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

WCC 2026

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

[1]German Aerospace Center (DLR) - [2]Technical University of Munich

June 08, 2026

DLR

Fully Homomorphic Encryption (FHE)

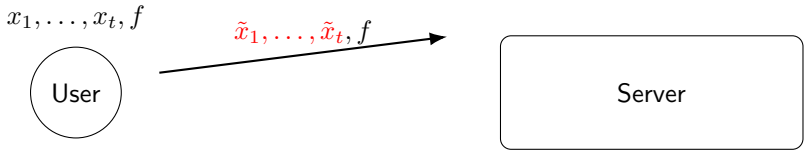
Goal: Perform arbitrary computations on encrypted data

Fully Homomorphic Encryption (FHE)

Goal: Perform arbitrary computations on encrypted data

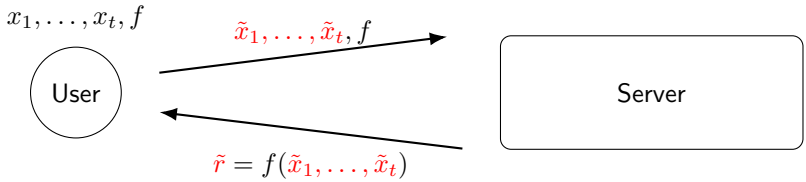
Fully Homomorphic Encryption (FHE)

Goal: Perform arbitrary computations on encrypted data



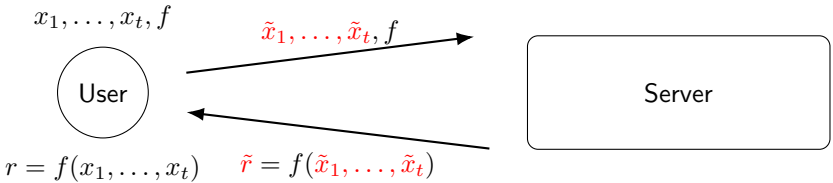
Fully Homomorphic Encryption (FHE)

Goal: Perform arbitrary computations on encrypted data



Fully Homomorphic Encryption (FHE)

Goal: Perform arbitrary computations on encrypted data



Fully Homomorphic Encryption (FHE)

- first construction of an FHE scheme, presented by Craig Gentry in 2009 [1]

1. C. Gentry. "A fully homomorphic encryption scheme". PhD thesis. Stanford University, 2009
2. F. Armknecht et al. "On Constructing Homomorphic Encryption Schemes from Coding Theory". In: *Cryptography and Coding*. Ed. by L. Chen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 23–40

Fully Homomorphic Encryption (FHE)

- first construction of an FHE scheme, presented by Craig Gentry in 2009 [1]
- many different approaches to construct FHE schemes, nearly all of them are lattice-based

1. C. Gentry. "A fully homomorphic encryption scheme". PhD thesis. Stanford University, 2009
2. F. Armknecht et al. "On Constructing Homomorphic Encryption Schemes from Coding Theory". In: *Cryptography and Coding*. Ed. by L. Chen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 23–40

Fully Homomorphic Encryption (FHE)

- first construction of an FHE scheme, presented by Craig Gentry in 2009 [1]
- many different approaches to construct FHE schemes, nearly all of them are lattice-based
- first SHE scheme based on coding theory, presented in 2011 by Armknecht et al. [2]

1. C. Gentry. "A fully homomorphic encryption scheme". PhD thesis. Stanford University, 2009
2. F. Armknecht et al. "On Constructing Homomorphic Encryption Schemes from Coding Theory". In: *Cryptography and Coding*. Ed. by L. Chen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 23–40

Fully Homomorphic Encryption (FHE)

- first construction of an FHE scheme, presented by Craig Gentry in 2009 [1]
- many different approaches to construct FHE schemes, nearly all of them are lattice-based
- first SHE scheme based on coding theory, presented in 2011 by Armknecht et al. [2]
- our contribution: identification of critical security vulnerabilities in the code-based scheme

1. C. Gentry. "A fully homomorphic encryption scheme". PhD thesis. Stanford University, 2009
2. F. Armknecht et al. "On Constructing Homomorphic Encryption Schemes from Coding Theory". In: *Cryptography and Coding*. Ed. by L. Chen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 23–40

Reed-Muller Codes

Notation:

- $\mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}$ the polynomial ring in t variables with degree at most ρ
- for a map f and a sequence of vectors $P = (p_1, \ldots, p_n)$, $\mathsf{Eval}_P(f) = (f(p_1), \ldots, f(p_n))$

Reed-Muller Codes

Notation:

