^m$ and g_i for $i = k+1, k+2, \ldots, l$ are calculated as follows:

$$g_i = f(s, g_{i-1}) + m_i \quad (7)$$

The output of H_k is $(g_1, \ldots, g_l) \in \mathbb{F}_q^{m \times l}$. Observe that the output of the experiment H_0 corresponds to the output of map $\mathcal{F}_{M,S}$ and H_l corresponds to the output of a map randomly sampled from a uniform distribution on the set of maps from $\mathbb{F}_q^m$ to $\mathbb{F}_q^{m \times l}$.

Consider a binary algorithm $\mathcal{A}$ that accepts elements of $\mathbb{F}_q^{m \times l}$ as inputs and aims to distinguish between the experiments H_0 and H_l. Let

$$\mathcal{P}_k = Pr\left[\mathcal{A}(H_k) = 1\right] \quad (8)$$

be the probability that $\mathcal{A}$ returns 1 when it takes elements generated from the experiment H_k as the input. If for any k, algorithm $\mathcal{A}$ can distinguish between samples from H_{k-1} and H_k, then $\mathcal{A}$ can be used to construct an adversary $\mathcal{A}'$, with oracle access to $f(s, \bullet)$ that can distinguish outputs of $f(s, \bullet)$ from that of a truly random map. Let the input of $\mathcal{A}'$ be (z, h) where z is randomly sampled from $U(\mathbb{F}_q^m)$ and h is either $f(s, z)$ or $f'(z)$ where f' is randomly sampled from the set of maps from $\mathbb{F}_q^m$ to $\mathbb{F}_q^m$. Generate the vectors

$$\begin{aligned} g_k &= h + m_k \\ g_{k+1} &= f(s, g_k) + m_{k+1} \\ &\vdots \\ g_l &= f(s, g_{l-1}) + m_l \end{aligned} \quad (9)$$

using oracle access to $f(s, \bullet)$. Further, randomly sample vectors $(g_1, \ldots, g_{k-2})$ from a uniform distribution on $\mathbb{F}_q^m$ and let $g_{k-1} = z$. Observe that if $h = f(s, z)$, then the distribution of the vectors $(g_1, \ldots, g_l)$ is identical to the distribution of the output of H_{k-1}. On the other hand, if $h = f'(z)$, then the distribution of this set of vectors is identical to that of the output of H_k. Thus, if $\mathcal{A}'$ can parse the vectors $(g_1, \ldots, g_l)$ to $\mathcal{A}$ which can distinguish between the output distributions of H_k and H_{k-1} with a significant advantage then, $\mathcal{A}'$ can distinguish between $f(s, \bullet)$ and a randomly sampled map. This contradicts the pseudorandomness of $f(s, \bullet)$. Hence, $|\mathcal{P}_k - \mathcal{P}_{k-1}| < \epsilon(m)$ where ϵ is a function that is negligible in m.

Now, the advantage of $\mathcal{A}$ in distinguishing between outputs of H_0 and H_l is given by

$$\begin{aligned} Adv(\mathcal{A}) &= |\mathcal{P}_0 - \mathcal{P}_l| \\ &= |\mathcal{P}_0 - \mathcal{P}_1 + \mathcal{P}_1 - \mathcal{P}_2 + \ldots + \mathcal{P}_{l-1} - \mathcal{P}_l| \\ &\leq |\mathcal{P}_0 - \mathcal{P}_1| + |\mathcal{P}_1 - \mathcal{P}_2| + \ldots + |\mathcal{P}_{l-1} - \mathcal{P}_l| \\ &\leq l\epsilon(m) \end{aligned} \quad (10)$$

Hence, $Adv(\mathcal{A})$ is negligible in m. □

The following subsection explains the construction of a pseudorandom map based on the hardness of the LWE problem.

A. LWE-based Pseudorandom Map (LWE-PRM)

In this section, we use the LWE problem for the construction of a *PRM*. We refer to such a PRM as an *LWE-PRM*. Here, multiple secret vectors $s_k \in \mathbb{F}_q^m$ for $k = 1, 2, \ldots, m$ are sampled randomly and a vector $v \xleftarrow{\$} \mathbb{F}_q^m$ randomly sampled such that the addition of noise $e \in \mathbb{F}_q$ sampled from distribution χ with the inner product of secret vector s_k and the vector v gives m elements in $\mathbb{F}_q$.

The following theorem is a special case of Lemma 6.2 from Peikert et al. [15], which is instrumental in the development of our results. This theorem proves the indistinguishability property of the *LWE-PRM* from a randomly sampled map from $\mathbb{F}_q^m \to \mathbb{F}_q^m$.

Lemma 1. *Consider $S = [s_1, s_2, \ldots, s_m]^T \in \mathbb{F}_q^{m \times m}$ with $s_k \xleftarrow{\$} \mathbb{F}_q^m$ for $k = 1, 2, \ldots, m$ to be a random secret vector matrix and $v \xleftarrow{\$} \mathbb{F}_q^m$ be a randomly chosen vector. Define the map $f_\chi(\bullet, v)$ such that*

$$f_\chi(S, v) := (S \times v + E) \pmod{q} \quad (11)$$

$$= \begin{bmatrix} \langle s_1, v \rangle + e_1 \\ \langle s_2, v \rangle + e_2 \\ \langle s_3, v \rangle + e_3 \\ \vdots \\ \langle s_m, v \rangle + e_m \end{bmatrix} \pmod{q}$$

with error vector $E = [e_1, e_2, \ldots, e_m]^T \in \mathbb{F}_q^m$ and $e_k \in \mathbb{F}_q$ sampled from distribution χ for $k = 1, 2, \ldots, m$. Then, under the $\mathcal{LWE}_{m,q,\chi}$ assumption, $f_\chi(\bullet, v)$ is a pseudorandom map.

Proof. See in the Appendix. □

For the sake of completeness, a brief proof of Lemma (1) is given in the appendix.

