A Somewhat Homomorphic Encryption Scheme based on Multivariate Polynomial Evaluation

Uddipana Dowerah and Srinivasan Krishnaswamy
Indian Institute of Technology, Guwahati
{d.uddipan, srinikris}@iitg.ac.in

Abstract. We propose a symmetric key homomorphic encryption scheme based on the evaluation of multivariate polynomials over a finite field. The proposed scheme is somewhat homomorphic with respect to addition and multiplication. Further, we define a generalization of the Learning with Errors problem called the Hidden Subspace Membership problem and show that the semantic security of the proposed scheme can be reduced to the hardness of this problem.

Keywords: Homomorphic Encryption · Multivariate Polynomials · Learning with Errors · Hidden Subspace Membership

1 Introduction

An encryption scheme is said to be homomorphic for a set of functions if these functions can be evaluated on the plaintexts from the corresponding ciphertexts without decryption. A scheme is called fully homomorphic if functions with an arbitrary number of additions and multiplications can be homomorphically evaluated. If the number of additions and multiplications is limited, then the scheme is said to be somewhat homomorphic. Homomorphic encryption has wide applications in multiparty computation [9], secure electronic voting [4], private information retrieval [16] etc.

The first feasible construction of a fully homomorphic encryption scheme was proposed in [11]. This scheme is based on ideal lattices and uses the concept of bootstrapping to convert a somewhat homomorphic scheme to a fully homomorphic one. This concept was subsequently used in many other constructions [7,12,20,21]. As an alternative to bootstrapping, a number of schemes were proposed [5,6,8,13,14] based on the Learning with Errors (LWE) problem [18,19].

A multivariate polynomial based encryption scheme depends on the difficulty of solving a system of non-linear equations over a finite field. Polly Cracker schemes [10,2] were attempts at constructing homomorphic encryption schemes using multivariate polynomials. The security of these schemes depends on the Ideal Membership Problem and relies on the hardness of computing a Gröbner basis for an ideal. These schemes, however, are vulnerable to Linear Algebra-based attacks and attacks using efficient Gröbner basis construction algorithms [2,22]. Attempts have been made to overcome these vulnerabilities with the addition of noise as proposed in [11,5].
In this paper, we propose a multivariate polynomial based homomorphic encryption scheme. The encryption process involves noisily evaluating a multivariate polynomial at a set of secret points and adding the scaled plaintext bit to each of these evaluations. The polynomial is randomly chosen from a secret ideal. In order to prove the security of the scheme, we have defined a generalization of the Learning with Errors (LWE) problem \cite{18,19} called the Hidden Subspace Membership (HSM) problem and have shown that the semantic security of the proposed scheme can be reduced to the hardness of this problem.

The remainder of this paper is organized as follows: Section 2 contains the preliminaries for the proposed work. Section 3 contains the construction of the proposed scheme. In section 4, we discuss the homomorphic properties of the scheme and section 5 deals with the analysis of its security.

2 Preliminaries

The following notations are used in the paper. \(\lambda\) denotes the security parameter. \(\mathbb{Z}\) and \(\mathbb{N}\) denote the set of integers and natural numbers respectively. Given a set \(S\), \(x \overset{\$}{\leftarrow} S\) means that \(x\) is sampled uniformly at random from \(S\). For a real number \(x\), \(\lfloor x \rfloor\), \(\lceil x \rceil\) and \(\lfloor x \rfloor_{\pm}\) denote the rounding of \(x\) down, up or to the nearest integer of \(x\). \(\mathbb{Z}_q\) denotes the set of integers in the interval \((-\frac{q}{2}, \frac{q}{2}]\). \(\mathbb{F}_q\) denotes a finite field of cardinality \(q\), where \(q\) is a prime integer. It represents the elements in the interval \([-\lfloor \frac{q}{2} \rfloor, \lfloor \frac{q}{2} \rfloor]\). \(\mathbb{F}_q[x_1, \ldots, x_l]_{\leq r}\) denotes the set of polynomials in \(x_1, \ldots, x_l\) with coefficients in \(\mathbb{F}_q\) of degree \(\leq r\). Given a set of points \(\{z_1, \ldots, z_n\} \in \mathbb{F}_q^l\) and a polynomial \(f \in \mathbb{F}_q[x_1, \ldots, x_l]_{\leq r}\), \(f(z_1, \ldots, z_n) \in \mathbb{F}_q^n\) denotes the evaluation of \(f\) at these points. We use uppercase bold letters \(A, B, \ldots\) to denote matrices and lowercase bold letters \(a, b, \ldots\) to denote vectors.