- $\mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}$ the polynomial ring in t variables with degree at most ρ
- for a map f and a sequence of vectors $P = (p_1, \ldots, p_n)$, $\mathsf{Eval}_P(f) = (f(p_1), \ldots, f(p_n))$

Definition

The q-**ary Reed-Muller code** of order ρ is defined as

$$\mathcal{C} = RM_q(t, \rho) = \{\mathsf{Eval}_{\mathbb{F}_q^t}(f) \mid f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}\}.$$

Reed-Muller Codes

Notation:

- $\mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}$ the polynomial ring in t variables with degree at most ρ
- for a map f and a sequence of vectors $P = (p_1, \ldots, p_n)$, $\mathsf{Eval}_P(f) = (f(p_1), \ldots, f(p_n))$

Definition

The q-**ary Reed-Muller code** of order ρ is defined as

$$\mathcal{C} = RM_q(t, \rho) = \{\mathsf{Eval}_{\mathbb{F}_q^t}(f) \mid f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}\}.$$

For a set $S \subseteq \{1, \ldots, n\}$, $n = q^t$, the **punctured RM code** is

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

Evaluation Codes

Definition

Let $\mathcal{X}$ be a geometric object 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 tuple of distinct points. The **evaluation code** with respect to $\mathcal{L}$ and P is given by $\mathcal{C} = \{\mathrm{Eval}_P(f) : f \in \mathcal{L}\} \subseteq \mathbb{F}_q^n$.

Evaluation Codes

Definition

Let $\mathcal{X}$ be a geometric object 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 tuple of distinct points. The **evaluation code** with respect to $\mathcal{L}$ and P is given by $\mathcal{C} = \{\mathrm{Eval}_P(f) : f \in \mathcal{L}\} \subseteq \mathbb{F}_q^n$.

- $\mathcal{X} = \mathbb{F}_q^t$

Evaluation Codes

Definition

Let $\mathcal{X}$ be a geometric object 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 tuple of distinct points. The **evaluation code** with respect to $\mathcal{L}$ and P is given by $\mathcal{C} = \{\mathrm{Eval}_P(f) : f \in \mathcal{L}\} \subseteq \mathbb{F}_q^n$.

- $\mathcal{X} = \mathbb{F}_q^t$
- $\mathcal{L} = \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}$

Evaluation Codes

Definition

Let $\mathcal{X}$ be a geometric object 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 tuple of distinct points. The **evaluation code** with respect to $\mathcal{L}$ and P is given by $\mathcal{C} = \{\mathrm{Eval}_P(f) : f \in \mathcal{L}\} \subseteq \mathbb{F}_q^n$.

- $\mathcal{X} = \mathbb{F}_q^t$
- $\mathcal{L} = \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}$
- $n = q^t$

Evaluation Codes

Definition

Let $\mathcal{X}$ be a geometric object 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 tuple of distinct points. The **evaluation code** with respect to $\mathcal{L}$ and P is given by $\mathcal{C} = \{\mathrm{Eval}_P(f) : f \in \mathcal{L}\} \subseteq \mathbb{F}_q^n$.

- $\mathcal{X} = \mathbb{F}_q^t$
- $\mathcal{L} = \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho}$
- $n = q^t$
- $\mathcal{C} = RM_q(t, \rho)$

Power Codes

For $x, y \in \mathbb{F}_q^n$, let $x * y \in \mathbb{F}_q^n$ denote the componentwise multiplication.

Power Codes

For $x, y \in \mathbb{F}_q^n$, let $x * y \in \mathbb{F}_q^n$ denote the componentwise multiplication.

Definition

Let $\mathcal{C}$ be an $[n, k]$-linear code. The μ-**th power product code** is defined as

$$\mathcal{C}^{(\mu)} = \langle \{ c_1 * c_2 * \cdots * c_\mu \mid c_i \in \mathcal{C} \} \rangle.$$

Power Codes

For $x, y \in \mathbb{F}_q^n$, let $x * y \in \mathbb{F}_q^n$ denote the componentwise multiplication.

Definition

Let $\mathcal{C}$ be an $[n, k]$-linear code. The μ-**th power product code** is defined as

$$\mathcal{C}^{(\mu)} = \langle \{ c_1 * c_2 * \cdots * c_\mu \mid c_i \in \mathcal{C} \} \rangle.$$

Example

$\mathcal{C} = \{(1, 2), (2, 1), (0, 0)\} \subset \mathbb{F}_3^2$

Power Codes

For $x, y \in \mathbb{F}_q^n$, let $x * y \in \mathbb{F}_q^n$ denote the componentwise multiplication.

