On the Security of Some Code-Based (F)HE Approaches Using Reed-Muller Codes

Svenja Lage[1] and Luana Kurmann[1,2]

[1]Institute of Communications and Navigation,
German Aerospace Center (DLR)
[2]Technical University of Munich
{svenja.lage, luana.kurmann}@dlr.de

Abstract

We analyze the security of the somewhat homomorphic encryption scheme proposed by Armknecht et al. [AAPS11], which can be seen as a fundamental step toward fully homomorphic encryption based on coding theory and Reed-Muller codes in particular. Through our cryptanalysis, we identify critical vulnerabilities that enable partial key recovery and, in many cases, full message recovery. Our analysis also exposes critical weaknesses in two later code-based fully homomorphic encryption schemes by Challa and Gunta [CG16, CG21b], both of which adopt Reed-Muller codes as their underlying structure.

Key Words : Homomorphic encryption, Reed-Muller codes, Cryptanalysis

1 Introduction

Privacy-preserving computation, especially in modern cloud environments, demands cryptographic techniques that balance confidentiality and computational efficiency. One promising approach in this context is Fully Homomorphic Encryption (FHE), which enables arbitrary computations to be performed directly on encrypted data. This allows potentially expensive computations to be outsourced to any non-trusted server while ensuring that both the input data and all intermediate and final results remain confidential from the server. Although the idea of such an encryption dates back to 1978 [RAD78], its existence was unproven for decades. It was only in 2009, when Craig Gentry proposed the first construction of an FHE scheme [Gen09]. Gentry started from a Somewhat Homomorphic Encryption (SHE) scheme, which supports only a limited number of additions and multiplications. He

then turned this scheme into a fully homomorphic scheme by using a bootstrapping procedure. The bootstrapping procedure refreshes the ciphertext noise, which increases with each operation, and would eventually prevent successful decryption. Following Gentry's work, many different approaches to construct FHE schemes emerged, nearly all of them based on lattice-based cryptography (compare [MSM+22]). However, relying on a single hardness assumption is risky; a diversity of hard problems increases robustness. One promising alternative to lattice-based encryption is code-based cryptography, which is nearly as old as RSA [RSA78], with the McEliece scheme [McE78] serving as the most prominent and well-studied example.

While numerous code-based encryption schemes exist, code-based FHE remains challenging. In this work, we analyze the pioneer code-based somewhat homomorphic encryption scheme by Armknecht et al. [AAPS11]. This scheme, though not fully homomorphic, was the first code-based construction to support both addition and multiplication of ciphertexts, using specific codes, for example Reed-Muller codes. However, we identify critical security vulnerabilities within the scheme, allowing an attacker to recover parts of the secret key. If, in addition, only a few plaintext-ciphertext pairs are known, the attacker can even recover the messages. Consequently, for many practical parameter choices and scenarios, the scheme must be considered broken. The idea to use Reed-Muller codes for code-based fully homomorphic encryption was adapted by Challa and Gunta in two different constructions, ([CG21b],[CG23]) and ([CG16],[CG21a]). However, we found that the first approach's homomorphic multiplication relies on incorrect decoding. The second approach allows for homomorphic addition and multiplication but suffers from a critical security issue.

2 Preliminaries

Let q be a power of a prime and $\mathbb{F}_q$ the finite field with q elements. For a vector $v \in \mathbb{F}_q^n$ and a set $I \subseteq \{1, \ldots, n\}$, we denote by v_I the restriction of v to the components in I. Given two vectors $v_1, v_2 \in \mathbb{F}_q^n$, let $v_1 \star v_2 \in \mathbb{F}_q^n$ be the componentwise multiplication. For a vector $v = (v_1, \ldots, v_k) \in \mathbb{F}_q^k$ and a matrix $G \in \mathbb{F}_q^{k \times n}$ with entries $g_{i,j}$ for $i = 1, \ldots k$ and $j = 1, \ldots, n$, we define the following vector-matrix product

$$v \times G = \begin{pmatrix} v_1 g_{1,1} & \ldots & v_1 g_{1,n} \\ \vdots & & \vdots \\ v_k g_{k,1} & \ldots & v_k g_{k,n} \end{pmatrix}.$$

An $[n, k]$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of length n and dimension k is a k-dimensional linear subspace of $\mathbb{F}_q^n$. Every linear code $\mathcal{C}$ can be represented by a generator

matrix $G \in \mathbb{F}_q^{k \times n}$ of rank k. A set $I \subseteq \{1, \ldots, n\}$ of size k is called an information set of $\mathcal{C}$ if the corresponding columns of the generator matrix are linearly independent. As a basis for all schemes, we consider a special class of linear codes, namely linear evaluation codes, defined as follows.

