Somewhat Homomorphic Encryption based on Random Ideal Codes

Carlos Aguilar-Melchor[1], **Victor Dyseryn**[2], Philippe Gaborit[3]

[1]Sandbox AQ
[2]Telecom Paris, France
[3]XLIM, Université de Limoges, France

July 14, 2025

Outline

Outline

What is Homomorphic Encryption?

Public-key version

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$
- $\mathsf{Enc}(m, \mathsf{pk}) \to \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) \to m$
- $\mathsf{Eval}(f, \mathsf{ct}_1, \mathsf{ct}_2) \to \mathsf{ct}$

Proposition (Correctness)

$$\mathsf{Dec}(\mathsf{Eval}(f, \mathsf{Enc}(m_1, \mathsf{pk}), \mathsf{Enc}(m_2, \mathsf{pk})), \mathsf{sk}) = f(m_1, m_2)$$

What is Homomorphic Encryption?

- $f \in \{+, \times\} \rightarrow$ partial homomorphic encryption (RSA)
- $f \in \mathbb{F}_d[X] \rightarrow$ somewhat homomorphic encryption [BGN05]
- $f \in \mathbb{F}[X] \rightarrow$ fully homomorphic encryption [Gen09]

Noisy ciphertexts

$$\mathsf{ct}_1 = \boldsymbol{A}\boldsymbol{m}_1 + \boldsymbol{e}_1$$
$$\mathsf{ct}_2 = \boldsymbol{A}\boldsymbol{m}_2 + \boldsymbol{e}_2$$

$$\mathsf{Eval}(+, \mathsf{ct}_1, \mathsf{ct}_2) = \boldsymbol{A}(\boldsymbol{m}_1 + \boldsymbol{m}_2) + \underbrace{\boldsymbol{e}_1 + \boldsymbol{e}_2}_{\text{double noise}}$$

In general:

$$\mathsf{Eval}(f, \mathsf{Enc}(m_1, \mathsf{pk}), \mathsf{Enc}(m_2, \mathsf{pk})) \neq \mathsf{Enc}(f(m_1, m_2), \mathsf{pk}).$$

Bootstrapping: how to reduce ciphertext noise

$$(\mathsf{pk}_1, \mathsf{sk}_1) = \mathsf{KeyGen}(1^\lambda)$$
$$\mathsf{ct}_0 \approx \mathsf{Enc}(m, \mathsf{pk}_1)$$

$$(\mathsf{pk}_2, \mathsf{sk}_2) = \mathsf{KeyGen}(1^\lambda)$$
$$\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{ct}_0, \mathsf{pk}_2) \approx \mathsf{Enc}(\mathsf{Enc}(m, \mathsf{pk}_1), \mathsf{pk}_2)$$
$$\mathsf{ct}_2 = \mathsf{Enc}(\mathsf{sk}_1, \mathsf{pk}_2)$$

$$\mathsf{Eval}(\mathsf{Dec}(\cdot,\cdot), \mathsf{ct}_1, \mathsf{ct}_2) = \ ?$$

Bootstrapping: how to reduce ciphertext noise

$$\mathsf{ct}_0 \approx \mathsf{Enc}(m, \mathsf{pk}_1)$$
$$\mathsf{ct}_1 = \mathsf{Enc}(\mathsf{ct}_0, \mathsf{pk}_2)$$
$$\mathsf{ct}_2 = \mathsf{Enc}(\mathsf{sk}_1, \mathsf{pk}_2)$$

$$\mathsf{Dec}(\mathsf{Eval}(\mathsf{Dec}(\cdot,\cdot), \mathsf{ct}_1, \mathsf{ct}_2), \mathsf{sk}_2) = \mathsf{Dec}(\mathsf{ct}_0, \mathsf{sk}_1) = m$$

$$\big(\mathsf{Eval}(\mathsf{Dec}(\cdot,\cdot), \mathsf{ct}_1, \mathsf{ct}_2) \approx \mathsf{Enc}(m, \mathsf{pk}_2)\big)$$

History of fully homomorphic encryption

There has been a burst of activity in the last decade:

- 2009: Gentry's first FHE [Gen09]
- 2010-2015: Practical somewhat homomorphic encryption
- 2016: TFHE [CGGI16], bootstrapping below 100ms
- 2016-present: remarkable progress

... but most of existing constructions are based on **structured lattices**.