Definition

Let $\mathcal{C}$ be an $[n, k]$-linear code. The μ-**th power product code** is defined as

$$\mathcal{C}^{(\mu)} = \langle \{ c_1 * c_2 * \cdots * c_\mu \mid c_i \in \mathcal{C} \} \rangle.$$

Example

$\mathcal{C} = \{(1, 2), (2, 1), (0, 0)\} \subset \mathbb{F}_3^2$

$\mathcal{C}^{(2)} = \{(1, 1), (2, 2), (0, 0)\}$

Multiplicative Codes

For a code-based (F)HE Scheme, we need

Multiplicative Codes

For a code-based (F)HE Scheme, we need

- sum of two codewords is again a codeword

Multiplicative Codes

For a code-based (F)HE Scheme, we need

- sum of two codewords is again a codeword ✓

Multiplicative Codes

For a code-based (F)HE Scheme, we need

- sum of two codewords is again a codeword ✓
- product of two codewords is again a codeword

Multiplicative Codes

For a code-based (F)HE Scheme, we need

- sum of two codewords is again a codeword ✓
- product of two codewords is again a codeword ❓

Multiplicative Codes

For a code-based (F)HE Scheme, we need

- sum of two codewords is again a codeword ✓
- product of two codewords is again a codeword ❓

Definition

Let $\mathcal{C}$ be an evaluation code with evaluation points P. The code is called μ-**multiplicative** if there exists an evaluation code $\widehat{\mathcal{C}}$ with evaluation points P such that $\mathcal{C}^{(\ell)} \subseteq \widehat{\mathcal{C}}$ for all $\ell \leq \mu$.

Multiplicative Codes

For a code-based (F)HE Scheme, we need

- sum of two codewords is again a codeword ✓
- product of two codewords is again a codeword ❓

Definition

Let $\mathcal{C}$ be an evaluation code with evaluation points P. The code is called μ-**multiplicative** if there exists an evaluation code $\widehat{\mathcal{C}}$ with evaluation points P such that $\mathcal{C}^{(\ell)} \subseteq \widehat{\mathcal{C}}$ for all $\ell \leq \mu$.

For $\mu \leq q$ there exist RM codes that are μ-multiplicative.

Multiplicative Codes

For a code-based (F)HE Scheme, we need

- sum of two codewords is again a codeword ✓
- product of two codewords is again a codeword ❓

Definition

Let $\mathcal{C}$ be an evaluation code with evaluation points P. The code is called μ-**multiplicative** if there exists an evaluation code $\widehat{\mathcal{C}}$ with evaluation points P such that $\mathcal{C}^{(\ell)} \subseteq \widehat{\mathcal{C}}$ for all $\ell \leq \mu$.

For $\mu \leq q$ there exist RM codes that are μ-multiplicative.

$\mathcal{C} = RM_q(m, \rho)$ and $\widehat{\mathcal{C}} = RM_q(m, \mu\rho)$

Code-based SHE Scheme - Setup

Code-based SHE Scheme - Setup

- maximal number of multiplications μ and encryptions L

Code-based SHE Scheme - Setup

- maximal number of multiplications μ and encryptions L
- a punctured, μ-multiplicative RM code $\mathcal{C} = \mathcal{P}_S(RM_q(t, \rho))$

Code-based SHE Scheme - Setup

- maximal number of multiplications μ and encryptions L
- a punctured, μ-multiplicative RM code $\mathcal{C} = \mathcal{P}_S(RM_q(t, \rho))$
- $P = (p_1, \ldots, p_n)$ the corresponding evaluation points

Code-based SHE Scheme - Setup

- maximal number of multiplications μ and encryptions L
- a punctured, μ-multiplicative RM code $\mathcal{C} = \mathcal{P}_S(RM_q(t, \rho))$
- $P = (p_1, \ldots, p_n)$ the corresponding evaluation points
- random vector $y \in \mathbb{F}_q^t$, $y \neq p_i$

Code-based SHE Scheme - Setup

- maximal number of multiplications μ and encryptions L
- a punctured, μ-multiplicative RM code $\mathcal{C} = \mathcal{P}_S(RM_q(t, \rho))$
- $P = (p_1, \ldots, p_n)$ the corresponding evaluation points
- random vector $y \in \mathbb{F}_q^t$, $y \neq p_i$
- a set $I \subset \{1, \ldots, n\}$

Code-based SHE Scheme - Setup

- maximal number of multiplications μ and encryptions L
- a punctured, μ-multiplicative RM code $\mathcal{C} = \mathcal{P}_S(RM_q(t, \rho))$
- $P = (p_1, \ldots, p_n)$ the corresponding evaluation points
- random vector $y \in \mathbb{F}_q^t$, $y \neq p_i$
- a set $I \subset \{1, \ldots, n\}$