Definition 1. *(Linear Evaluation Codes) Let $\mathcal{X}$ be a geometric object, in the following we choose $\mathcal{X}$ to be the cartesian product of a finite field $\mathbb{F}_q$, and $\mathcal{L} \subseteq \{f : \mathcal{X} \to \mathbb{F}_q\}$ a vector space of functions from $\mathcal{X}$ to $\mathbb{F}_q$. Let $P = (p_1, \ldots, p_n) \in \mathcal{X}^n$ be a set of evaluation points. For $f \in \mathcal{L}$, let $Eval_P(f)$ denote the evaluation of f in P, i.e., $Eval_P(f) = (f(p_1), \ldots, f(p_n)) \in \mathbb{F}_q^n$. The evaluation code with respect to $\mathcal{L}$ and P is given by $\mathcal{C} = \{Eval_P(f) : f \in \mathcal{L}\} \subseteq \mathbb{F}_q^n$.*

Evaluation codes cover a broad range of well-investigated classes of codes, such as Reed-Solomon [RS60] or Reed-Muller codes ([Ree54, Mul54, DGW70]). Since the code-based FHE approaches we study in this work are built upon Reed-Muller codes, we provide a concrete definition below.

Definition 2. *(Reed-Muller Codes) Let $\mathbb{F}_q[x_1, \ldots, x_m]$ be the polynomial ring in m variables. The q-ary Reed-Muller code $\mathcal{C} = RM_q(m, \rho)$ of order ρ is defined as*

$$\mathcal{C} = RM_q(m, \rho) = \left\{ Eval_{\mathbb{F}_q^m}(f) : f \in \mathbb{F}_q[x_1, \ldots, x_m],\ deg(f) \leq \rho \right\}.$$

The code has length $n = q^m$ and dimension $k = \binom{m+\rho}{m}$. Given a subset $\mathcal{S}$ of $\{1, \ldots, n\}$, the punctured Reed-Muller code $\mathcal{P}_{\mathcal{S}}(\mathcal{C})$ can be defined by deleting all coordinates in $\mathcal{S}$ from all codewords of $\mathcal{C}$, i.e.,

$$\mathcal{P}_{\mathcal{S}}(\mathcal{C}) = \{(c_i)_{i \notin \mathcal{S}} : (c_1, \ldots, c_n) \in \mathcal{C}\}.$$

Definition 3. *(Power Code) Let $\mathcal{C}$ be an $[n, k]$-linear code. The square code $\mathcal{C}^{\star 2}$ with dimension denoted by $k^{\star 2}$ is defined by $\mathcal{C}^{\star 2} = \langle \{c_1 \star c_2 : c_1, c_2 \in \mathcal{C}\} \rangle$. Iteratively, for every $\mu \geq 1$, we define the μ-th power product code with dimension $k^{\star \mu}$ by*

$$\mathcal{C}^{\star \mu} = \langle \{c_1 \star \ldots \star c_\mu : c_i \in \mathcal{C} \text{ for } i = 1, \ldots, \mu\} \rangle.$$

For random codes, the dimension $k^{\star \mu}$ of the μ-th power product code grows polynomially in k [CCMZ15]. However, for certain code classes, such as Reed-Muller codes, the dimension grows only linearly in k, which, in particular, makes them more suitable for applications such as the code-based somewhat homomorphic encryption scheme in [AAPS11].

3 A Code-Based SHE Scheme

In [AAPS11], Armknecht, Augot, Perret, and Sadeghi introduced a code-based SHE scheme. This scheme enables an unlimited number of additions

and a limited number of multiplications using a code-based symmetric key encryption. To enable homomorphic multiplication, the authors employ a special class of linear evaluation codes.

Definition 4. *(μ-Multiplicative Codes) Let $\mathcal{C}$ be an $[n,k]$-linear evaluation code with evaluation points P. The code is called μ-multiplicative if there exists an $[n,\widehat{k}]$-linear evaluation code $\widehat{\mathcal{C}}$ with evaluation points P such that $\mathcal{C}^{\star l} \subseteq \widehat{\mathcal{C}}$ for every $l \leq \mu$.*

Using μ-multiplicative codes, the somewhat homomorphic encryption scheme in [AAPS11] is defined as follows.