We now proceed to describe the proposed multi-recipient encryption scheme based on the pseudorandom map mentioned in Lemma (1).

B. Multi-Key Multi-Recipient (MKMR) Encryption Scheme

The multi-recipient encryption scheme described in this subsection is a symmetric encryption scheme involving multiple messages encrypted using independent secret keys to generate a single ciphertext stream. This stream is then decrypted by the recipients using their respective secret keys to recover the

message intended for them. Let the number of recipients be m. Corresponding to each recipient there is a unique secret key $s_k \xleftarrow{\$} \mathbb{F}_q^m$ for $k = 1, 2, \ldots, m$. The proposed encryption scheme consists of the following steps:

- **Setup(λ):** This algorithm takes the security parameter λ as input and returns an integer m, a prime q and a discrete Gaussian distribution χ over $\mathbb{F}_q$.
- **KeyGen(m, q):** The algorithm *KeyGen(.)* takes m and q generated by **Setup$(\bullet)$** and outputs m secret keys $s_1, s_2, \ldots, s_m$ sampled from a uniform distribution over $\mathbb{F}_q^m$.
- **Encrypt** (denoted as $\boldsymbol{Enc(s_1, s_2, \ldots, s_m, \mathcal{M})}$): Consider a m recipient encryption scheme where each recipient has a message stream of length l. The message stream corresponding to the jth recipient is $\begin{bmatrix} m_{j1} & m_{j2} & \ldots & m_{jl} \end{bmatrix} \in \mathbb{F}_q^l$. Now stacking these message streams together gives a message matrix $\mathcal{M} \in \mathbb{F}_q^{m \times l}$ which is represented as

$$\mathcal{M} = \begin{bmatrix} m_{11} & m_{12} & \ldots & m_{1l} \\ m_{21} & m_{22} & \ldots & m_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ m_{m1} & m_{m2} & \ldots & m_{ml} \end{bmatrix} \quad (12)$$

Let m_i be the ith column of the matrix $\mathcal{M}$. The ciphertext is a sequence of vectors $v_0, v_1, \ldots, v_l$ in $\mathbb{F}_q^m$. The vector v_0 is the initialization vector randomly sampled from a uniform distribution over $\mathbb{F}_q^m$. The remaining vectors are recursively generated as follows,

$$v_i = m_i + f_\chi (S, v_{i-1}) \pmod{q}$$
$$= m_i + \begin{bmatrix} \langle s_1, v_{i-1} \rangle + e_1 \\ \langle s_2, v_{i-1} \rangle + e_2 \\ \langle s_3, v_{i-1} \rangle + e_3 \\ \vdots \\ \langle s_m, v_{i-1} \rangle + e_m \end{bmatrix} \pmod{q} \quad (13)$$

where $E_i = [e_1, e_2, \ldots, e_m]^T \in \mathbb{F}_q^m$ is randomly sampled from the distribution χ. The encryption procedure is described in Algorithm (1).

Algorithm 1 *Enc$(\bullet)$*

1: **Input:** $s_1, s_2, \ldots, s_m, \mathcal{M} = \begin{bmatrix} m_1 & m_2 & \ldots & m_l \end{bmatrix}$
2: **Output:** $\mathcal{C}$
3: $I_v \xleftarrow{\$} \mathbb{F}_q^m$
4: Set $v_0 = I_v$
5: Set $i = 1$
6: **while** $i < l$ **do**
7: $\quad E_i \xleftarrow{\$} \chi^m$
8: $\quad v_i = m_i + \begin{bmatrix} \langle s_1, v_{i-1} \rangle + e_1 \\ \langle s_2, v_{i-1} \rangle + e_2 \\ \langle s_3, v_{i-1} \rangle + e_3 \\ \vdots \\ \langle s_m, v_{i-1} \rangle + e_m \end{bmatrix} \pmod{q}$
9: $\quad$ Update $i = i + 1$
10: **end while**
11: $\mathcal{C} = \begin{bmatrix} v_0 & v_1 & \ldots & v_l \end{bmatrix}$
12: **return** $\mathcal{C}$

- **Decrypt** (denoted as $\boldsymbol{Dec(s_j, \mathcal{C})}$): The decryption process is the reverse of encryption. Given the secret key s_j, the jth receiver recursively recovers its message stream $[m_{j1}, m_{j2}, \ldots, m_{jl}]$ as follows:

$$m_{ji} = v_{ji} - \left[\langle s_j, v_{i-1} \rangle \right] \pmod{q}, \text{ for } 1 \le i < l \quad (14)$$

where v_{ji} is the jth entry of the vector v_i. It can be easily verified that the recovered message is the same as the original message with some added noise. The decryption process for the jth receiver is given in Algorithm (2).

Algorithm 2 *Dec$(\bullet)$*

1: **Input:** $s_j, \mathcal{C} = \begin{bmatrix} v_0 & v_1 & \ldots & v_l \end{bmatrix}$
2: **Output:** $\mathcal{M}_j = \begin{bmatrix} m_{j1} & m_{j2} & \ldots & m_{jl} \end{bmatrix}$
3: Set $i = 1$
4: **while** $i < l$ **do**
5: $\quad m_{ji} = v_{ji} - \left[\langle s_j, v_{i-1} \rangle \right] \pmod{q}$
6: $\quad$ Update $i = i + 1$
7: **end while**
8: $\mathcal{M}_j = \begin{bmatrix} m_{j1} & m_{j2} & \ldots & m_{jl} \end{bmatrix}$
9: **return** $\mathcal{M}_j$

We now proceed to analyze the security of the proposed scheme.