🔑 (P, y, I)

Code-based SHE Scheme

🔑 (P, y, I)

Code-based SHE Scheme

🔑 (P, y, I)

✉ message $m \in \mathbb{F}_q$

Code-based SHE Scheme

(P, y, I)

message $m \in \mathbb{F}_q$

$$\mathcal{L}_m = \{f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho} \mid f(y) = m\}$$

Code-based SHE Scheme

- (P, y, I)
- message $m \in \mathbb{F}_q$

$$\mathcal{L}_m = \{f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho} \mid f(y) = m\}$$

$$m \xrightarrow{f \in \mathcal{L}_m} w = (f(p_1), \ldots, f(p_n))$$

Code-based SHE Scheme

(P, y, I)

message $m \in \mathbb{F}_q$

$$\mathcal{L}_m = \{f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho} \mid f(y) = m\}$$

$$m \xrightarrow{f \in \mathcal{L}_m} w = (f(p_1), \ldots, f(p_n)) \xrightarrow{e \in \mathbb{F}_q^n, e_I = 0} (c = w + e, 1)$$

Code-based SHE Scheme

(P, y, I)

message $m \in \mathbb{F}_q$

$$\mathcal{L}_m = \{f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho} \mid f(y) = m\}$$

$$m \xrightarrow{f \in \mathcal{L}_m} w = (f(p_1), \ldots, f(p_n)) \xrightarrow{e \in \mathbb{F}_q^n, e_I = 0} (c = w + e, 1)$$

$$(\tilde{c}, \gamma), \gamma \leq \mu$$

$$(c_1, \gamma_1) + (c_2, \gamma_2) = (c_1 + c_2, \max\{\gamma_1, \gamma_2\})$$

$$(c_1, \gamma_1) \cdot (c_2, \gamma_2) = (c_1 * c_2, \gamma_1 + \gamma_2)$$

Code-based SHE Scheme

(P, y, I)

message $m \in \mathbb{F}_q$

$$\mathcal{L}_m = \{f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho} \mid f(y) = m\}$$

$$m \xrightarrow{f \in \mathcal{L}_m} w = (f(p_1), \ldots, f(p_n)) \xrightarrow{e \in \mathbb{F}_q^n, e_I = 0} (c = w + e, 1)$$

$$\tilde{w} = (\tilde{f}(p_1), \ldots, \tilde{f}(p_n)) \xleftarrow{\tilde{c}_I \text{ error-free}} (\tilde{c}, \gamma), \gamma \leq \mu$$

$$(c_1, \gamma_1) + (c_2, \gamma_2) = (c_1 + c_2, \max\{\gamma_1, \gamma_2\})$$

$$(c_1, \gamma_1) \cdot (c_2, \gamma_2) = (c_1 * c_2, \gamma_1 + \gamma_2)$$

Code-based SHE Scheme

(P, y, I)

message $m \in \mathbb{F}_q$

$$\mathcal{L}_m = \{f \in \mathbb{F}_q[x_1, \ldots, x_t]_{\leq \rho} \mid f(y) = m\}$$

$$m \xrightarrow{f \in \mathcal{L}_m} w = (f(p_1), \ldots, f(p_n)) \xrightarrow{e \in \mathbb{F}_q^n, e_I = 0} (c = w + e, 1)$$

$$\tilde{m} \xleftarrow{\tilde{f}(y) = \tilde{m}} \tilde{w} = (\tilde{f}(p_1), \ldots, \tilde{f}(p_n)) \xleftarrow{\tilde{c}_I \text{ error-free}} (\tilde{c}, \gamma), \gamma \leq \mu$$

$$(c_1, \gamma_1) + (c_2, \gamma_2) = (c_1 + c_2, \max\{\gamma_1, \gamma_2\})$$

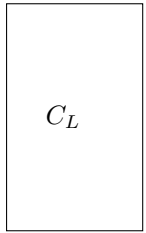
$$(c_1, \gamma_1) \cdot (c_2, \gamma_2) = (c_1 * c_2, \gamma_1 + \gamma_2)$$

Partial Key Recovery

access to (at most) L ciphertexts $c_1, \ldots, c_L$

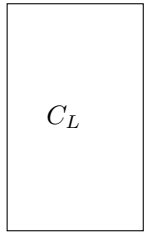
Partial Key Recovery

access to (at most) L ciphertexts $c_1, \ldots, c_L \Rightarrow C_L = \begin{pmatrix} c_1 \\ \vdots \\ c_L \end{pmatrix} \in \mathbb{F}_q^{L \times n}$