Setup: The user selects the security level s, the expected number of fresh encryptions L, and the maximum degree μ of the supported polynomials. The setup algorithm samples an $[n,k]$-linear, μ-multiplicative evaluation code $\mathcal{C}$ over a function space $\mathcal{L}$, alongside evaluation points $P = (p_1,\ldots,p_n) \in \mathcal{X}^n$. A random element $y \in \mathcal{X}$ distinct from all points in P is chosen as the message support. Additionally, a set $I \subset \{1,\ldots,n\}$ of error-free positions is sampled, where the cardinality $|I| = T$ is determined by the chosen input parameters and the code. The secret key is given by $sk = (P, y, I)$.

Encryption: Given the secret key sk, the encryption procedure encodes a plaintext message $m \in \mathbb{F}_q$ into a codeword $w \in \mathbb{F}_q^n$ of $\mathcal{C}$ as follows. Let $\mathcal{L}_m = \{f \in \mathcal{L} : f(y) = m\}$. To encode $m \in \mathbb{F}_q$, randomly chose $f \in \mathcal{L}_m$ and evaluate f at all points in P. Add a uniformly random error vector $e \in \mathbb{F}_q^n$ with support on $I^C = \{1,\ldots,n\} \setminus I$. The resulting ciphertext is a tuple $(c,1) = (w+e,1)$, where the second component tracks the number of multiplications.

Decryption: Given the secret key sk, a ciphertext (c,γ) with noisy codeword c and multiplication count $\gamma \leq \mu$ can be decrypted via polynomial interpolation using the undisturbed values. The message is obtained by evaluating the received polynomial in the message support y.

The scheme supports two types of homomorphic operations - unlimited additions and limited multiplications: Given two ciphertexts (c_1,γ_1) and (c_2,γ_2), their sum is calculated as $(c_1+c_2, \max\{\gamma_1,\gamma_2\})$. To multiply the two ciphertexts, calculate $(c_1 \star c_2, \gamma_1+\gamma_2)$ with the componentwise product of the noisy codewords. Both operations preserve the encryption of the corresponding plaintext operations [AAPS11, Theorem 1].

The authors analyzed the security of their scheme under various aspects. When only a single ciphertext is available, decoding the noisy codeword is

a hard problem. However, this hardness guarantee softens when an attacker has access to multiple noisy codewords with the same error support. The scheme's security is hence based on its connection to the Decisional Synchronized Codewords Problem (DSCP) as introduced in Definition 5 of [AAPS11].

Definition 5. *(Decisional Synchronized Codewords Problem (DSCP)) Consider an $[n,k]$-linear code $\mathcal{C}$. Let $\mathcal{S}$ be a sampler that takes $(\mathcal{C},T,L)$ as input and proceeds as follows.*

1) *Choose a random subset $I \subset \{1,\dots,n\}$ of size $|I| = T$. Randomly sample L pairwise distinct vectors $e_1,\dots,e_L \in \mathbb{F}_q^n$ with $\mathrm{supp}(e_i) \subseteq I^C$ for $i = 1,\dots,L$.*

2) *Sample L distinct codewords $w_1,\dots,w_L \in \mathcal{C}$. Compute the ciphertexts $c_i = w_i + e_i \in \mathbb{F}_q^n$, $i = 1,\dots,L$, and output $C = (c_1,\dots,c_L) \in \mathbb{F}_q^{Ln}$.*

Define two samplers $\mathcal{S}^{bad}$ and $\mathcal{S}^{good}$, where both output a sample (C,i). For both samplers, C is derived from the sampler $\mathcal{S}$. The index i is sampled either randomly among all error positions for $\mathcal{S}^{bad}$ or from all error-free positions for $\mathcal{S}^{good}$. The Decisional Synchronized Codewords Problem assumption holds if a polynomial-time adversary is not able to distinguish the output of $\mathcal{S}^{bad}$ and $\mathcal{S}^{good}$ with a probability significantly greater than $1/2$ (i.e., apart from a negligible probability).

Note that the DSCP is closely related to the Interleaved Decoding (ID) problem [PHL+22], where in the ID problem, an attacker aims to distinguish the output C from a matrix without the given interleaving structure.