C. Security

We start by defining indistinguishability under chosen plaintext attack (IND-CPA) security for a symmetric multirecipient scheme . The IND-CPA game for a symmetric multirecipient scheme which is played between an adversary and a challenger has the following stages

1) *Initialize*: The challenger randomly samples a set of m-keys from $\mathbb{F}_q^m$. Further, she also randomly samples a bit $b \in \{0, 1\}$.
2) *Querying the challenger (encryption oracle)*: The adversary chooses a set of p m-tuples of messages $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_p)$ and sends to the challenger. The challenger acts as an encryption oracle, encrypts these message tuples and sends it back to the adversary. Let the corresponding ciphertexts be $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p$.
3) *Challenge*: The adversary chooses two m-tuples of messages $\mathcal{M}_{01}$ and $\mathcal{M}_{11}$ which are not identical to each other and to any of the message tuples previously queried and sends them to the challenger. Based on the value of b, the challenger encrypts $\mathcal{M}_{b1}$ and sends it to the adversary.
4) *Guessing b*: The adversary attempts to guess the value of b using the information at her disposal. She wins the game on guessing b correctly.

The IND-CPA security of the proposed scheme follows as a direct consequence of the following two results.

Lemma 2. *Consider a set of p m-tuples $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_p)$ of message streams of length l, where p is a polynomial in m. Let $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p)$ be the corresponding ciphertexts obtained by encrypting the message streams using Algorithm (1). Then, under the $\mathcal{LWE}_{m,q,\chi}$ assumption, $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p)$ is*

indistinguishable from a set of p elements each independently randomly sampled from a uniform distribution over $\mathbb{F}_q^{m \times (l+1)}$.

Proof. Consider an algorithm $\mathcal{A}$ that aims to distinguish between $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p)$ and from a set of p elements each independently randomly sampled from a uniform distribution over $\mathbb{F}_q^{m \times (l+1)}$. Let $H_0, H_1, \ldots, H_p$ be a set of $p+1$ hybrid experiments that returns p elements of $\mathbb{F}_q^{m \times (l+1)}$. In particular, for $0 \leq i \leq p$, the output of H_i is a p-tuple, the first i elements of which are independently randomly sampled from $U(\mathbb{F}_q^{m \times (l+1)})$ and the remaining elements are $(\mathcal{C}_{i+1}, \mathcal{C}_{i+2}, \ldots, \mathcal{C}_p)$. Note that H_0 returns the ciphertext $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p)$ and H_p returns p elements each independently randomly sampled from a uniform distribution over $\mathbb{F}_q^{m \times (l+1)}$.

Let $\mathcal{P}_i$ be the probability that $\mathcal{A}$ returns 1 when its input is the output of H_i. We claim that, for any $1 \leq k \leq p$, $|\mathcal{P}_p - \mathcal{P}_{p-i}| \leq il\epsilon(m)$. We prove this using induction.

Base case: Observe that, $|\mathcal{P}_p - \mathcal{P}_0|$ is the advantage of the Algorithm $\mathcal{A}$. Now, as a consequence of Theorem (1) and Lemma (1), $|\mathcal{P}_p - \mathcal{P}_{p-1}|$ is less than $l\epsilon(m)$, where $\epsilon(m)$ is the maximum advantage of an adversary against the pseudo-random map $f_\chi(S, \bullet)$.

Induction step: Assume that the claim is true for $i = k$. We have to prove that $|\mathcal{P}_p - \mathcal{P}_{p-(k+1)}| \leq (k+1)l\epsilon(m)$.

Observe that, distinguishing between the outputs H_{p-k} and $H_{p-(k+1)}$ is equivalent to distinguishing between $C_{p-(k+1)}$ and a randomly sampled element of $\mathbb{F}_q^{m \times (l+1)}$. Therefore, $|\mathcal{P}_{p-(k+1)} - \mathcal{P}_{p-k}| \leq l\epsilon(m)$. Now,

$$
\begin{aligned}
|\mathcal{P}_p - \mathcal{P}_{p-(k+1)}| &\leq |\mathcal{P}_p - \mathcal{P}_{p-k} + \mathcal{P}_{p-k} - \mathcal{P}_{p-(k+1)}| \\
&\leq |\mathcal{P}_p - \mathcal{P}_{p-k}| + |\mathcal{P}_{p-k} - \mathcal{P}_{p-(k+1)}| \\
&\leq kl\epsilon(m) + l\epsilon(m) = (k+1)l\epsilon(m)
\end{aligned}
$$

Hence, the claim is proved.

Therefore $|\mathcal{P}_p - \mathcal{P}_0| \leq pl\epsilon(m)$. As p is polynomial in m and ϵ is a negligible function of m, $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p)$ is indistinguishable from a set of p elements each independently randomly sampled from a uniform distribution over $\mathbb{F}_q^{m \times (l+1)}$. $\square$

We now prove that the encryptions of two distinct m-tuples of message streams are indistinguishable.

Lemma 3. *Consider two m-tuples of messages $\mathcal{M}_{01}$ and $\mathcal{M}_{02}$ wherein each message is of length l where l is bounded by a polynomial in m. Let $\mathcal{C}_{01} = [v_0, v_1, v_2, \ldots, v_l] \in \mathbb{F}_q^{m \times (l+1)}$ and $\mathcal{C}_{02} = [v'_o, v'_1, v'_2, \ldots, v'_l] \in \mathbb{F}_q^{m \times (l+1)}$ be the ciphertexts obtained by respectively encrypting $\mathcal{M}_{01}$ and $\mathcal{M}_{02}$, using Algorithm 1. Then, under the $\mathcal{LWE}_{m,q,\chi}$ assumption, $\mathcal{C}_{01}$ and $\mathcal{C}_{02}$ are indistinguishable from each other and a randomly sampled element of $\mathbb{F}_q^{m \times (l+1)}$.*

Proof. Consider an algorithm $\mathcal{A}$ with a binary output that takes inputs from $\mathbb{F}_q^{m \times (l+1)}$.