Outline

What is Homomorphic Encryption?

Secret-key version

- $\mathsf{KeyGen}(1^\lambda) \to \mathsf{sk}$
- $\mathsf{Enc}(m, \mathsf{sk}) \to \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) \to m$
- $\mathsf{Eval}(f, \mathsf{ct}_1, \mathsf{ct}_2) \to \mathsf{ct}$

Proposition (Correctness)

$$\mathsf{Dec}(\mathsf{Eval}(f, \mathsf{Enc}(m_1, \mathsf{sk}), \mathsf{Enc}(m_2, \mathsf{sk})), \mathsf{sk}) = f(m_1, m_2)$$

Lattice-based HE (secret-key version)

$$\mathsf{sk} = \boldsymbol{s} \in \mathbb{F}_q^k$$

$$\mathsf{Enc}(m, \mathsf{sk}) = (\boldsymbol{A} \in \mathbb{F}_q^{n \times k}, \boldsymbol{v} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + \mathit{Encode}(m))$$
$$\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) = \mathit{Decode}(\boldsymbol{v} - \boldsymbol{A}\boldsymbol{s})$$

Usually: $\mathit{Encode}(m) = m \mod p$ (with $p < q$)

The LWE assumption

$$\boldsymbol{A}, \begin{pmatrix} \\ \boldsymbol{A} \\ \\ \end{pmatrix} \begin{pmatrix} \\ \boldsymbol{s} \\ \\ \end{pmatrix} + \begin{pmatrix} \\ \boldsymbol{e} \\ \\ \end{pmatrix} \approx \boldsymbol{A}, \begin{pmatrix} \\ \boldsymbol{y} \\ \\ \end{pmatrix}$$

$$\boldsymbol{A} \hookleftarrow \mathbb{F}_q^{k \times n}$$
$$\boldsymbol{s} \hookleftarrow \mathbb{F}_q^{k}$$
$$\boldsymbol{e} \hookleftarrow \chi_{q,n,\sigma}$$

$$\boldsymbol{A} \hookleftarrow \mathbb{F}_q^{k \times n}$$
$$\boldsymbol{y} \hookleftarrow \mathbb{F}_q^{n}$$

Linear homomorphism

$$\mathsf{ct}_1 = (\boldsymbol{A}_1, \boldsymbol{A}_1\boldsymbol{s} + \boldsymbol{e}_1 + \mathit{Encode}(m_1))$$
$$\mathsf{ct}_2 = (\boldsymbol{A}_2, \boldsymbol{A}_2\boldsymbol{s} + \boldsymbol{e}_2 + \mathit{Encode}(m_2))$$

$$\mathsf{Eval}(+, \mathsf{ct}_1, \mathsf{ct}_2) = \mathsf{ct}_1 + \mathsf{ct}_2 = (\boldsymbol{A}_1 + \boldsymbol{A}_2, (\boldsymbol{A}_1 + \boldsymbol{A}_2)\boldsymbol{s} + \underbrace{\boldsymbol{e}_1 + \boldsymbol{e}_2}_{\sigma' \approx \sqrt{2}\sigma} + \mathit{Encode}(m_1 + m_2))$$

Ideal Lattice-based HE

$$\mathsf{sk} = \boldsymbol{s} \in \mathcal{R} = \mathbb{F}_q[X]/\mathcal{I}$$

$$\mathsf{Enc}(m, \mathsf{sk}) = (\boldsymbol{a} \in \mathcal{R}, \boldsymbol{v} = \boldsymbol{a} \cdot \boldsymbol{s} + \boldsymbol{e} + \mathit{Encode}(m))$$
$$\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) = \mathit{Decode}(\boldsymbol{v} - \boldsymbol{a} \cdot \boldsymbol{s})$$