Theorem 1. *[AAPS11, Theorem 3] Consider the SHE scheme with parameters $(\mathcal{C},\widehat{\mathcal{C}},T,L)$. Let $\mathcal{C}'$ be a code with $(\mathcal{C}')^{\star 2} \subseteq \mathcal{C}$ that has a at least one encryption of zero with only non-zero components and denote by $(\mathcal{C}')^{-}$ the code obtained from $\mathcal{C}'$ by removing one point from the support. The SHE scheme is secure if the $DSCP[\mathcal{C}',T,L]$ and the $DSCP[(\mathcal{C}')^{-},T,L]$ assumptions hold and if*

$$\frac{TL(n-T+3)}{q} = negl(s),$$

where $negl(\cdot)$ denotes a negligible function.

The authors initialize the scheme using punctured Reed-Muller codes, setting $\mathcal{C}' = \mathcal{P}_{\mathcal{S}}(\mathrm{RM}_q(m,\rho))$, $\mathcal{C} = \mathcal{P}_{\mathcal{S}}(\mathrm{RM}_q(m,2\rho))$, and $\widehat{\mathcal{C}} = \mathcal{C}^{\star\mu} = \mathcal{P}_{\mathcal{S}}(\mathrm{RM}_q(m,2\mu\rho))$ for some set $\mathcal{S} \subset \{1,\dots,q^m\}$ such that $\mathcal{S}^C$ contains an information set of $\widehat{\mathcal{C}}$ and whose size depends on the chosen security level. For security, they restrict the number of fresh ciphertexts to $L < n - T$ and fix parameters to resist the most powerful known attacks, information set decoding (e.g. compare [Pet10, PHL+22]) and the low weight dual codewords attack (e.g. see [MHT23]). In particular, they set $m = 3$ and $|I| = k^{\star\mu}$. Concrete parameters for various security levels are provided in Table 1.

4 Breaking the SHE Scheme

We propose a two-stage attack on the code-based SHE scheme presented in Section 3. First, an attacker can identify the error-free positions I by a partial key recovery attack with access to only a few ciphertexts and no further knowledge of the code. Especially, this shows that the DSCP assumption does not hold in the scheme's operational regime. The partial key recovery attack can be used to recover the messages under the additional assumption that an attacker has access to or can guess only a few plaintext-ciphertext pairs.

Both attack steps are based on the fact that an attacker with access to L fresh ciphertexts can create new noisy codewords with the same error support by componentwise multiplication. Let

$$N(\nu) = \min\left\{n, \binom{L+\nu-1}{\nu}\right\} \tag{1}$$

denote the number of ciphertexts, an attacker obtains in the power code $\mathcal{C}^{\star\nu}$ with dimension $k^{\star\nu}$ for $\nu = 1, \ldots, \mu$. Since we need at most n ciphertexts, we additionally bound $N(\nu)$ by n to reduce the computational cost. The following theorem presents our main result.

Theorem 2. *Let q and n be given, and suppose an attacker has access to L fresh ciphertexts encrypted under the same secret key in the code-based SHE scheme. If there exists a $\nu \in \{2, \ldots, \mu - 1\}$ with $N(\nu) > k^{\star\nu} + (n - T)$, then the error support can be recovered with a time complexity of $O(n^4)$ with very high success probability. If, in addition, L' plaintext-ciphertext pairs are known, where L' fulfills $L'k^{\star\nu} > T$, then the messages can be recovered with an additional effort of $O(n^3)$.*

The success probability of the attack is determined by the probabilities specified in Lemma 1, which follows below. The condition for the partial key recovery attack to be applicable in Theorem 2 translates to a minimum value L of fresh ciphertexts. For the case of Reed-Muller codes as proposed in [AAPS11], the minimal values of L are displayed in Table 1. As the table shows, even small numbers of ciphertexts can lead to successful attacks. For all considered parameter sets, only two known plaintext-ciphertext pairs are needed to decrypt the messages.

Due to space limitations, we provide a description of the attacks below but omit formal proofs for brevity.