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be the probabilities of $\mathcal{A}$ returning 1 for inputs $\mathcal{C}_{01}$ and $\mathcal{C}_{02}$ respectively.

$$
\begin{aligned}
\mathcal{P}_1 &= Pr\left[\mathcal{A}\left(\mathcal{C}_{01}\right) = 1\right] \\
\mathcal{P}_2 &= Pr\left[\mathcal{A}\left(\mathcal{C}_{02}\right) = 1\right]
\end{aligned}
$$

Let $\mathcal{P}_0$ be the probability of $\mathcal{A}$ returning 1 when the input is randomly sampled from the distribution $U(\mathbb{F}_q^{m \times l})$.

$$
\mathcal{P}_0 = Pr\left[\mathcal{A}\left(\mathcal{C}_0\right) = 1\right] \tag{15}
$$

From Theorem 1 and Lemma 1, $|\mathcal{P}_1 - \mathcal{P}_0|$ and $|\mathcal{P}_2 - \mathcal{P}_0|$ are less than $l\epsilon(m)$ where $\epsilon(m)$ is a negligible function of the security parameter. Let their values be ϵ_1 and ϵ_2, respectively.

Now, the advantage of $\mathcal{A}$ in distinguishing between $\mathcal{C}_{01}$ and $\mathcal{C}_{02}$ is given by

$$
\begin{aligned}
Adv(\mathcal{A}) &= |\mathcal{P}_1 - \mathcal{P}_2| \\
&= |\mathcal{P}_1 - \mathcal{P}_0 + \mathcal{P}_0 - \mathcal{P}_2| \\
&\leq |\mathcal{P}_1 - \mathcal{P}_0| + |\mathcal{P}_0 - \mathcal{P}_2| \\
&\leq |\mathcal{P}_1 - \mathcal{P}_0| + |\mathcal{P}_2 - \mathcal{P}_0| \\
&\leq l\epsilon(m) + l\epsilon(m) = 2l\epsilon(m)
\end{aligned} \tag{16}
$$

Hence, $Adv(\mathcal{A})$ is negligible. Hence, ciphertext streams $\mathcal{C}_{01}$ and $\mathcal{C}_{02}$ are indistinguishable from each other. $\square$

Using the preceding couple of lemmas, the following theorem establishes the IND-CPA security of the proposed scheme.

Theorem 2. *Consider a set of p m-tuples $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_p)$ of message streams of length l, where p is a polynomial in m. Let $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p)$ be the corresponding ciphertexts obtained by encrypting the message streams with an m-tuple secret key S using Algorithm (1). Assume two m-tuples of messages $\mathcal{M}_{01}$ and $\mathcal{M}_{02}$ that are distinct from each other and each of the message streams $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_p)$. Further, let $\mathcal{C}_{01}$ and $\mathcal{C}_{02}$ be the ciphertexts of $\mathcal{M}_{01}$ and $\mathcal{M}_{02}$, respectively, obtained using the secret key S in Algorithm (1). Then, under the $\mathcal{LWE}_{m,q,\chi}$ assumption, no algorithm with access to the pairs $(\mathcal{M}_i, \mathcal{C}_i)$ for $1 \leq i \leq p$ can distinguish between $\mathcal{C}_{01}$ and $\mathcal{C}_{02}$ with any significant advantage i.e., the encryption scheme is IND-CPA secure.*

Proof. Let Δ be the advantage of an algorithm $\mathcal{A}$, with access to the pairs $(\mathcal{M}_i, \mathcal{C}_i)$ in distinguishing between $\mathcal{C}_{01}$ and $\mathcal{C}_{02}$. To the contrary, assume that Δ is not negligible in m. Now, if the $\mathcal{C}_i$s that are fed to the algorithm $\mathcal{A}$ are replaced by randomly sampled elements of $\mathbb{F}_q^{m \times (l+1)}$, then, by Lemma (3), the advantage of $\mathcal{A}$ is less than $2l\epsilon(m)$ where ϵ is a negligible function of m.

Now, the algorithm $\mathcal{A}$ can be used to create an algorithm $\mathcal{A}'$ that can distinguish between the p-tuple $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p$ from a set of p randomly sampled elements of $\mathbb{F}_q^{m \times (l+1)}$ with significant advantage. Given access to both the challenger and the adversary algorithms in the IND-CPA game and a set of p message-ciphertext pairs $(\mathcal{M}_i, \mathcal{C}_i)$ $(1 \leq i \leq p)$, $\mathcal{A}'$ can instruct the adversary $\mathcal{A}$ to generate a pair of messages $\mathcal{M}_{01}, \mathcal{M}_{02}$ and the challenger to generate a challenge for the adversary as in the IND-CPA game. The algorithm $\mathcal{A}'$ returns 1 if $\mathcal{A}$ guesses the challenge message correctly. Clearly, the advantage of $\mathcal{A}'$ is $\Delta - 2l\epsilon(m)$ which is not negligible. This contradicts Lemma (2). Hence, Δ is a negligible function of m and the proposed scheme is IND-CPA secure. $\square$

The above notion of IND-CPA security ensures the security of the encrypted data against an adversary who does not

have access to the secret keys. However, in a multi-recipient scheme, it is important that any receiver or set of receivers should not be able to extract information about message streams that are not intended for them. We now extend the idea to IND-CPA security to the case when the adversary knows some of the keys. Assume that the adversary knows k of the keys. Without loss of generality, we can assume these to be the last k keys. We now proceed to prove that if, in addition to the k keys, the adversary also knows the last k entries of the other keys, she can still not distinguish between the first $m - k$ rows of encryptions of two distinct messages.