Partial Key Recovery

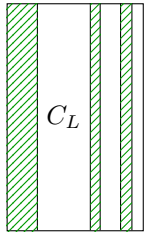
access to (at most) L ciphertexts $c_1, \ldots, c_L \Rightarrow C_L = \begin{pmatrix} c_1 \\ \vdots \\ c_L \end{pmatrix} \in \mathbb{F}_q^{L \times n}$



(P, y, I)

Partial Key Recovery

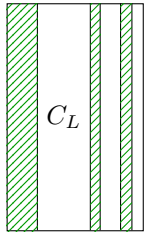
access to (at most) L ciphertexts $c_1, \ldots, c_L \Rightarrow C_L = \begin{pmatrix} c_1 \\ \vdots \\ c_L \end{pmatrix} \in \mathbb{F}_q^{L \times n}$



(P, y, I)

Partial Key Recovery

access to (at most) L ciphertexts $c_1, \ldots, c_L \Rightarrow C_L = \begin{pmatrix} c_1 \\ \vdots \\ c_L \end{pmatrix} \in \mathbb{F}_q^{L \times n}$



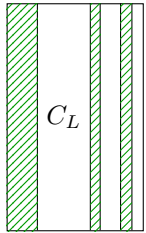
(P, y, I)

$c_i * c_j$

Partial Key Recovery

access to (at most) L ciphertexts $c_1, \ldots, c_L \Rightarrow C_L = \begin{pmatrix} c_1 \\ \vdots \\ c_L \end{pmatrix} \in \mathbb{F}_q^{L \times n}$

create more noisy codewords $c_{L+1}, \ldots, c_{\tilde{L}}$



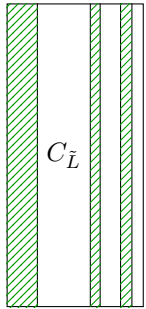
(P, y, I)

$c_i * c_j$

Partial Key Recovery

access to (at most) L ciphertexts $c_1, \ldots, c_L \Rightarrow C_L = \begin{pmatrix} c_1 \\ \vdots \\ c_L \end{pmatrix} \in \mathbb{F}_q^{L \times n}$

create more noisy codewords $c_{L+1}, \ldots, c_{\tilde{L}}$



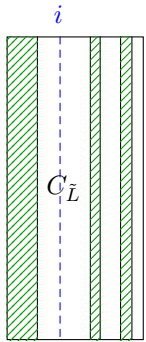
(P, y, I)

$c_i * c_j$

Partial Key Recovery

access to (at most) L ciphertexts $c_1, \ldots, c_L \Rightarrow C_L = \begin{pmatrix} c_1 \\ \vdots \\ c_L \end{pmatrix} \in \mathbb{F}_q^{L \times n}$

create more noisy codewords $c_{L+1}, \ldots, c_{\tilde{L}}$



(P, y, I)

$c_i * c_j$

$C_{\tilde{L}}[i]$

Partial Key Recovery

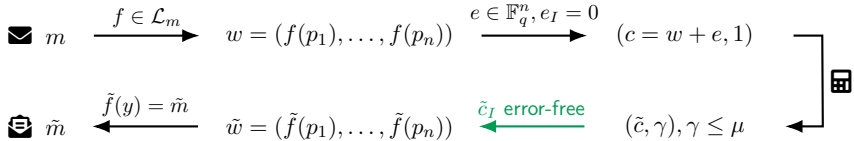
Lemma

If the number of ciphertexts $\tilde{L}$ is large enough, then it holds

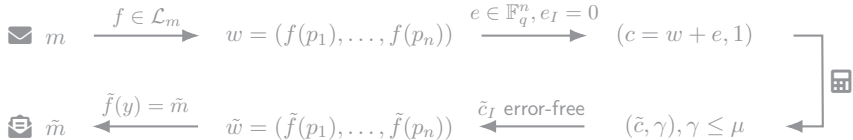
- *if $i \notin I$, then* $\mathsf{rk}(C_{\tilde{L}}[i]) = \mathsf{rk}(C_{\tilde{L}}) - 1$ *with high probability,*
- *if $i \in I$, then* $\mathsf{rk}(C_{\tilde{L}}[i]) = \mathsf{rk}(C_{\tilde{L}})$ *with high probability.*

So, the error support can be recovered with a time complexity of $\mathcal{O}(n^4)$ with high probability.