The \(\ell_1\) norm of a vector \(v\) is denoted by \(\|v\|_1\) and the inner product of two vectors \(v_1, v_2\) is denoted using \(\langle v_1, v_2 \rangle := v_1^T v_2\). A function \(f(x) : \mathbb{N} \rightarrow \mathbb{R}\) is called negligible if, for every \(c \in \mathbb{N}\), there exists an integer \(n_c\) such that \(|f(x)| < \frac{1}{x^c}\) for all \(x \geq n_c\).

2.1 Hidden Subspace Membership

The Hidden Subspace membership (HSM) problem involves distinguishing a random vector from a noisy vector of a given subspace \(S\). We use the game playing framework adopted from \cite{3} to formally define the HSM problem.

**Definition 1. (Hidden Subspace Membership).** Let \(S\) be an \(l\) dimensional subspace of the vector space \(V := \mathbb{F}_q^n\), for some \(n,q \in \mathbb{N}\) and \(l \geq 1\), such that \(q\) is prime and let \(\mathcal{N}\) be a noise distribution on \(\mathbb{F}_q^n\). Then, the HSM problem denoted as \(\text{HSM}_{n,q,\mathcal{N}}\) can be defined in terms of the game shown in Figure 1. A PPT adversary \(A\) wins the game if it can guess the value of \(\beta\) with a non-negligible advantage, given by

\[
\text{Adv}^{\text{HSM},A}_{\text{HSM}_{n,q,\mathcal{N}}} (\lambda) := \left| \Pr[\text{HSM}^A_{n,q,\mathcal{N}}(\lambda) \Rightarrow 1] - \frac{1}{2} \right|
\]
This problem can be seen as a generalization of the Decisional Learning with Errors (DLWE) problem which is defined as follows:

**Definition 2. (Decisional Learning With Errors).** Given a noise distribution \( X \) on \( \mathbb{Z}_q \) and an integer \( q = q(\lambda) \), the DLWE problem can be defined in terms of the game shown in Figure 1.3. A PPT adversary \( A \) wins the game if it can guess the value of \( \beta \) with a non-negligible advantage given by

\[
Adv^{LWE,A}_{n,q,X}(\lambda) := \left| P_{LWE_n,q,X}(\lambda) \Rightarrow 1 \right| - \frac{1}{2}
\]

An LWE sample \((a_i, b_i) \in \mathbb{Z}_n \times \mathbb{Z}_q\) that satisfies \(a_i^T s + e_i = b_i \mod q\) can be written as:

\[
[a_i - b_i] \begin{bmatrix} s \\ 1 \end{bmatrix} \approx X \cdot 0 \mod q
\]

which is a noisy equation with the noise being sampled from the distribution \( X \) on \( \mathbb{Z}_q \). Hence, the DLWE problem can be seen as an instance of the HSM problem where the subspace is \((s 1)^\perp \subseteq \mathbb{Z}_n\) and the noise is added only to the
last element of the vector. The above discussion is formalized in terms of the following lemma.

**Lemma 1.** Let \( S \) be an \( n \)-dimensional subspace of the vector space \( \mathbb{Z}_q^{n+1} \). Let \( X \) be a zero mean distribution on \( \mathbb{Z}_q \) and let \( \mathcal{N} := (\mathbf{0}, X) \), where \( \mathbf{0} \in \mathbb{Z}_q^n \). Then, any PPT adversary \( A \) against the HSM problem \( \text{HSM}_{n+1,q,N} \) can be transformed into a PPT adversary \( B \) against the LWE problem \( \text{DLWE}_{n,q,N} \) such that

\[
\text{Adv}^\text{HSM,A}_{n+1,q,N}(\lambda) = \text{Adv}^\text{DLWE,B}_{n,q,N}(\lambda)
\]

**Proof.** We construct an adversary \( B \) against \( \text{DLWE}_{n,q,N} \) from an adversary \( A \) against \( \text{HSM}_{n+1,q,N} \). Observe that, an HSM sample \( \mathbf{v}_i \leftarrow \mathbf{v}_i + \mathbf{e}_i \), where \( \mathbf{v}_i \overset{\$}{\leftarrow} S \) and \( \mathbf{e}_i \overset{\$}{\leftarrow} X \), satisfies the equation \( \mathbf{v}_i^T \mathbf{s}_i \approx 0 \), where \( \mathbf{s}_i := (s, 1) \in \mathbb{Z}_q^{n+1} \).