Theorem 3. *Consider a set of p m-tuples $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_p)$ of message streams of length l, where p is a polynomial in m. Let $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_p)$ be the corresponding ciphertexts obtained by encrypting the message streams with a secret key matrix $S = [s_1, s_2, \ldots, s_m]^T$ using Algorithm (1). (The rows of S constitute the m secret keys). Let $\mathcal{M} = (m_1, m_2, \ldots, m_l)$ be an arbitrary message that is distinct from $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_p)$ and let $\mathcal{C}$ be the corresponding ciphertext obtained using S in Algorithm (1). Consider an adversary $\mathcal{A}$ who has access to the following:*

(i) *pairs $(\mathcal{M}_i, \mathcal{C}_i)$ for $1 \leq i \leq p$.*

(ii) *The last k secret keys from S, and*

(iii) *The last k entries of the remaining $m - k$ secret keys in S.*

(iv) *An oracle that evaluates the following map f from $\mathbb{F}_q^{m-k}$ to $\mathbb{F}_q^{m-k}$.*

$$f(v) = S_1 v + \epsilon,$$

where ϵ is randomly sampled from χ^{m-k} and S_1 is the matrix consisting of the first $m - k$ entries of the first $m - k$ rows of S i.e. the top left $(m - k) \times (m - k)$ submatrix of S.

Then, under the $\mathcal{LWE}_{(m-k),q,\chi}$ assumption, the adversary cannot efficiently distinguish the first $m - k$ rows of $\mathcal{C}$ from a matrix randomly sampled from a uniform distribution over $\mathbb{F}_q^{(m-k)\times(l+1)}$.

Proof. We partition $S \in \mathbb{F}_q^{m \times m}$ as $S = \left[\begin{array}{c|c} S_1 & S_2 \\ \hline S_3 & S_4 \end{array} \right]$, where $S_1 \in \mathbb{F}_q^{(m-k)\times(m-k)}$. Therefore, $\mathcal{A}$ has access to $S_2, S_3,$ and S_4. We now prove that even with access to S_2, S_3 and S_4, the first $m - k$ rows of $\mathcal{C}$ remain indistinguishable from a matrix randomly sampled from a uniform distribution over $\mathbb{F}_q^{(m-k)\times(l+1)}$.

Consider $l + 1$ hybrid experiments H_i for $1 \leq i \leq l + 1$. We define the output of the experiments next. Corresponding to an experiment H_i, partition $\mathcal{C}$ as follows:

$$\mathcal{C} = \left[\begin{array}{c|c} \mathcal{C}_{1i} & \mathcal{C}_2 \\ \hline \mathcal{C}_{3i} & \mathcal{C}_{4i} \end{array} \right] \in \mathbb{F}_q^{m\times(l+1)}, \text{ where } \mathcal{C}_{1i} \in \mathbb{F}_q^{(m-k)\times i}$$

(17)

We define a new matrix $\widehat{\mathcal{C}}_i$ using the matrix in eq. (17) as follows

$$\widehat{\mathcal{C}}_i := \left[\begin{array}{c|c} \mathcal{C}_{1i} & \mathcal{U}_i \\ \hline \mathcal{C}_{3i} & \mathcal{C}_{4i} \end{array} \right] \in \mathbb{F}_q^{m\times(l+1)}, \text{ where } \mathcal{C}_{1i} \in \mathbb{F}_q^{(m-k)\times i}$$

$\mathcal{U}_i$ are randomly sampled elements from $\mathbb{F}_q^{(m-k)\times(l+1-i)}$. The output of H_i is the first $m - k$ rows of $\widehat{\mathcal{C}}_i$, i.e., $\begin{bmatrix} \mathcal{C}_{1i} & \mathcal{U}_i \end{bmatrix}$. Hence, we need to prove that the output of the experiments $H_1, \cdots, H_{l+1}$ are indistingushable from a matrix randomly sampled from a uniform distribution over $\mathbb{F}_q^{(m-k)\times(l+1)}$. We prove this using induction.

Base case: Note that the output of H_1 experiment are the first $m - k$ rows of $\widehat{\mathcal{C}}_1 = \begin{bmatrix} v_0 & \mathcal{U}_1 \end{bmatrix}$. Since v_0 is randomly sampled in the encryption algorithm, the output of H_1 is identical to a randomly sampled element from $U(\mathbb{F}_q^{(m-k)\times(l+1)})$.

Induction step: Assume that the outputs of the experiments $H_1, H_2, \ldots, H_t$ are indistinguishable from each other and from randomly sampled elements of $\mathbb{F}_q^{(m-k)\times(l+1)}$. We now proceed to prove that this also holds true for the output of H_{t+1}.

Let P_i be the probability that $\mathcal{A}$ outputs 1 when its input is the output of H_i, for $1 \leq i \leq l$. Let

$$\widehat{\mathcal{C}}_{t-1} = \left[\begin{array}{c|c} \mathcal{C}_{1(t-1)} & \mathcal{U}_{t-1} \\ \hline \mathcal{C}_{3(t-1)} & \mathcal{C}_{4(t-1)} \end{array} \right] = \left[\begin{array}{ccc|cccc} \bar{v}_0 & \cdots \bar{v}_{t-2} & \bar{w}_{t-1} & \bar{w}_t & \cdots & \bar{w}_l \\ \hline \bar{\bar{v}}_0 & \cdots \bar{\bar{v}}_{t-2} & \bar{\bar{v}}_{t-1} & \bar{\bar{v}}_t & \cdots & \bar{\bar{v}}_l \end{array} \right]$$

Replace $\bar{w}_t$ with $\tilde{w}_t = \bar{m}_t + f(\bar{w}_{t-1}) + S_2 \bar{\bar{v}}_{t-1} = \bar{m}_t + S_1 \bar{w}_{t-1} + S_2 \bar{\bar{v}}_{t-1} + e$ where e is randomly sampled from χ^{m-k} and $\bar{m}_t$ consists of the first $m - k$ entries of m_t. Define

$$\mathfrak{K}_{t-1} := \left[\begin{array}{ccc|cccc} \bar{v}_0 & \cdots \bar{v}_{t-2} & \bar{w}_{t-1} & \tilde{w}_t & \cdots & \bar{w}_l \\ \hline \bar{\bar{v}}_0 & \cdots \bar{\bar{v}}_{t-2} & \bar{\bar{v}}_{t-1} & \bar{\bar{v}}_t & \cdots & \bar{\bar{v}}_l \end{array} \right]$$

Let $\tilde{\mathcal{P}}_{t-1}$ be the probability that $\mathcal{A}$ returns 1 when the input is the first $m - k$ rows of $\mathfrak{K}_{t-1}$. Now, as S_2 is known to the adversary, distinguishing between $\mathfrak{K}_{t-1}$ and the output of H_{t-1} is equivalent to solving an instance of the $\mathcal{LWE}_{(m-k),q,\chi}$ problem. Therefore $\epsilon_1 = |\tilde{\mathcal{P}}_{t-1} - \mathcal{P}_{t-1}|$ is a negligible function of $m - k$.