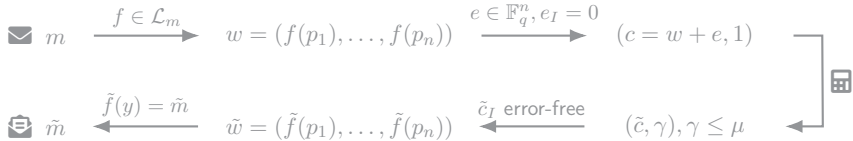
Alternative Description



Alternative Description

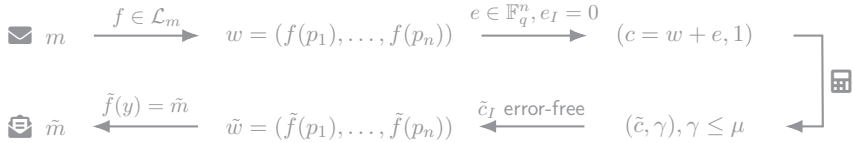


Alternative Description



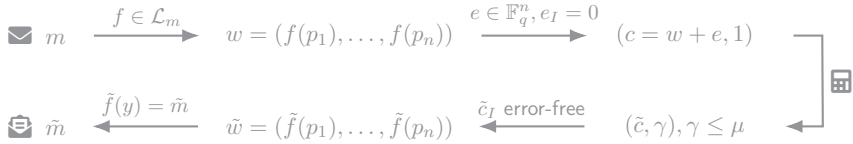
- $V_0 \subset \mathbb{F}_q^n$ subspace containing all encryptions of 0

Alternative Description



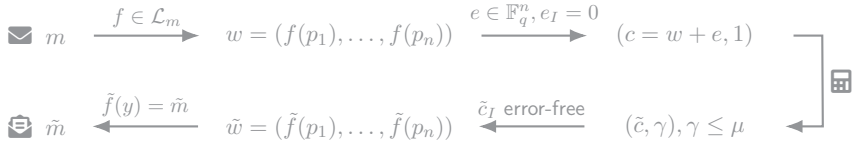
- $V_0 \subset \mathbb{F}_q^n$ subspace containing all encryptions of 0
- $c^* \in \mathbb{F}_q^n$ an arbitrary encryption of 1

Alternative Description



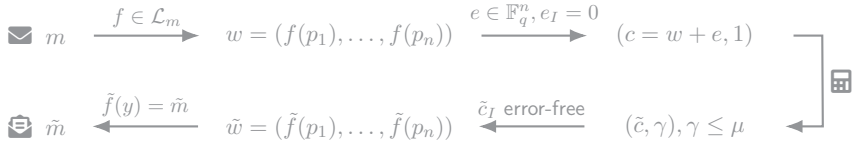
- $V_0 \subset \mathbb{F}_q^n$ subspace containing all encryptions of 0
- $c^* \in \mathbb{F}_q^n$ an arbitrary encryption of 1
- $V_{\text{err}} \subset \mathbb{F}_q^n$ subspace of error vectors

Alternative Description



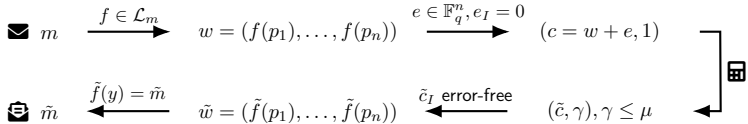
- $V_0 \subset \mathbb{F}_q^n$ subspace containing all encryptions of 0
- $c^* \in \mathbb{F}_q^n$ an arbitrary encryption of 1
- $V_{\text{err}} \subset \mathbb{F}_q^n$ subspace of error vectors
- encryption of $m \in \mathbb{F}_q$ is $c = v_0 + m \cdot c^* + v_e$

Alternative Description

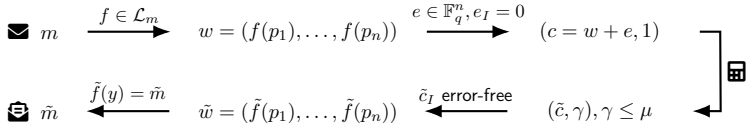


- $V_0 \subset \mathbb{F}_q^n$ subspace containing all encryptions of 0
- $c^* \in \mathbb{F}_q^n$ an arbitrary encryption of 1
- $V_{\text{err}} \subset \mathbb{F}_q^n$ subspace of error vectors
- encryption of $m \in \mathbb{F}_q$ is $c = v_0 + m \cdot c^* + v_e$
- $\exists\, v_{\text{key}} \in \mathbb{F}_q^n$ such that $m = c \cdot v_{\text{key}}^\top$