When \( A \) queries the Sample oracle of HSM, \( B \) queries the Sample oracle of DLWE to obtain \( (\mathbf{a}, b) \) and returns the vector \( (\mathbf{a}, -b) \in \mathbb{Z}_q^{n+1} \) to \( A \). Similarly, when \( A \) queries the Challenge oracle of HSM, \( B \) queries the Challenge oracle of DLWE and answers similarly. If \( A \) outputs the correct value of \( \beta \) for \( \text{HSM}_{n+1,q,N} \), then \( B \) also happens to output the correct value of \( \beta \) for \( \text{DLWE}_{n,q,N} \).

Thus solving the LWE problem over \( \mathbb{Z}_q^n \) is equivalent to solving the HSM problem over \( \mathbb{Z}_q^{n+1} \) for a subspace of dimension \( n \), where only the last entry is affected by noise.

**Definition 3.** (Discrete Gaussian distribution). For \( \alpha > 0 \) and for \( q = q(\lambda) \), the density function of a Gaussian distribution \( \Psi_\alpha \) over \( \mathbb{R} \) is given by,

\[
D_\alpha(x) = \frac{1}{\sqrt{2\pi\alpha}} \exp\left(-\frac{1}{2} \left(\frac{x}{\alpha}\right)^2\right)
\]

Then, the discrete Gaussian distribution \( \overline{\Psi}_\alpha \) on \( \mathbb{Z}_q \) is the distribution with mean zero and standard deviation \( \alpha q \), obtained by sampling an element \( x \leftarrow D_\alpha \) and outputting \( \lfloor x \cdot q \rfloor \mod q \).

When the noise is sampled according to the distribution \( \overline{\Psi}_\alpha \) with \( \alpha q \geq 2\sqrt{n} \), there exists a quantum reduction from the decisional variant of the shortest vector problem (GAPSVP) to the LWE problem \( [18] \). A classical reduction has also been proposed in \( [17] \).

We assume that the HSM problem is hard for an \( l \)-dimensional subspace of an \( n \)-dimensional space when \( n - l \) entries are corrupted by noise sampled from a discrete Gaussian distribution. (The justification for this assumption and a detailed analysis of the hardness of the HSM problem will be given in the complete paper.)

### 3 The Proposed Scheme

Consider an ideal \( I \) of the polynomial ring \( \mathbb{F}_q[x_1, \ldots, x_\ell] \), where \( q \) is polynomial in the security parameter \( \lambda \). Let \( I \leq r \) denotes the set of polynomials in \( I \) with degree \( \leq r \). \( \mathbb{F}_q[x_1, \ldots, x_\ell]_{\leq r} \) is a vector space over \( \mathbb{F}_q \) of dimension \( N := \ell + r \) and \( I_{\leq r} \) is a subspace of this vector space. Let \( \text{dim}(I_{\leq r}) \) be the dimension of this subspace. A polynomial \( f \in \mathbb{F}_q[x_1, \ldots, x_\ell]_{\leq r} \) evaluated at all points of \( \mathbb{F}_q^\ell \) generates a vector space in \( \mathbb{F}_q^N \). The set of such vectors obtained by evaluating
all polynomials in $\mathbb{F}_q[x_1, \ldots, x_\ell]_{\leq r}$ constitutes an $N$-dimensional subspace of $\mathbb{F}_q^r$. Evaluating polynomials in $I_{\leq r}$ gives us a $\text{dim}(I_{\leq r})$-dimensional subspace $\mathcal{V}_{I_{\leq r}}$. The ciphertext size $n$ is chosen such that $n$ is polynomial in $\lambda$ but is significantly less than $q$ and $\text{dim}(I_{\leq r}) < n \leq N$. We then choose $n$ distinct points $\{z_1, \ldots, z_n\} \in \mathbb{F}_q^n$ which satisfy the following conditions:

1. Every vector in $\mathbb{F}_q^n$ can be got by evaluating a polynomial in $\mathbb{F}_q[x_1, \ldots, x_\ell]_{\leq r}$ at $(z_1, \ldots, z_n)$.
2. Every vector in $\mathbb{F}_q^{\text{dim}(I_{\leq r})}$ can be got by evaluating a polynomial in $I_{\leq r}$ at $(z_1, \ldots, z_{\text{dim}(I_{\leq r})})$.

The conditions imposed on $(z_1, \ldots, z_n)$ ensure that for every given vector $s_2 \in \mathbb{F}_q^{\text{dim}(I_{\leq r})}$, there exists a vector $s \in (\mathcal{V}_{I_{\leq r}})\perp$ such that $s = (s_1, s_2)$.

Let $v_i \in \mathbb{F}_q^n$ be the vector obtained by evaluating the monomials of degree $\leq r$ at the point $z_i \in \mathbb{F}_q^r$, for $1 \leq i \leq n$. Let $G \in \mathbb{F}_q^{n \times N}$ be the matrix obtained by assigning $G(i,:) = v_i$ for $1 \leq i \leq n$. Let $f(x_1, \ldots, x_\ell)$ be a polynomial, sampled uniformly at random from $I_{\leq r}$. If $f \in \mathbb{F}_q^n$ denotes the coefficient vector of $f$, then $f(z_1, \ldots, z_n) = G \cdot f \in \mathbb{F}_q^n$.

Let us now consider an example to illustrate the construction of $G$. For $\ell = 2, r = 2$ and $N = 6$, the monomials of $\mathbb{F}_q[x_1, x_2]_{\leq 2}$ according to the lexicographic order are $\{1, x_1, x_2, x_1^2, x_1x_2, x_2^2\}$. If $n = 3$, then let $z_1 = (z_{11}, z_{12}), z_2 = (z_{21}, z_{22}), z_3 = (z_{31}, z_{32})$ be 3 distinct points in $\mathbb{F}_q^2$. Then, $G \in \mathbb{F}_q^{3 \times 6}$ represents the following matrix:

$$G = \begin{bmatrix} 1 & z_{11} & z_{12} & z_{11}z_{21} & z_{12}z_{22} & z_{11}z_{22} \\ 1 & z_{12} & z_{22} & z_{12}z_{21} & z_{22}z_{12} & z_{12}z_{22} \\ 1 & z_{13} & z_{23} & z_{13}z_{23} & z_{23}z_{13} & z_{23}z_{23} \end{bmatrix}$$ (2)

The proposed encryption scheme consists of the following algorithms. The plaintext space is $\{0, 1\}$ and the ciphertexts are vectors of order $n$ over $\mathbb{F}_q$. Let $\mathcal{X}$ be a noise distribution that samples its entries from the discrete Gaussian distribution $\mathbb{F}_n$ on $\mathbb{Z}_q$.

- **KeyGen($1^\lambda$):** Consider an ideal $I \subseteq \mathbb{F}_q[x_1, \ldots, x_\ell]$ and a set of $n$ distinct points $\{z_1, \ldots, z_n\}$ in $\mathbb{F}_q^r$ and construct the matrix $G \in \mathbb{F}_q^{n \times N}$. Choose a vector $s = (s_1, s_2) \in (\mathcal{V}_{I_{\leq r}})\perp$ and a constant $p \in \mathbb{N}$ such that, if $s = \sum_{i=1}^n s_i$ denotes the sum of the elements of $s$ and $e$ denotes a vector of order $n$ whose entries are sampled from the distribution $\mathcal{X}$, then $\eta(q) < s \cdot p \leq \lfloor q/2 \rfloor$ and the distribution of $(s, e)$ has a standard deviation $< k(q)$, where $\eta$ and $k$ are constants that depend on the probability of decryption error and the number of homomorphic operations. The secret key is a basis for the ideal $I$, the set of points $\{z_1, \ldots, z_n\}$ and the integer $p$. If the choice of $I$ is restricted to a radical ideal whose variety has a finite number of points, then the ideal can also be expressed in terms of its variety.