Similarly, let

$$\widehat{\mathcal{C}}_t = \left[\begin{array}{c|c} \mathcal{C}_{1t} & \mathcal{U}_t \\ \hline \mathcal{C}_{3t} & \mathcal{C}_{4t} \end{array} \right] = \left[\begin{array}{ccc|cccc} \bar{v}_0 & \cdots \bar{v}_{t-1} & \bar{w}'_t & \bar{w}'_{t+1} & \cdots & \bar{w}'_l \\ \hline \bar{\bar{v}}_0 & \cdots \bar{\bar{v}}_{t-1} & \bar{\bar{v}}_t & \bar{\bar{v}}_{t+1} & \cdots & \bar{\bar{v}}_l \end{array} \right]$$

Replace $\bar{w}'_t$ by $\tilde{w}'_t = \bar{m}_t + f(\bar{v}_{t-1}) + S_2 \bar{\bar{v}}_{t-1} = \bar{m}_t + S_1 \bar{v}_{t-1} + S_2 \bar{\bar{v}}_{t-1} + e'$ where e' is randomly sampled from χ^{m-k}. Define

$$\mathfrak{K}_t := \left[\begin{array}{ccc|cccc} \bar{v}_0 & \cdots \bar{v}_{t-1} & \tilde{w}'_t & \bar{w}'_{t+1} & \cdots & \bar{w}'_l \\ \hline \bar{\bar{v}}_0 & \cdots \bar{\bar{v}}_{t-1} & \bar{\bar{v}}_t & \bar{\bar{v}}_{t+1} & \cdots & \bar{\bar{v}}_l \end{array} \right]$$

Let $\tilde{\mathcal{P}}_t$ be the probability that $\mathcal{A}$ returns 1 when the input is the first $m - k$ rows of $\mathfrak{K}_t$. Observe that the adversary can access the oracle to generate $\mathfrak{K}_{t-1}$ and $\mathfrak{K}_t$ from $\widehat{\mathcal{C}}_{t-1}$ and $\widehat{\mathcal{C}}_t$ respectively. Therefore, if the adversary can distinguish between $\mathfrak{K}_{t-1}$ and $\mathfrak{K}_t$, then he can effectively distinguish between $\widehat{\mathcal{C}}_{t-1}$ and $\widehat{\mathcal{C}}_t$. This contradicts the induction assumption. Therefore $|\tilde{\mathcal{P}}_{t-1} - \tilde{\mathcal{P}}_t| = \epsilon_2$ is negligible. Now,

$$\begin{aligned} |\tilde{\mathcal{P}}_t - \mathcal{P}_{t-1}| &= |\tilde{\mathcal{P}}_t - \tilde{\mathcal{P}}_{t-1} + \tilde{\mathcal{P}}_{t-1} - \mathcal{P}_{t-1}| \\ &\leq |\tilde{\mathcal{P}}_t - \tilde{\mathcal{P}}_{t-1}| + |\tilde{\mathcal{P}}_{t-1} - \mathcal{P}_{t-1}| \\ &= \epsilon_1 + \epsilon_2. \end{aligned}$$

Hence, $|\tilde{\mathcal{P}}_t - \mathcal{P}_{t-1}|$ is a negligible function of $m - k$.

Observe that the distribution of $\mathfrak{K}_t$ is identical to that of $\widehat{\mathcal{C}}_{t+1}$. Therefore, $\tilde{\mathcal{P}}_t = \mathcal{P}_{t+1}$. Hence, $|\mathcal{P}_{t+1} - \mathcal{P}_{t-1}|$ is a negligible function of $m - k$. Hence the output of H_{t+1} is

indistinguishable from that of H_{t-1} and therefore from the outputs of $H_1, H_2, \ldots, H_t$.

Hence, by induction, the outputs of H_{l+1} and H_1 are indistinguishable from each other and a randomly sampled element of $\mathbb{F}_q^{(m-k)\times(l+1)}$. $\qquad\square$

The following subsection discusses the choice of parameters based on the desired level of security.

D. Choice of Parameters

The work of Biasioli et al. [16], provides a framework for estimating the desired security parameter λ while choosing dimension m in the LWE problem. For different choices of λ, different values of m are chosen. From [16, Section 6], typically for a 128-bit security level, i.e. $\lambda = 128$, the LWE dimension is chosen to be $m(\lambda) = 1024$, and the value of parameter q is chosen such that $log\,q = 20 - 41$.

E. Example

We now demonstrate how the proposed algorithm can be used to encrypt images. The length of the secret vectors is 1024. The value of q is chosen as $2^{31} - 1$. As this number is a Mersenne prime, the $mod\,q$ equivalent of any integer can be found very efficiently.

As the proposed algorithm operates over the field $\mathbb{F}_q$, the plain-text images are first converted to a string of elements in $\mathbb{F}_q$ as follows.

Generating an $\mathbb{F}_q$ *string :* Consider a gray-scale image of size $(r \times c)$ (having r rows of c pixels each) where each pixel is encoded as an 8 bit word. To encrypt the image, we consider a window of $t = \frac{\lfloor log_2 q \rfloor}{8}$ consecutive pixels on the same row. Each window contains less than $log_2 q$ bits and the corresponding integer value can be considered as an element of $\mathbb{F}_q$. The window traverses each row of the image from left to right, shifting one pixel at a time, and then proceeds to the next row. For each row, the first window position contains the first t pixels of that row (starting from the left). As the window approaches the right end of a row, it wraps around the first few pixels from the left. For example, the last window position in any row contains the rightmost pixel of that row and the first $t - 1$ pixels of that row. Thus, each row has y window positions and each pixel is contained in t of them. The total number of window positions is the same as the number of pixels in an image i.e., (rc).