4.1 Partial Key Recovery Attack

To recover the error support, an attacker can proceed as follows. Start with $\nu = 2$ and calculate all possible $N(\nu)$ codewords in the ν-th power product

code, where $N(\nu)$ is defined as in Equation (1). Stack the noisy codewords $c_1, \ldots, c_{N(\nu)}$ into a matrix

$$C^\nu = \begin{pmatrix} c_1 \\ \vdots \\ c_{N(\nu)} \end{pmatrix} \in \mathbb{F}_q^{N(\nu) \times n}.$$

If $rk(C^\nu) < N(\nu)$, then the current value of ν fulfills $N(\nu) > k^{\star\nu} + (n - T)$ with high probability. If $rk(C^\nu) = N(\nu)$, increase the value of ν and repeat the procedure. To identify the error-free positions I, the attacker studies the matrix C^ν. Delete one column of the matrix. If the deleted column is error-free, the rank of the modified matrix will remain unchanged with high probability. However, if the column contains errors, the rank will decrease by one with high probability. By iteratively going through all n columns in this manner, the attacker can identify I with high probability. The complexity of the attack is driven by the n rank calculations, each of them requiring $O(n^3)$ operations.
The following lemma specifies the success probability to distinguish between error-free and disturbed columns.

Lemma 1. *Let $\nu \in \{2, \ldots, \mu - 1\}$ be fixed. For $k^{\star\nu} < z < n$, let $p_{\mathcal{C}^{\star\nu}}(z)$ denote the probability that the generator matrix of $\mathcal{C}^{\star\nu}$ restricted to z randomly chosen columns contains an information set. Assume that $N(\nu) > k^{\star\nu} + (n - T)$ and let C^ν be a codeword matrix with $rk(C^\nu) < N(\nu)$. Denote with $C^\nu[i]$ for $i = 1, \ldots, n$ the matrix arising from C^ν by deleting column i. Then the following statements hold.*

1) *If $i \in I^C$ is a disturbed column, then $rk(C^\nu[i]) = rk(C^\nu) - 1$ with probability at least $(1 - q^{-1})$.*
2) *If $i \in I$, then we have $rk(C^\nu[i]) = rk(C^\nu)$ with probability at least $p_{\mathcal{C}^{\star\nu}}(T - 1)$.*

For the scheme to be secure, as displayed in Table 1, the field order q needs to be large, yielding a high success probability in part one of Lemma 1. Typically, the probability $p_{\mathcal{C}^{\star\nu}}(T-1)$ with $T-1 \gg k^{\star\nu}$ is very close to one likewise. However, its exact value depends on the specific codes employed. Given that a broad class of codes can be applied within the scheme and due to space limitations, we only provide a formula for random codes here, strengthening the reader's intuition on the probability. For random codes, the probability is lower bounded by

$$p_{\mathcal{C}^{\star\nu}}(T - 1) \geq \prod_{i=T-k^{\star\nu}}^{T-1} (1 - q^{-i}),$$

(e.g. see [FG15]). Since the probability is close to one for different codes as well, we can distinguish error columns and error-free ones with very high probability.

4.2 Message Recovery

Although the error support can be recovered, decoding the messages is not trivial without knowledge of the code itself. Due to the systematic encoding procedure and the puncturing, an attacker, unaware of the evaluation points P, is not able to interpolate the polynomials. Further, to obtain the messages from the polynomials, knowledge of the message support y is needed. For a successful attack on the messages, we therefore require a slightly stronger attack scenario. As before, we assume access to L fresh ciphertexts, where L is sufficiently large to enable the error support recovery attack as described in Section 4.1. Additionally, we assume that the attacker is able to guess or has access to L' plaintext-ciphertext pairs.

1) First, use the partial key recovery attack on the L fresh ciphertexts to obtain the error-free positions I.

2) From the known plaintext-ciphertext pairs, create L' encryptions of zero by subtracting each message from all components of the corresponding ciphertext.

3) An attacker can create new known plaintext-ciphertexts pairs in $\mathcal{C}^{\star 2}$ by multiplying the L' encryptions of zero with the unknown L ciphertexts or by multiplying two ciphertexts with known plaintexts. By repeated multiplication, one obtains $M(\nu)$ known plaintext-ciphertext pairs $(m_1, c_1), \ldots, (m_{M(\nu)}, c_{M(\nu)})$ in $\mathcal{C}^{\star\nu}$ for $\nu \in \{2, \ldots, \mu\}$.