- **Encrypt($sk, m$):** To encrypt a message $m \in \{0, 1\}$, sample a polynomial $f$ of degree $\leq r$, uniformly at random from the ideal $I$ and a vector $e = (0, \mathbb{F})$,
where \( \mathbf{c} \) is a vector of order \( n - \dim(I_{\leq r}) \) and the entries of \( \mathbf{c} \) are chosen according to the distribution \( \mathcal{X} \). If \( \mathbf{f} \) denotes the coefficient vector of \( f \) and \( \mathbf{1} \) denotes the all 1’s vector of order \( n \) and \( M := m \cdot p \), then the ciphertext can be computed as

\[
c = M \cdot \mathbf{1} + G \cdot \mathbf{f} + \mathbf{e} \pmod{q}
\]  

(3)

- **Decrypt**(sk, c): Given the ciphertext \( c \), the plaintext \( m \) can be recovered as

\[
m = \frac{1}{\sigma_s \cdot p} \langle (s, c) \pmod{q} \rangle \pmod{2}
\]  

(4)

**Remark 1.** This scheme can also be seen as a coding theory based scheme. If the polynomial chosen in the above encryption scheme is \( f \), then the ciphertext can be seen as a noisy punctured Reed-Muller encoding of the polynomial \( f + m \).

**Correctness of Decryption.** Since \( s \in (\mathcal{V}_{\leq r})^\perp \), \( \langle s, G\mathbf{f} \rangle = 0 \pmod{q} \). Therefore,

\[
\langle s, c \rangle = m \cdot \langle \sigma_s p \rangle + \langle s_2, \mathbf{c} \rangle \pmod{q}
\]  

(5)

If \( \|s_2, \mathbf{c}\| < \left\lfloor \frac{(\sigma_s \cdot p)}{2} \right\rfloor \), then \( \frac{1}{\sigma_s \cdot p} \langle (s, c) \pmod{q} \rangle = m \pmod{2} \). If for some \( \epsilon > 0 \), it holds that

\[
Pr_{\mathbf{c} \in \mathcal{X}^{n-\dim(I_{\leq r})}} \left[ \|s_2, \mathbf{c}\| > \left\lfloor \frac{(\sigma_s \cdot p)}{2} \right\rfloor \right] \leq \epsilon
\]  

(6)

then, the probability of decryption error is at most \( \epsilon \). In other words, the decryption function will output the correct message with probability \( 1 - \epsilon \). Since the entries of \( \mathbf{c} \) are sampled from the distribution \( \mathcal{X} \), \( \langle s_2, \mathbf{c} \rangle \) is distributed with a standard deviation \( \|s_2\|_2 \alpha q \). If \( \mathcal{X}_{\|s\|_2 \approx \alpha q} \) denotes this distribution, then using Chebyshev’s inequality, we can write

\[
Pr_{x \in \mathcal{X}_{\|s\|_2 \approx \alpha q}} \left[ |x| > \left\lfloor \frac{(\sigma_s \cdot p)}{2} \right\rfloor \right] \leq Pr_{x \in \mathcal{X}_{\|s\|_2 \approx \alpha q}} \left[ |x| > k \alpha q \right] \leq \frac{1}{k^2}
\]  

(7)

where \( k < \frac{\sigma_s \cdot p}{2 \|s_2\|_2 \alpha q} \) and \( \epsilon = \frac{1}{k^2} \). Therefore, if \( p \) is chosen such that \( \sigma_s \cdot p > (2 \|s_2\|_2 \alpha q) / \sqrt{\epsilon} \), then the probability of decryption error is \( \leq \epsilon \).

For the case when only additive homomorphism is required, we can choose \( s = (s_1, s_2) \in (\mathcal{V}_{\leq r})^2 \) such that \( s_2 \) is of the form \( s_2 = (0, \ldots, 0, 1) \). Thus \( (s, e) \) will just be equal to the last entry of \( e \). However as we will see in the subsequent section that this may not be possible when multiplicative homomorphism is required.