An MKMR Example: To implement the MKMR scheme on images with the chosen parameters, we need a set of 1024 images. As it is impossible to demonstrate the results of such encryption in this article, we have considered a set of 4 gray-scale images shown in Fig. (2). These images are converted to 4 streams over $\mathbb{F}_q$ as described above. The other messages are replaced by random strings. The time taken for the encryption and decryption processes is therefore equal to the time needed for encrypting and decrypting 1024 images. Each image is consists of 512×512 pixels. Thus the total size of data encrypted in the process is approximately 260 MB. The corresponding secret vectors are randomly sampled from
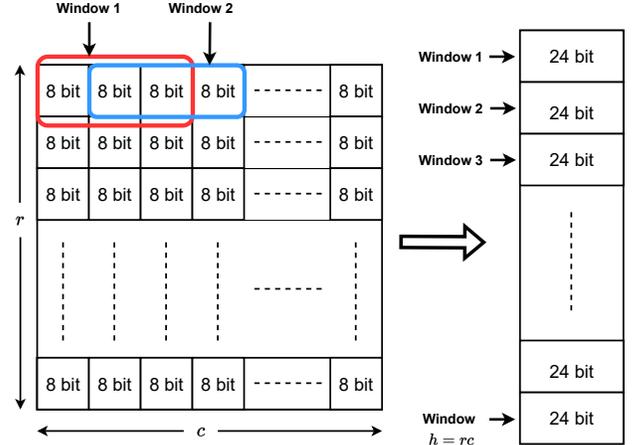

Fig. 1. A gray-scale image of size $(r \times c)$ (on the left) transformed to a message stream of length h (on the right)

a uniform distribution over $\mathbb{F}_q^m$. The window size in this case is taken as 3. Thus each window has 24 bits and is stored as a 32-bit signed integer. During decryption, we first recover the sequence of windows. Each pixel can be recovered from 3 windows. We determine the value of the pixel by considering the window where it occurs in the second position. This is because the central pixel in any window is less effected by noise. The plain-text images, encrypted images and decrypted images are shown in Fig. (2), (3) and (4) respectively. The total time taken for the encryption process (not considering the time taken to convert the images into message streams) is 4 seconds on a workstation with an INTEL i5, 2.6 GHz processor, 16 GB RAM, and an Windows-11 operating system.

IV. Conclusion

This paper presents a scheme for lattice-based multi-recipient symmetric key cryptography. The proposed scheme considers the case when a single sender communicates with multiple receivers through a single ciphertext. The proposed method aims to achieve high speed encryption while allowing for some addition of noise in the recovered message. The encryption and decryption speeds of these implementations are promising and it will be interesting to explore hardware implementations for higher speeds and efficiency.

Appendix
Proof of Lemma 1

Proof. Construct a series of hybrid experiments $H_0, H_1, \ldots, H_m$ where in the experiment H_k, the elements $(v_1, v_2, \ldots, v_k)$ are obtained using equation (11) where the error terms $e_1, e_2, \ldots, e_k$ are randomly sampled from uniform distribution over $\mathbb{F}_q$ and v_i for $i = k+1, k+2, \ldots, m$ are calculated using equation (11) where the error terms $e_{k+1}, e_{k+2}, \ldots, e_m$ are sampled from distribution χ.

The output of H_k is $(v_1, v_2, \ldots, v_m) \in \mathbb{F}_q^m$. Observe that the experiment H_0 corresponds to the output $(v_1, v_2, \ldots, v_m)$ where the error terms are sampled from distribution χ and
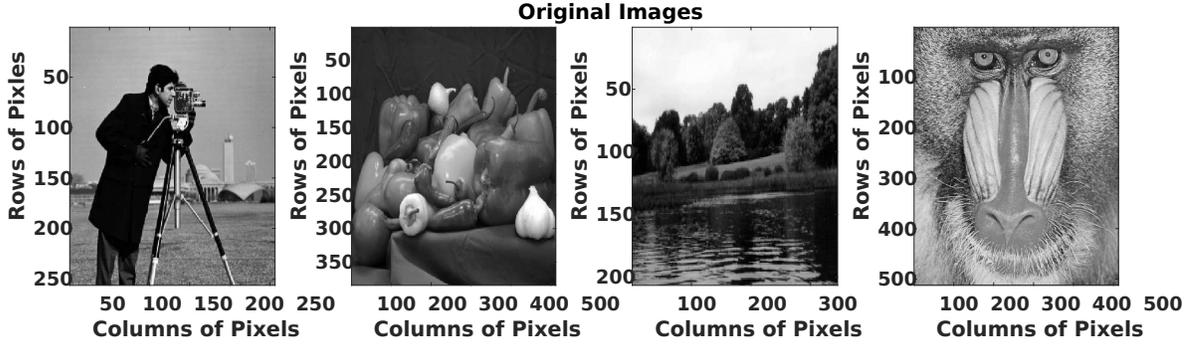
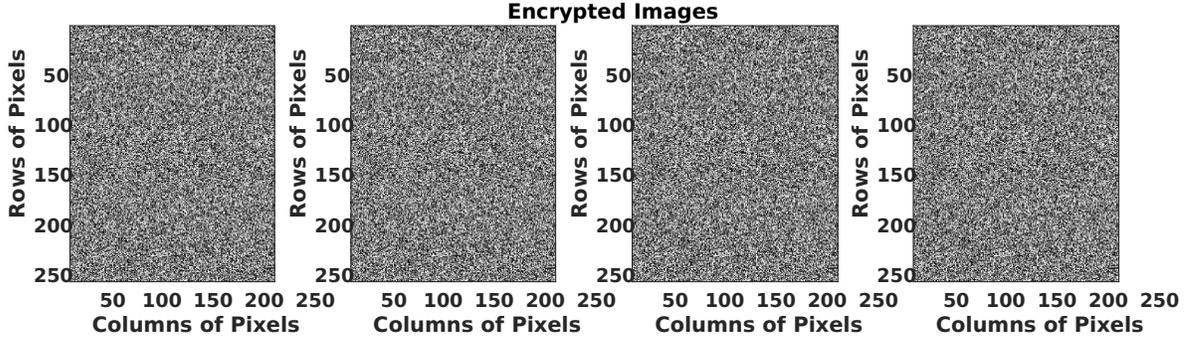Fig. 2. Simulation plot of Original Images