Multiplication

$$\mathsf{ct}_1 = (\boldsymbol{a}_1, \boldsymbol{v}_1) = (\boldsymbol{a}_1, \boldsymbol{v}_1 = \boldsymbol{a}_1 \cdot \boldsymbol{s} + \boldsymbol{e}_1 + \mathit{Encode}(m_1))$$
$$\mathsf{ct}_2 = (\boldsymbol{a}_2, \boldsymbol{v}_2) = (\boldsymbol{a}_2, \boldsymbol{v}_2 = \boldsymbol{a}_2 \cdot \boldsymbol{s} + \boldsymbol{e}_2 + \mathit{Encode}(m_2))$$

$$\mathsf{Eval}(\times, \mathsf{ct}_1, \mathsf{ct}_2) = \mathsf{ct}_1 \cdot \mathsf{ct}_2 = (\boldsymbol{a}_1 \cdot \boldsymbol{a}_2, \boldsymbol{a}_1 \cdot \boldsymbol{v}_2 + \boldsymbol{a}_2 \cdot \boldsymbol{v}_1, \boldsymbol{v}_1 \cdot \boldsymbol{v}_2) = (\boldsymbol{b}_0, \boldsymbol{b}_1, \boldsymbol{b}_2)$$

$$\boldsymbol{b}_0 \boldsymbol{s}^2 + \boldsymbol{b}_1 \boldsymbol{s} + \boldsymbol{b}_2 = \boldsymbol{e} + \mathit{Encode}(m_1 m_2)$$

Why homomorphic encryption with codes?

- An alternative to structured lattices
- Faster and simpler decryption circuit
- Support and multi-dimensional approach

The LPN assumption

$$\boldsymbol{A}, \begin{pmatrix} & \\ & \boldsymbol{A} \\ & \end{pmatrix} \begin{pmatrix} \\ \boldsymbol{s} \\ \end{pmatrix} + \begin{pmatrix} \\ \boldsymbol{e} \\ \end{pmatrix} \approx \boldsymbol{A}, \begin{pmatrix} \\ \boldsymbol{y} \\ \end{pmatrix}$$

$$\boldsymbol{A} \hookleftarrow \mathbb{F}_q^{k \times n}$$
$$\boldsymbol{s} \hookleftarrow \mathbb{F}_q^{k}$$
$$\boldsymbol{e} \hookleftarrow \chi_{q,n,\sigma}$$

$$\boldsymbol{A} \hookleftarrow \mathbb{F}_q^{k \times n}$$
$$\boldsymbol{y} \hookleftarrow \mathbb{F}_q^{n}$$

The difference between LWE and LPN

LWE

$$\chi_{q,n,\sigma} = (\lfloor \mathcal{N}(0,\sigma) \rceil \mod q)^n$$

LPN

$$\chi_{q,n,\sigma} = (Ber_q(\sigma))^n$$

$$Ber_q(\sigma) = \begin{cases} 0 & \text{with probability } 1-\sigma \\ i \in \mathbb{F}_q^* & \text{with probability } \sigma/(q-1) \end{cases}$$

Same linear homomorphism for LPN, but way more constrained

$$\mathsf{ct}_1 = (\boldsymbol{A}_1, \boldsymbol{A}_1\boldsymbol{s} + \boldsymbol{e}_1 + \mathit{Encode}(m_1))$$
$$\mathsf{ct}_2 = (\boldsymbol{A}_2, \boldsymbol{A}_2\boldsymbol{s} + \boldsymbol{e}_2 + \mathit{Encode}(m_2))$$

$$\mathsf{Eval}(+, \mathsf{ct}_1, \mathsf{ct}_2) = \mathsf{ct}_1 + \mathsf{ct}_2 = (\boldsymbol{A}_1 + \boldsymbol{A}_2, (\boldsymbol{A}_1 + \boldsymbol{A}_2)\boldsymbol{s} + \underbrace{\boldsymbol{e}_1 + \boldsymbol{e}_2}_{\sigma' \approx 2\sigma} + \mathit{Encode}(m_1 + m_2))$$

Maximum noise to decrypt:

- For LWE, $\sigma'\sqrt{n} = o(q)$
- For LPN, $\sigma' < 1/2$

Previous code-based approaches used structured codes

Examples are:

- Reed-Muller [AAPS11]
- Reed-Solomon [BL11] (broken by [GOT12])

$\Longrightarrow$ highly **structured** codes

Outline

Support

Gives additional information on the localization of the error.

Definition (Hamming support)

The Hamming support of a word $\boldsymbol{x} \in (\mathbb{F}_q)^n$ is the set of indexes of its non-zero coordinates:

$$Supp_h(\boldsymbol{x}) = \{i : x_i \neq 0\}$$

Errors with the same support form a linear subspace!