### 4 Homomorphic Properties

If \( \phi : \{0,1\}^l \rightarrow \{0,1\} \) denotes a function to be performed on the plaintexts \( m_1, \ldots, m_l \), then homomorphically evaluating \( \phi \) involves calculating a new ciphertext \( c_{\text{out}} \) such that \( \text{Dec}(c_{\text{out}}, sk) = \phi(m_1, \ldots, m_l) \). Any function \( \phi \) involving binary variables can be evaluated using a set of addition and multiplication gates. The remainder of this section analyses homomorphic addition and multiplication of ciphertexts in the proposed scheme.
4.1 Addition.

Given two ciphertexts \( c_1 \) and \( c_2 \) of the respective plaintexts \( m_1 \) and \( m_2 \), where \( c_1 = M_1 \cdot 1 + G \cdot f_1 + e_1 \) and \( c_2 = M_2 \cdot 1 + G \cdot f_2 + e_2 \), homomorphic addition of \( m_1 \) and \( m_2 \) can be performed by computing

\[
c_{\text{add}} = c_1 + c_2 \pmod{q} = (M_1 + M_2) \cdot 1 + G(f_1 + f_2) + (e_1 + e_2) \pmod{q}
\]

(8)

Since \( \langle s, G(f_1 + f_2) \rangle = 0 \pmod{q} \) and given that, \( M_i = m_i \cdot p \) and \( e_i = (0, \overline{e}_i) \) for \( i \in \{1, 2\} \), where \( \overline{e}_i \) is a vector of order \( n - \dim(I_{\leq r}) \) and its entries are sampled from the distribution \( \mathcal{X} \), we have

\[
\langle s, c_{\text{add}} \rangle = \langle m_1 + m_2, \sigma_p \rangle + \langle s_2, \overline{e}_1 + \overline{e}_2 \rangle \pmod{q}
\]

(9)

If \( c_{\text{add}} := \langle s_2, \overline{e}_1 + \overline{e}_2 \rangle \pmod{q} \), then \( c_{\text{add}} \) decrypts correctly to \( (m_1 + m_2) \pmod{2} \) as long as \( (m_1 + m_2) \cdot \sigma_p \pmod{q} < \lfloor q/2 \rfloor \) and \( |c_{\text{add}}| < \lfloor (\sigma_p / 2) \rfloor \). The distribution of \( e_{\text{add}} \) is Gaussian with a standard deviation \( \sqrt{2} \|s_2\|_2 q^2 \). It can be easily verified that due to the increase in the standard deviation after addition, the probability of decryption error increases by a factor of 2.

4.2 Multiplication.

Multiplication is based on the fact that, given two polynomials \( f_1, f_2 \in \mathbb{F}_q[x_1, \ldots, x_r] \subseteq \mathbb{F}_q \),

\[
f_1(z) \cdot f_2(z) = (f_1 \cdot f_2)(z)
\]

(10)

where \( \deg(f_1f_2) \leq 2r \). Therefore, \( f_1 f_2 \in I \) but it is not an element of the subspace \( I_{\leq r} \). In order to do homomorphic multiplication, \( n \) must be greater than the dimension of \( \mathcal{V}_{I_{\leq r}} \) and the vector \( s = (s_1, s_2) \) must be an element of \( (\mathcal{V}_{I_{\leq r}})^\perp \) such that \( s_2 \in \mathbb{F}_q^{n - \dim(I_{\leq r})} \). The noise must be added to the last \( n - \dim(I_{\leq r}) \) entries.

Given two ciphertexts \( c_1 \) and \( c_2 \), the homomorphic multiplication of its respective plaintexts \( m_1 \) and \( m_2 \) can be obtained by taking the component-wise product of \( c_1 \) and \( c_2 \). In order to maintain the invariant structure \( \langle s, c \rangle = m \cdot \langle s, \sigma_p \rangle + \langle s_2, \overline{e} \rangle \) for decryption, we multiply the product by \( 1/p \). Specifically, if \( c_1 = M_1 \cdot 1 + G \cdot f_1 + e_1 \) and \( c_2 = M_2 \cdot 1 + G \cdot f_2 + e_2 \), then

\[
c_{\text{mult}} = \frac{1}{p} (c_1 \circ c_2) \pmod{q}
\]

\[
= (m_1 m_2) \cdot 1 + m_1 \cdot G f_2 + m_1 \cdot e_2 + m_2 \cdot G f_1 + m_2 \cdot e_1
\]

\[
+ \frac{1}{p} \left[ G(f_1 \circ e_2 + e_1 \circ G f_2 + (G f_1 \circ G f_2) + (e_1 \circ e_2)) \right] \pmod{q}
\]