4) Following the arguments in [AAPS11, Section 4.2] and using the knowledge of I from the partial key recovery attack, there is $v_{key} \in \mathbb{F}_q^T$ such that for every ciphertext $c \in \mathbb{F}_q^n$ with underlying plaintext $m \in \mathbb{F}_q$, decryption is equivalent to $c_I \cdot v_{key}^\top = m$. Hence, the attacker can consider the following system of linear equations

$$Cv_{key}^\top = \begin{pmatrix} (c_1)_I \\ \vdots \\ (c_{M(\nu)})_I \end{pmatrix} v_{key}^\top = \begin{pmatrix} m_1 \\ \vdots \\ m_{M(\nu)} \end{pmatrix} = D,$$

with known matrices C and D. If C has full column rank, the attacker can solve the linear system for v_{key} and use this decoding key to decode arbitrary ciphertexts. Let $\nu \in \{1, \ldots, \mu - 1\}$ be such that $N(\nu) > k^{\star\nu} + (n - T)$. Then the matrix C, whose rows are punctured codewords in $\mathcal{C}^{\star(\nu+1)}$, has full column rank with high probability if $L' k^{\star\nu} > T$.

For the attack to succeed, an attacker needs at least L' plaintext-ciphertext pairs. For Reed-Muller codes and the proposed parameters from [AAPS11], L' is equal to two for all parameter sets as displayed in Table 1. Hence,

in this case, only two plaintext-ciphertext pairs are sufficient to recover all messages.

Table 1: Example parameter choices for the SHE scheme in [AAPS11] for different security levels s and at most μ multiplications. Additionally, the minimal values of L and L' for the attack to be applicable are shown.

	$s = 80$			$s = 128$		
	$\mu = 5$	$\mu = 10$	$\mu = 15$	$\mu = 5$	$\mu = 10$	$\mu = 15$
Scheme parameters						
Field order q	2^{115}	2^{119}	2^{122}	2^{165}	2^{169}	2^{172}
Number of evaluation points n	60,176	448,017	1,475,597	114,189	862,336	2,853,838
Code dimension k	165	165	165	455	286	286
Number of error-free positions $\|I\|$	12,341	91,881	302,621	39,711	176,851	585,276
Polynomial degree ρ	4	4	4	6	5	5
Attack parameters						
Minimal value of L	33	14	11	38	15	12
Minimal value of L'	2	2	2	2	2	2

Applications for somewhat homomorphic encryption schemes typically involve either a rather complex function to be applied on the data and/or a huge amount of input data. Otherwise, there is no need for the client to outsource the computation using a costly encryption scheme. However, for both scenarios, we identify critical vulnerabilities in the scheme proposed by Armknecht et al. [AAPS11]. If the function is complex, the maximum number of multiplications μ on the ciphertexts will be large, which decreases the minimum value of ciphertexts an attacker needs to remove the error. On the other hand, having lots of input data, even for small values of μ, we can remove the error support. In both cases, we can recover the messages with little side knowledge.

5 On Two Different FHE Approaches

Inspired by [AAPS11], Challa and Gunta proposed two approaches for code-based symmetric FHE schemes based on binary Reed-Muller codes. Both approaches claim not only full homomorphism but also certain security guarantees. However, they suffer from major structural and security issues, on which we shortly want to comment here. Due to space limitations, we summarize their key ideas here, with detailed description and corresponding attacks deferred to the full version of this abstract.

5.1 The First Approach

In [CG16, CG21a], Challa and Gunta presented a first variant of an FHE scheme based on binary Reed-Muller codes. Therein, a plaintext $m \in \mathbb{F}_2^k$ is first encoded into a valid Reed-Muller codeword. Encryption then proceeds by obfuscating this codeword, without introducing errors, by embedding its

bits into a randomly chosen larger vector at user-selected, fixed positions. Critically, the decoding procedure described in the paper fails to recover the original message. As the homomorphic multiplication relies on this decoding procedure, it can not be replaced with a different decoding algorithm. Hence, the scheme is not fully homomorphic as claimed.

5.2 The Second Approach

In [CG21b] and [CG23], the authors proposed another FHE scheme based on binary Reed-Muller codes. The scheme supports an unlimited number of additions and componentwise multiplications. To encrypt a message $m \in \mathbb{F}_2^k$, the user calculates

$$Enc(m) = \sigma(m \times G_{RM} + E) \in \mathbb{F}_2^{k \times n},$$

where G_{RM} is the secret generator matrix of a binary $[n, k]$-linear Reed-Muller code. The matrix $E \in \mathbb{F}_2^{k \times n}$ is an error matrix, with its columns supported only on a particular secret subset $J \subset \{1, \ldots, n\}$ of all entries and σ is a secret scrambling map based on a permutation table that neither preserves columns nor rows. However, due to the specific vector-matrix multiplication employed, an attacker can exploit structural relationships between ciphertext components. This vulnerability allows us to recover the plaintext m up to a permutation of its entries when only a few ciphertexts are available. Additionally, if the attacker obtains or guesses few plaintext-ciphertext pairs, all messages can be uniquely identified with high probability.