Message Recovery

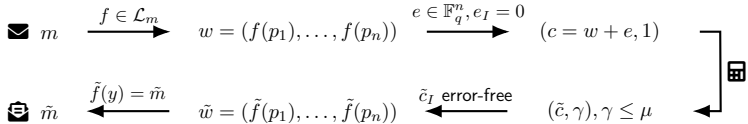


Message Recovery



assume we know L' plaintext-ciphertext pairs m_i, c_i

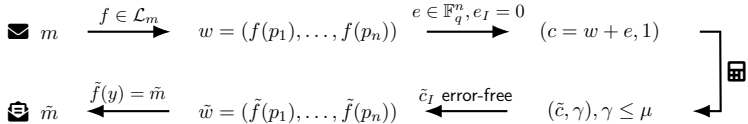
Message Recovery



assume we know L' plaintext-ciphertext pairs m_i, c_i

1. Obtain I using the partial key recovery attack

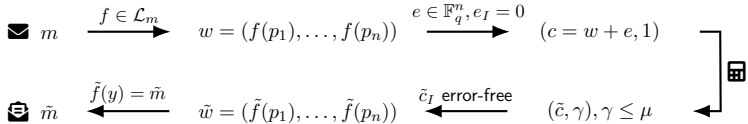
Message Recovery



assume we know L' plaintext-ciphertext pairs m_i, c_i

1. Obtain I using the partial key recovery attack
2. Create L' encryptions of 0 by computing $c_i' = c_i - \overbrace{(m_i, \ldots, m_i)}^{n \text{ times}}$

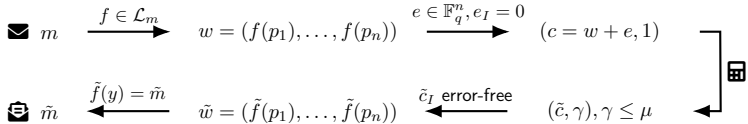
Message Recovery



assume we know L' plaintext-ciphertext pairs m_i, c_i

1. Obtain I using the partial key recovery attack
2. Create L' encryptions of 0 by computing $c_i' = c_i - \overbrace{(m_i, \ldots, m_i)}^{n \text{ times}}$
   $\mathcal{L}_0 = \{f - m \mid f \in \mathcal{L}_m\}$

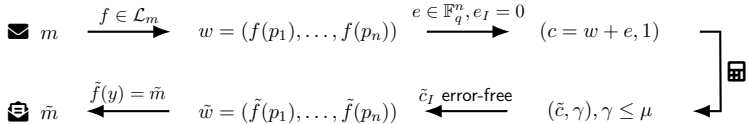
Message Recovery



assume we know L' plaintext-ciphertext pairs m_i, c_i

1. Obtain I using the partial key recovery attack
2. Create L' encryptions of 0 by computing $c_i' = c_i - \overbrace{(m_i, \ldots, m_i)}^{n \text{ times}}$
   $\mathcal{L}_0 = \{f - m \mid f \in \mathcal{L}_m\}$
3. Create more encryptions of 0

Message Recovery



assume we know L' plaintext-ciphertext pairs m_i, c_i

1. Obtain I using the partial key recovery attack
2. Create L' encryptions of 0 by computing $c_i' = c_i - \overbrace{(m_i, \ldots, m_i)}^{n \text{ times}}$
   $\mathcal{L}_0 = \{f - m \mid f \in \mathcal{L}_m\}$
3. Create more encryptions of 0
4. We know there exists v_{key} such that $c_I \cdot v_{\text{key}}^\top = m$

Message Recovery

assume we know L' plaintext-ciphertext pairs m_i, c_i

1. Obtain I using the partial key recovery attack
2. Create L' encryptions of 0 by computing $c'_i = (c_{i1}, \ldots, c_{in}) - (m_i, \ldots, m_i)$
3. Create more encryptions of 0
4. We know there exists v_{key} such that $c_I \cdot v_{\text{key}}^\top = m$

Message Recovery

assume we know L' plaintext-ciphertext pairs m_i, c_i

1. Obtain I using the partial key recovery attack
2. Create L' encryptions of 0 by computing $c'_i = (c_{i1}, \ldots, c_{in}) - (m_i, \ldots, m_i)$
3. Create more encryptions of 0
4. We know there exists v_{key} such that $c_I \cdot v_{\text{key}}^\top = m$
5. Solve the linear system $\begin{pmatrix} (\tilde{c}_1)_I \\ \vdots \\ (\tilde{c}_\lambda)_I \end{pmatrix} v_{\text{key}}^\top = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ to find v_{key}

Message Recovery

Theorem

Assume that we already recovered the set I.
If the number of known plaintext-ciphertext pairs L' is large enough, the messages can be recovered with a time complexity of $\mathcal{O}(n^3)$.