Reusing the same support

$$\begin{aligned} \mathsf{ct}_1 &= (\boldsymbol{A}_1, \boldsymbol{A}_1\boldsymbol{s} + \quad \boldsymbol{e}_1 \quad + \mathit{Encode}(m_1)) \\ \mathsf{ct}_2 &= (\boldsymbol{A}_2, \boldsymbol{A}_2\boldsymbol{s} + \underbrace{\boldsymbol{e}_2}_{\text{same support}} + \mathit{Encode}(m_2)) \end{aligned}$$

$$\mathsf{Eval}(+, \mathsf{ct}_1, \mathsf{ct}_2) = \mathsf{ct}_1 + \mathsf{ct}_2 = (\boldsymbol{A}_1 + \boldsymbol{A}_2, (\boldsymbol{A}_1 + \boldsymbol{A}_2)\boldsymbol{s} + \underbrace{\boldsymbol{e}_1 + \boldsymbol{e}_2}_{\sigma' \leq \sigma} + \mathit{Encode}(m_1 + m_2))$$

Security reduction (single ciphertext)

$$\boldsymbol{v} = \begin{pmatrix} \\ \boldsymbol{A} \\ \\ \end{pmatrix} \begin{pmatrix} \\ \boldsymbol{s} \\ \\ \end{pmatrix} + \begin{pmatrix} \\ \boldsymbol{e} \\ \\ \end{pmatrix} + \begin{pmatrix} \\ \mathit{Encode}(\boldsymbol{m}) \\ \\ \end{pmatrix}$$

Security reduction (two ciphertexts)

$$\begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \end{pmatrix} = \begin{pmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_2 \end{pmatrix} \begin{pmatrix} \boldsymbol{s} \end{pmatrix} + \begin{pmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \end{pmatrix} + \begin{pmatrix} \mathit{Encode}(\boldsymbol{m}_1) \\ \mathit{Encode}(\boldsymbol{m}_2) \end{pmatrix}$$

Non standard error distribution!

Outline

Changing to rank metric

$\mathbb{F}_q$ is now an extension field : $\mathbb{F}_q = \mathbb{F}_{p^m}$

$$\begin{aligned} \mathsf{sk} &= \boldsymbol{s} \in \mathbb{F}_q^k \\ \textit{noise} &= \boldsymbol{e} \in E^n \text{ , with } E \text{ a } \mathbb{F}_p\text{-subspace of } \mathbb{F}_q \text{ of dimension } \sigma m \end{aligned}$$

$$\begin{aligned} \mathsf{Enc}(\mu, \mathsf{sk}) &= (\boldsymbol{A} \in \mathbb{F}_q^{n \times k}, \boldsymbol{v} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + \textit{Encode}(\mu)) \\ \mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) &= \textit{Decode}(\boldsymbol{v} - \boldsymbol{A}\boldsymbol{s}) \end{aligned}$$

The Rank Decoding Problem (RDP) assumption

$$\boldsymbol{A}, \begin{pmatrix} \boldsymbol{A} \\ \end{pmatrix} \begin{pmatrix} \boldsymbol{s} \\ \end{pmatrix} + \begin{pmatrix} \boldsymbol{e} \\ \end{pmatrix} \approx \boldsymbol{A}, \begin{pmatrix} \boldsymbol{y} \\ \end{pmatrix}$$

$$\boldsymbol{A} \hookleftarrow \mathbb{F}_q^{k \times n}$$
$$\boldsymbol{s} \hookleftarrow \mathbb{F}_q^{k}$$
$$E \hookleftarrow \chi_{p^m,\sigma}$$
$$\boldsymbol{e} \hookleftarrow E^n$$

$$\boldsymbol{A} \hookleftarrow \mathbb{F}_q^{k \times n}$$
$$\boldsymbol{y} \hookleftarrow \mathbb{F}_q^{n}$$

A well studied assumption

- Enables efficient public-key encryption (NIST Round 2 candidates: ROLLO, RQC)
- Connections with the well-known MinRank problem
- Many cryptanalysis efforts