6 Conclusion

We analyzed the security of three code-based approaches towards code-based FHE and demonstrated that all have critical weaknesses. Our primary focus was the somewhat homomorphic encryption scheme proposed by Armknecht et al. [AAPS11], which, although the first code-based scheme to support both addition and multiplication, suffers from a critical security vulnerability. We proved that an attacker can recover the error support and, if only few plaintext-ciphertext pairs are known, successfully decrypt ciphertexts in polynomial time. Additionally, we examined two later FHE constructions by Challa and Gunta [CG16, CG21b], which rely on Reed-Muller codes. Only the second approach derives a valid fully homomorphic encryption scheme. However, it is insecure as an attacker can recover the messages at least up to a fixed permutation.

Acknowledgments

This work has been supported by funding from Agentur für Innovation in der Cybersicherheit GmbH.

References

[AAPS11] F. Armknecht, D. Augot, L. Perret, and A.-R. Sadeghi. On constructing homomorphic encryption schemes from coding theory. In L. Chen, editor, *Cryptography and Coding*, pages 23–40, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[CCMZ15] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor. Squares of random linear codes. *IEEE Transactions on Information Theory*, 61(3):1159–1173, 2015.

[CG16] R. Challa and V. Gunta. Reed-Muller code based symmetric key fully homomorphic encryption scheme. In I. Ray, M. S. Gaur, M. Conti, D. Sanghi, and V. Kamakoti, editors, *Information Systems Security*, pages 499–508, Cham, 2016. Springer International Publishing.

[CG21a] R. Challa and V. Gunta. A modified symmetric key fully homomorphic encryption scheme based on Read-Muller code. *Baghdad Science Journal*, 18, 2021.

[CG21b] R. Challa and V. Gunta. Towards the construction of Reed-Muller code based symmetric key FHE. *Ingénierie des Systèmes d'Information*, 26(6):585–590, 2021.

[CG23] R. Challa and V. Gunta. Provable security of RM code based FHE scheme. *University of Bahrain Journal*, 2023.

[DGW70] P. Delsarte, J. M. Goethals, and F. J. Mac Williams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16(5):403–442, 1970.

[FG15] J. Fulman and L. Goldstein. Stein's method and the rank distribution of random matrices over finite fields. *The Annals of Probability*, 43(3):1274–1314, 2015.

[Gen09] C. Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009.

[McE78] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, pages 114–116, 1978.

[MHT23] C. Meyer-Hilfiger and J.-P. Tillich. Rigorous foundations for dual attacks in coding theory. In G. Rothblum and H. Wee, editors, *Theory of Cryptography*, pages 3–32, Cham, 2023. Springer Nature Switzerland.

[MSM+22] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. P. Fitzek, and N. Aaraj. Survey on fully homomorphic encryption, theory, and applications. *Proceedings of the IEEE*, 110(10):1572–1609, 2022.

[Mul54] D. E. Muller. Application of Boolean algebra to switching circuit design and to error detection. *Transactions of the I.R.E. Professional Group on Electronic Computers*, EC-3(3):6–12, 1954.

[Pet10] C. Peters. Information-set decoding for linear codes over Fq. In N. Sendrier, editor, *Post-Quantum Cryptography*, pages 81–94, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[PHL+22] A. Porwal, L. Holzbaur, H. Liu, J. Renner, A. Wachter-Zeh, and V. Weger. Interleaved Prange: A new generic decoder for interleaved codes. In J. H. Cheon and T. Johansson, editors, *Post-Quantum Cryptography*, pages 69–88, Cham, 2022. Springer International Publishing.

[RAD78] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of Secure Computation*, pages 169–179. Academic Press, 1978.

[Ree54] I. Reed. A class of multiple-error-correcting codes and the decoding scheme. *Transactions of the IRE Professional Group on Information Theory*, 4(4):38–49, 1954.

[RS60] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.