(11)

where \( \circ \) denotes the component-wise product of two vectors. Given that, \( M_i = m_i \cdot p \) and \( e_i = (0, \overline{e}_i) \) for \( i \in \{1, 2\} \), where \( \overline{e}_i \) is a vector of order \( n - \dim(I_{\leq r}) \) and its entries are sampled from the distribution \( \mathcal{X} \),

\[
\langle s, c_{\text{mult}} \rangle = \langle m_1 m_2, \sigma_p \rangle + \left( s_2, m_1 \cdot \overline{e}_2 + m_2 \cdot \overline{e}_1 + \frac{1}{p} \cdot (\overline{e}_1 \circ \overline{e}_2) \right) \pmod{q}
\]

(12)
If \( e_{\text{mult}} := \langle s_2, m_1 \cdot \bar{x}_2 + m_2 \cdot \bar{x}_1 + \frac{1}{p} (\bar{x}_1 \circ \bar{x}_2) \rangle \pmod{q} \), then \( e_{\text{mult}} \) decrypts correctly to \( m_1 m_2 \) as long as \( |e_{\text{mult}}| < \lfloor (s_p \cdot p)/2 \rfloor \), where \( e_{\text{mult}} \) is a random variable with mean zero and standard deviation \( < \sqrt{2a_q + \frac{1}{\sqrt{p}}(a_q)^2} \).

While homomorphic addition does not impose any constraints on the ciphertext size, it does lead to an increase in noise. This limits the number of additions possible. Homomorphic multiplication introduces more noise than addition and the size of the ciphertext increases significantly with the number of multiplications possible. The increase in noise by homomorphic operations can be countered by using techniques such as modulus switching \([8,6]\). (The complete paper will contain a more detailed discussion about the same.) Countering the increase in ciphertext size for homomorphic multiplication remains a challenge.

5 Security

We show that the proposed scheme is semantically secure based on the hardness of the Hidden Subspace Membership problem. In a Chosen Plaintext Attack (CPA) model, the adversary has a number of plaintext-ciphertext pairs at its disposal. A symmetric key encryption scheme is said to be semantically secure or indistinguishable under a chosen plaintext attack (IND-CPA) if, given sufficient samples (plaintext-ciphertext pairs), no adversary can distinguish between the encryptions of 0 from the encryptions of messages of its choice with probability more than \( \frac{1}{2} \).

Definition 4. (IND-CPA Security). The IND-CPA security of a symmetric encryption scheme can be defined in terms of the game shown in Figure 1.3. A PPT adversary \( A \) selects two messages \( (m_0, m_1) \) such that one of them is 0 and the Left-Right oracle outputs the encryption of one of the messages by choosing \( \beta \in \{0, 1\} \). \( A \) wins the game if it can guess the value of \( \beta \) with a non-negligible advantage defined by

\[
\text{Adv}^{\text{IND-CPA}}_\text{A}(\lambda) := \left| \Pr[A^{\text{IND-CPA}}(\lambda) = 1] - \Pr[A^{\text{IND-CPA}}(0)^{\text{Enc}}(\lambda) = 1] \right|
\]

It is clear from the construction of the scheme that the encryptions of 0 are noisy elements of the subspace \( \mathcal{V}_{2r} \subseteq \mathbb{F}_q^n \). Therefore, distinguishing an
Theorem 1. A PPT adversary $A$ that breaks the IND-CPA security of the proposed scheme with non-negligible advantage $\epsilon$ can be converted into a PPT adversary $B$ that can solve an instance of the HSM problem with advantage at least $\frac{\epsilon}{2}$.

Proof. $B$ initializes $A$ with the parameters $(q, n, X)$. When $A$ asks for an encryption of 0, $B$ queries the procedure Sample of the HSM game to get $v \leftarrow v + e$, where $e \overset{\$}{\leftarrow} X^n$ and returns the vector $c = v$. Similarly, when $A$ queries the Left-Right oracle of the IND-CPA game, $B$ queries the procedure Challenge of the HSM game to get $v$ and returns a vector $c$ upon choosing $\beta \overset{\$}{\leftarrow} \{0, 1\}$ and setting $c = v + (p \cdot m_{\beta}) \cdot 1$.