Reusing the same support

$$\begin{aligned} \mathsf{ct}_1 &= (\boldsymbol{A}_1, \boldsymbol{A}_1\boldsymbol{s} + \quad \boldsymbol{e}_1 \quad + \mathit{Encode}(\mu_1)) \\ \mathsf{ct}_2 &= (\boldsymbol{A}_2, \boldsymbol{A}_2\boldsymbol{s} + \underbrace{\boldsymbol{e}_2}_{\text{same support } E} + \mathit{Encode}(\mu_2)) \end{aligned}$$

$$\mathsf{Eval}(+, \mathsf{ct}_1, \mathsf{ct}_2) = \mathsf{ct}_1 + \mathsf{ct}_2 = (\boldsymbol{A}_1 + \boldsymbol{A}_2, (\boldsymbol{A}_1 + \boldsymbol{A}_2)\boldsymbol{s} + \underbrace{\boldsymbol{e}_1 + \boldsymbol{e}_2}_{\sigma' \leq \sigma} + \mathit{Encode}(\mu_1 + \mu_2))$$

Security reduction (two ciphertexts)

$$\begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \end{pmatrix} = \begin{pmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_2 \end{pmatrix} \begin{pmatrix} \boldsymbol{s} \end{pmatrix} + \begin{pmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \end{pmatrix} + \begin{pmatrix} \mathit{Encode}(\mu_1) \\ \mathit{Encode}(\mu_2) \end{pmatrix}$$

In rank metric, **totally standard** error distribution!

Encryption / decryption algorithms

Rank Somewhat Homomorphic Encryption (RankSHE)

$$\mathsf{sk} = \boldsymbol{s} \in \mathbb{F}_q^n, \mathrm{Supp}(\boldsymbol{e}) = E, e^\perp \notin E$$

$$\mathrm{Enc}(\boldsymbol{\mu} \in \mathbb{F}_p^n, \mathsf{sk}) = (\boldsymbol{u} \in \mathbb{F}_q^n, \boldsymbol{v} = \boldsymbol{u} \cdot \boldsymbol{s} + \underbrace{\boldsymbol{e}}_{\boldsymbol{e} \in E} + e^\perp \cdot \boldsymbol{\mu})$$

$$\mathrm{Dec}((\boldsymbol{u}, \boldsymbol{v}), \mathsf{sk}) = \varphi_{e^\perp}(\boldsymbol{v} - \boldsymbol{u} \cdot \boldsymbol{s})$$

In this work: $\mathit{Encode}(\boldsymbol{\mu}) = e^\perp \cdot \boldsymbol{\mu}$ with $e^\perp \notin E$ and $\boldsymbol{\mu} \in \mathbb{F}_p^n$

Proposition

The security of **RankSHE** *with ℓ independent ciphertexts is reduced to the ℓ-IRDP problem (decoding in an ideal $[\ell n, n]_{p^m}$ code)*

Linear forms

Definition

$\varphi_{e^\perp}$ is an $\mathbb{F}_p$-linear form defined on $\mathbb{F}_q$ such that:

$$\varphi_{e^\perp}(e^\perp) = 1$$
$$\varphi_{e^\perp}(e) = 0 \quad (e \in E)$$

Informally,

$$\varphi_{e^\perp}(x) = \frac{\langle e^\perp, x \rangle}{\langle e^\perp, e^\perp \rangle}$$

Definition

$$\varphi_{e^\perp}(\boldsymbol{x}) = (\varphi_{e^\perp}(x_i))_i$$

Linear forms

Lemma

For $\boldsymbol{v} \in \mathbb{F}_q^n$ *and* $\boldsymbol{\mu} \in \mathbb{F}_p^n$,

$$\varphi_{e^\perp}(\boldsymbol{\mu} \cdot \boldsymbol{v}) = \boldsymbol{\mu} \cdot \varphi_{e^\perp}(\boldsymbol{v}).$$

Addition

$$\mathsf{Enc}(\boldsymbol{\mu}_1, \mathsf{sk}) + \mathsf{Enc}(\boldsymbol{\mu}_2, \mathsf{sk}) = \mathsf{Enc}(\boldsymbol{\mu}_1 + \boldsymbol{\mu}_2, \mathsf{sk})$$

$$\boldsymbol{v}_1 = \boldsymbol{u}_1 \cdot \boldsymbol{s} + \boldsymbol{e}_1 + e^{\perp} \cdot \boldsymbol{\mu}_1$$
$$\boldsymbol{v}_2 = \boldsymbol{u}_2 \cdot \boldsymbol{s} + \boldsymbol{e}_2 + e^{\perp} \cdot \boldsymbol{\mu}_2$$

$$\boldsymbol{v}_1 + \boldsymbol{v}_2 = (\boldsymbol{u}_1 + \boldsymbol{u}_2) \cdot \boldsymbol{s} + \boldsymbol{e}_1 + \boldsymbol{e}_2 + e^{\perp} \cdot (\boldsymbol{\mu}_1 + \boldsymbol{\mu}_2)$$