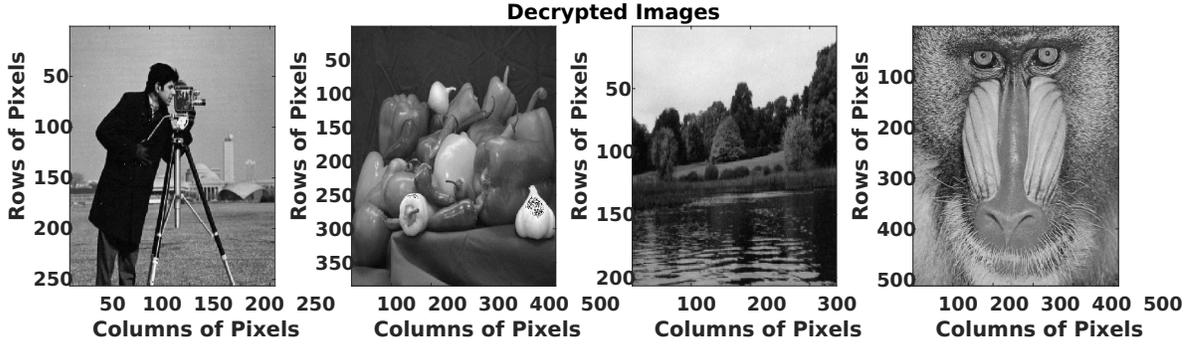Fig. 3. Simulation plot of Encrypted Images

Fig. 4. Simulation plot of Decrypted Images

H_m corresponds to the output $(v_1, v_2, \ldots, v_m)$ where the error terms are randomly sampled from uniform distribution.

Consider a binary algorithm $\mathcal{A}$ that accepts elements from $\mathbb{F}_q^m$ and aims to distinguish between experiments H_0 and H_m. Let

$$\mathcal{P}_k = Pr\left[\mathcal{A}(H_k) = 1\right] \tag{18}$$

be the probability that $\mathcal{A}$ returns 1 when it takes elements generated from the experiment H_k as the input. If for any k, algorithm $\mathcal{A}$ can distinguish between samples from H_{k-1} and H_k, then $\mathcal{A}$ can be used to construct an adversary $\mathcal{A}'$, with oracle access to $f_\chi(s, \bullet)$ that can distinguish outputs of $f_\chi(s, \bullet)$ from that of a truly random map. But under the $\mathcal{LWE}_{m,q,\chi}$ assumption, the advantage of $\mathcal{A}'$ i.e. $Adv(\mathcal{A}')$ is negligible function of m. So, $Adv(\mathcal{A})$ is also negligible function of m. Hence, the map f_χ is indistinguishable from

a truly random map in $\mathbb{F}_q^m$. Therefore, f_χ is a pseudorandom map.

$\square$

REFERENCES

[1] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," in *Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19.* Springer, 2000, pp. 259–274.

[2] K. Kurosawa, "Multi-recipient public-key encryption with shortened ciphertext," in *Public Key Cryptography: 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002 Paris, France, February 12–14, 2002 Proceedings 5.* Springer, 2002, pp. 48–63.

[3] M. Bellare, A. Boldyreva, and J. Staddon, "Randomness re-use in multi-recipient encryption schemeas," in *Public Key Cryptography—PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, January 6–8, 2003 Proceedings 6.* Springer, 2002, pp. 85–99.

[4] ——, "Multi-recipient encryption schemes: Security notions and randomness re-use," in *PKC*, vol. 2003, 2003, pp. 85–99.

[5] M. Bellare, A. Boldyreva, K. Kurosawa, and J. Staddon, "Multi-recipient encryption schemes: Efficient constructions and their security," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 3927–3943, 2007.

[6] ——, "Multirecipient encryption schemes: How to save on bandwidth and computation without sacrificing security," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 3927–3943, 2007.

[7] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[8] G.-L. Long, "Grover algorithm with zero theoretical failure rate," *Physical Review A*, vol. 64, no. 2, pp. 022–307, 2001.

[9] H. Bennett and C. Peikert, "Hardness of the (approximate) shortest vector problem: A simple proof via Reed-Solomon codes," *arXiv preprint arXiv:2202.07736*, 2022.

[10] D. Micciancio, "The shortest vector in a lattice is hard to approximate to within some constant," *SIAM journal on Computing*, vol. 30, no. 6, pp. 2008–2035, 2001.

[11] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in *Proceedings of the forty-first annual ACM symposium on Theory of computing*, 2009, pp. 333–342.

[12] J. Blömer and S. Naewe, "Sampling methods for shortest vectors, closest vectors and successive minima," *Theoretical Computer Science*, vol. 410, no. 18, pp. 1648–1665, 2009.

[13] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1–40, 2009.

[14] ——, "The learning with errors problem," *Invited survey in CCC*, vol. 7, no. 30, p. 11, 2010.

[15] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications," in *Proceedings of the fortieth annual ACM symposium on Theory of computing*, 2008, pp. 187–196.

[16] B. Biasioli, E. Kirshanova, C. Marcolla, and S. Rovira, "A tool for fast and secure LWE parameter selection: the FHE case," *Cryptology ePrint Archive*, 2024.