If the sample obtained from the Challenge oracle of HSM is a noisy element of $S$, then $A$ runs in a similar environment to that of the IND-CPA game and hence, $B$ outputs $\beta$ with probability $\frac{1}{2} + \epsilon$. On the other hand, if the sample returned is uniform in $F_q^n$, then $B$ outputs $\beta$ with probability $\frac{1}{2}$. Therefore, the probability that $B$ solves the HSM problem is $\geq \frac{1}{2} + \frac{\epsilon}{2}$. Hence, the advantage of $B$ in solving the HSM problem is $\geq \frac{\epsilon}{2}$.

6 Conclusions

A symmetric key homomorphic encryption scheme has been proposed based on the evaluation of multivariate polynomials. The security of the scheme is based on the hardness of the Hidden Subspace Membership problem. In its current form, the scheme is somewhat homomorphic and for a given ciphertext size, can perform a limited number of homomorphic additions and multiplications. Future work includes converting the scheme into a fully homomorphic one and designing a public key variant of the same.

References

1. Albrecht, M.R., Farshim, P., Faugere, J.C., Perret, L.: Polly cracker, revisited. In: Advances in Cryptology–ASIACRYPT 2011, pp. 179–196. Springer (2011)
2. Barkee, B., Can, D.C., Ecks, J., Moriarty, T., Ree, R.: Why you cannot even hope to use gröbner bases in public key cryptography: an open letter to a scientist who failed and a challenge to those who have not yet failed. Journal of Symbolic Computation 18(6), 497–501 (1994)
3. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: Foundations of Computer Science, 1997. Proceedings., 38th Annual Symposium on. pp. 394–403. IEEE (1997)
4. Benaloh, J.D.C.: Verifiable secret-ballot elections (1987)
5. Brakerski, Z.: Fully homomorphic encryption without modulus switching from classical gapsvp. In: Advances in cryptology–crypto 2012, pp. 868–886. Springer (2012)
6. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT) 6(3), 13 (2014)

7. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-lwe and security for key dependent messages. In: Advances in Cryptology–CRYPTO 2011, pp. 505–524. Springer (2011)

8. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) lwe. SIAM Journal on Computing 43(2), 831–871 (2014)

9. Cramer, R., Damgård, I., Nielsen, J.: Multiparty computation from threshold homomorphic encryption. Advances in cryptology—EUROCRYPT 2001 pp. 280–300 (2001)

10. Fellows, M., Koblitz, N.: Combinatorial cryptosystems galore. Contemporary Mathematics 168(2), 51–61 (1993)

11. Gentry, C.: A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University (2009)

12. Gentry, C., Halevi, S.: Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In: Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on. pp. 107–109. IEEE (2011)

13. Gentry, C., Halevi, S., Vaikuntanathan, V.: A simple bgn-type cryptosystem from lwe. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 506–522. Springer (2010)

14. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: Advances in Cryptology–CRYPTO 2013, pp. 75–92. Springer (2013)

15. Herold, G.: Polly cracker, revisited, revisited. In: International Workshop on Public Key Cryptography. pp. 17–33. Springer (2012)

16. Lipmaa, H.: On diophantine complexity and statistical zero-knowledge arguments. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 398–415. Springer (2003)

17. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the forty-first annual ACM symposium on Theory of computing. pp. 333–342. ACM (2009)

18. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) 56(6), 34 (2009)

19. Regev, O.: The learning with errors problem. Invited survey in CCC p. 15 (2010)

20. Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: International Workshop on Public Key Cryptography. pp. 420–443. Springer (2010)

21. Van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully homomorphic encryption over the integers. In: Advances in cryptology–EUROCRYPT 2010, pp. 24–43. Springer (2010)

22. Levy-dit Vehel, F., Marinari, M.G., Perret, L., Traverso, C.: A survey on polly cracker systems. In: Gröbner Bases, Coding, and Cryptography, pp. 285–305. Springer (2009)