Plaintext absorption

$$\boldsymbol{\mu}_1 \cdot \mathsf{Enc}(\boldsymbol{\mu}_2, \mathsf{sk}) = \mathsf{Enc}(\boldsymbol{\mu}_1 \cdot \boldsymbol{\mu}_2, \mathsf{sk})$$

$$\boldsymbol{v}_2 = \boldsymbol{u}_2 \cdot \boldsymbol{s} + \boldsymbol{e}_2 + e^{\perp} \cdot \boldsymbol{\mu}_2$$

$$\boldsymbol{\mu}_1 \cdot \boldsymbol{v}_2 = (\boldsymbol{\mu}_1 \cdot \boldsymbol{u}_2) \cdot \boldsymbol{s} + \boldsymbol{\mu}_1 \cdot \boldsymbol{e}_2 + e^{\perp} \cdot (\boldsymbol{\mu}_1 \cdot \boldsymbol{\mu}_2)$$

Multiplication

$$\mathsf{Eval}(\times, (\boldsymbol{u}_1, \boldsymbol{v}_1), (\boldsymbol{u}_2, \boldsymbol{v}_2)) = (\boldsymbol{u}_1 \cdot \boldsymbol{u}_2, \boldsymbol{u}_1 \cdot \boldsymbol{v}_2 + \boldsymbol{u}_2 \cdot \boldsymbol{v}_1, \boldsymbol{v}_1 \cdot \boldsymbol{v}_2)$$

$$\begin{aligned}
&\boldsymbol{u}_1 \cdot \boldsymbol{u}_2 \cdot \boldsymbol{s}^2 - (\boldsymbol{u}_1 \cdot \boldsymbol{v}_2 + \boldsymbol{u}_2 \cdot \boldsymbol{v}_1) \cdot \boldsymbol{s} + \boldsymbol{v}_1 \cdot \boldsymbol{v}_2 \\
&= (\boldsymbol{v}_1 - \boldsymbol{u}_1 \cdot \boldsymbol{s}) \cdot (\boldsymbol{v}_2 - \boldsymbol{u}_2 \cdot \boldsymbol{s}) \\
&= (\boldsymbol{e}_1 + e^{\perp} \cdot \boldsymbol{\mu}_1) \cdot (\boldsymbol{e}_2 + e^{\perp} \cdot \boldsymbol{\mu}_2) \\
&= \underbrace{\boldsymbol{e}_1 \cdot \boldsymbol{e}_2 + e^{\perp} \cdot (\boldsymbol{e}_1 \cdot \boldsymbol{\mu}_2 + \boldsymbol{e}_2 \cdot \boldsymbol{\mu}_1)}_{\boldsymbol{e}', \mathsf{Supp}(\boldsymbol{e}') \subset E^2 \oplus e^{\perp} E} + (e^{\perp})^2 \cdot \boldsymbol{\mu}_1 \cdot \boldsymbol{\mu}_2
\end{aligned}$$

$$\mathsf{Dec}\mathit{AfterMul}((\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}), \mathsf{sk}) = \varphi_{(e^{\perp})^2}(\boldsymbol{u} \cdot \boldsymbol{s}^2 - \boldsymbol{v} \cdot \boldsymbol{s} + \boldsymbol{w})$$

Summary

- Encryption scheme based on ideal random rank metric codes
- Unlimited additions
- Multiplication adds a component to the ciphertext and increases noise quadratically

Reducing ciphertext noise

$(\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w})$ decryptable under sk_1