Parameters

	$s = 80$			$s = 128$		
	$\mu = 5$	$\mu = 10$	$\mu = 15$	$\mu = 5$	$\mu = 10$	$\mu = 15$
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 $\lvert I\rvert$	$12,341$	$91,881$	$302,621$	$39,711$	$176,851$	$585,276$
Polynomial degree ρ	4	4	4	6	5	5
Attack parameters						
Minimal value of L						
Minimal value of L'						

Parameters

	$s = 80$			$s = 128$		
	$\mu = 5$	$\mu = 10$	$\mu = 15$	$\mu = 5$	$\mu = 10$	$\mu = 15$
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 $\lvert I\rvert$	$12,341$	$91,881$	$302,621$	$39,711$	$176,851$	$585,276$
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'						

Parameters

	$s = 80$			$s = 128$		
	$\mu = 5$	$\mu = 10$	$\mu = 15$	$\mu = 5$	$\mu = 10$	$\mu = 15$
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 $\lvert I\rvert$	$12,341$	$91,881$	$302,621$	$39,711$	$176,851$	$585,276$
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**

Two additional FHE Approaches

Two FHE schemes based on binary RM codes by Challa and Gunta: [3]

3. R. Challa and V. Gunta. "Reed-Muller Code Based Symmetric Key Fully Homomorphic Encryption Scheme". In: *Information Systems Security*. Springer International Publishing, 2016
R. Challa and V. Gunta. "Provable Security of RM Code Based FHE Scheme". In: *University of Bahrain Journal* (2023)

Two additional FHE Approaches

Two FHE schemes based on binary RM codes by Challa and Gunta: [3]

- decoding procedure of one scheme appears to be incorrect

3. R. Challa and V. Gunta. "Reed-Muller Code Based Symmetric Key Fully Homomorphic Encryption Scheme". In: *Information Systems Security*. Springer International Publishing, 2016
R. Challa and V. Gunta. "Provable Security of RM Code Based FHE Scheme". In: *University of Bahrain Journal* (2023)

Two additional FHE Approaches

Two FHE schemes based on binary RM codes by Challa and Gunta: [3]

- decoding procedure of one scheme appears to be incorrect
- recovery of plaintexts $m \in \mathbb{F}_2^k$ in the other scheme is possible

3. R. Challa and V. Gunta. "Reed-Muller Code Based Symmetric Key Fully Homomorphic Encryption Scheme". In: *Information Systems Security*. Springer International Publishing, 2016
R. Challa and V. Gunta. "Provable Security of RM Code Based FHE Scheme". In: *University of Bahrain Journal* (2023)

Two additional FHE Approaches

Two FHE schemes based on binary RM codes by Challa and Gunta: [3]

- decoding procedure of one scheme appears to be incorrect
- recovery of plaintexts $m \in \mathbb{F}_2^k$ in the other scheme is possible

$$m \times G_{RM} = \begin{pmatrix} m_1 g_{1,1} & \dots & m_1 g_{1,n} \\ & \vdots & \\ m_k g_{k,1} & \dots & m_k g_{k,n} \end{pmatrix} \in \mathbb{F}_2^{k \times n}$$

3. R. Challa and V. Gunta. "Reed-Muller Code Based Symmetric Key Fully Homomorphic Encryption Scheme". In: *Information Systems Security*. Springer International Publishing, 2016
R. Challa and V. Gunta. "Provable Security of RM Code Based FHE Scheme". In: *University of Bahrain Journal* (2023)

Two additional FHE Approaches

Two FHE schemes based on binary RM codes by Challa and Gunta: [3]

- decoding procedure of one scheme appears to be incorrect
- recovery of plaintexts $m \in \mathbb{F}_2^k$ in the other scheme is possible

$$\text{Enc}(m) = \sigma(m \times G_{RM} + E)$$

$$m \times G_{RM} = \begin{pmatrix} m_1 g_{1,1} & \dots & m_1 g_{1,n} \\ & \vdots & \\ m_k g_{k,1} & \dots & m_k g_{k,n} \end{pmatrix} \in \mathbb{F}_2^{k \times n}$$

3. R. Challa and V. Gunta. "Reed-Muller Code Based Symmetric Key Fully Homomorphic Encryption Scheme". In: *Information Systems Security*. Springer International Publishing, 2016
R. Challa and V. Gunta. "Provable Security of RM Code Based FHE Scheme". In: *University of Bahrain Journal* (2023)

Thank you for your attention!