$\Downarrow$

$(\boldsymbol{u}, \boldsymbol{v})$ decryptable under sk_2

Bootstrapping

$$\mathsf{Eval}(\mathsf{Dec}\mathit{AfterMul}(\cdot,\cdot),\ \underbrace{\mathsf{ct}_1}_{\mathsf{Enc}((\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}),\mathsf{sk}_2)},\ \underbrace{\mathsf{ct}_2}_{\mathsf{Enc}(\mathsf{sk}_1,\mathsf{sk}_2)}) \approx \mathsf{Enc}(\boldsymbol{\mu},\mathsf{sk}_2)$$

$$\widehat{\mathsf{Eval}}(\mathsf{Dec}\mathit{AfterMul}(\cdot,\cdot),\ \underbrace{\mathsf{ct}_1}_{(\boldsymbol{u},\boldsymbol{v},\boldsymbol{w})},\ \underbrace{\mathsf{ct}_2}_{\mathsf{Enc}(\varphi_{e^\perp}(\mathsf{sk}_1),\mathsf{sk}_2)}) \approx \mathsf{Enc}(\boldsymbol{\mu},\mathsf{sk}_2)$$

Bootstrapping

$$\mathsf{Dec}\mathit{AfterMul}((\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}),\mathsf{sk}_1) = \varphi_{(e^\perp)^2}(\boldsymbol{u}\cdot\boldsymbol{s}_1^2 - \boldsymbol{v}\cdot\boldsymbol{s}_1 + \boldsymbol{w})$$

$$\boldsymbol{u} = \sum_i \gamma_i \boldsymbol{u}^{(i)}$$
$$\boldsymbol{v} = \sum_i \gamma_i \boldsymbol{v}^{(i)}$$
$$\boldsymbol{w} = \sum_i \gamma_i \boldsymbol{w}^{(i)}$$

$$\mathsf{Dec}\mathit{AfterMul}((\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}),\mathsf{sk}_1) = \sum_i \underbrace{\boldsymbol{u}^{(i)}}_{\in\mathbb{F}_p}\cdot\underbrace{\boldsymbol{a}^{(i)}}_{\in\mathbb{F}_q} - \boldsymbol{v}^{(i)}\cdot\boldsymbol{b}^{(i)} + \boldsymbol{w}^{(i)}\cdot\boldsymbol{c}^{(i)}$$

Bootstrapping

$$
\begin{aligned}
\varphi_{(e^{\perp})^2}(\boldsymbol{u} \cdot \boldsymbol{s}_1^2) &= \sum_i \varphi_{(e^{\perp})^2}(\gamma_i \boldsymbol{u}^{(i)} \cdot \boldsymbol{s}_1^2) \\
&= \sum_i \varphi_{(e^{\perp})^2}(\boldsymbol{u}^{(i)} \cdot \gamma_i \boldsymbol{s}_1^2) \\
&= \sum_i \boldsymbol{u}^{(i)} \cdot \varphi_{(e^{\perp})^2}(\gamma_i \boldsymbol{s}_1^2) \\
&= \sum_i \boldsymbol{u}^{(i)} \cdot \boldsymbol{a}^{(i)}
\end{aligned}
$$

Bootstrapping

$$\mu = \mathsf{Dec}\mathit{AfterMul}((\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}), \mathsf{sk}_1) = \sum_i \boldsymbol{u}^{(i)} \cdot \boldsymbol{a}^{(i)} - \boldsymbol{v}^{(i)} \cdot \boldsymbol{b}^{(i)} + \boldsymbol{w}^{(i)} \cdot \boldsymbol{c}^{(i)}$$

with

$$\begin{aligned}
\boldsymbol{a}^{(i)} &= \varphi_{(e^{\perp})^2}(\gamma_i \boldsymbol{s}_1^2) \\
\boldsymbol{b}^{(i)} &= \varphi_{(e^{\perp})^2}(\gamma_i \boldsymbol{s}_1) \\
\boldsymbol{c}^{(i)} &= \varphi_{(e^{\perp})^2}(\gamma_i (1, 0, \ldots, 0))
\end{aligned}$$

Bootstrapping

$$\mathsf{ct}_{\boldsymbol{a}^{(i)}} = \mathsf{Enc}(\boldsymbol{a}^{(i)}, \mathsf{sk}_2) = \mathsf{Enc}(\varphi_{(e^{\perp})^2}(\gamma_i \boldsymbol{s}_1^2), \mathsf{sk}_2)$$
$$\mathsf{ct}_{\boldsymbol{b}^{(i)}} = \mathsf{Enc}(\boldsymbol{b}^{(i)}, \mathsf{sk}_2) = \mathsf{Enc}(\varphi_{(e^{\perp})^2}(\gamma_i \boldsymbol{s}_1), \mathsf{sk}_2)$$
$$\mathsf{ct}_{\boldsymbol{c}^{(i)}} = \mathsf{Enc}(\boldsymbol{c}^{(i)}, \mathsf{sk}_2) = \mathsf{Enc}(\varphi_{(e^{\perp})^2}(\gamma_i (1, 0, \ldots, 0)), \mathsf{sk}_2)$$

$$\begin{aligned}
&\widehat{\mathsf{Eval}}(\mathsf{Dec}\mathit{AfterMul}, (\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}), \mathsf{ct}_{\boldsymbol{a}^{(i)}}, \mathsf{ct}_{\boldsymbol{b}^{(i)}}, \mathsf{ct}_{\boldsymbol{c}^{(i)}}) \\
&\quad := \sum_i \boldsymbol{u}^{(i)} \cdot \mathsf{ct}_{\boldsymbol{a}^{(i)}} - \boldsymbol{v}^{(i)} \cdot \mathsf{ct}_{\boldsymbol{b}^{(i)}} + \boldsymbol{w}^{(i)} \cdot \mathsf{ct}_{\boldsymbol{c}^{(i)}} \\
&\quad = \mathsf{Enc}(\sum_i \boldsymbol{u}^{(i)} \cdot \boldsymbol{a}^{(i)} - \boldsymbol{v}^{(i)} \cdot \boldsymbol{b}^{(i)} + \boldsymbol{w}^{(i)} \cdot \boldsymbol{c}^{(i)}, \mathsf{sk}_2) \\
&\quad = \mathsf{Enc}(\boldsymbol{\mu}, \mathsf{sk}_2)
\end{aligned}$$

Bootstrapping

Our bootstrapping algorithm:

- Transforms a three-compenent ciphertext into a two-component ciphertext;
- reduces the noise from $\approx E_1^2$ to E_2;
- has no multiplicative cost;
- but... requires $3m$ independent ciphertexts under sk_2.

Security reduction ($3m$ ciphertexts)

The attacker needs to solve the RSD problem in an ideal $[3mn, n]_{p^m}$ code.

There exists a polynomial attack [GRS13] in an $[n, k]_{p^m}$ code when

$$(k+1)(\sigma m+1) \leq n+1.$$

$\Longrightarrow$ maximal number of independent ciphertexts $\approx \sigma m$.

Reducing the number of bootstrapping ciphertexts

We pack several plaintexts into a single ciphertext:

$$\mathsf{Enc}((\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_t) \in (\mathbb{F}_p^n)^t, \mathsf{sk}) = (\boldsymbol{u} \in \mathbb{F}_q^n, \boldsymbol{v} = \boldsymbol{u} \cdot \boldsymbol{s} + \underbrace{\boldsymbol{e}}_{\|\boldsymbol{e}\| \leq w} + \sum_{i=1}^{t} \chi^i e^{\perp} \cdot \boldsymbol{\mu}_i)$$

with $\chi \in \mathbb{F}_q$ s.t. $\chi^t = 1$.

Maximal packing index $t = \frac{1}{\sigma}$.

$\Longrightarrow$ reduces the number of bootstrapping plaintexts to $\frac{3m}{t} = 3\sigma m$.

Summary

- Encryption scheme based on ideal random rank metric codes
- Unlimited additions
- Multiplication adds a component to the ciphertext and increases noise quadratically
- Limited number of ciphertexts (sublinear in ciphetext size)

Parameters

d	q	m	n	w	ℓ	Security	Key size	ct size	Add	Mul	Bootstrap
1	2	172	20	13	9	128	3.7 kB	**0.9 kB**	0.002 ms	**0.5 ms**	**2 ms**
2	2	367	183	7	5	128	17.0 kB	16.8 kB	0.04 ms	52 ms	374 ms
3	2	1296	314	6	4	128	210 kB	102 kB	0.3 ms	944 ms	11 s
4	2	3125	713	5	3	128	1.22 MB	557 kB	1 ms	14.3 s	239 s

Table: Example of paramaters for our SHE scheme, with associated sizes and execution timings. d is the number of possible multiplications. q, m and n are parameters of the rank linear code and w is the rank weight of the error. ℓ is the number of independant ciphertexts that can be published.

Comparison

Scheme	ct size	Bootstrap ct size	Mul time	Bootstrap time
TFHE [CGGI20]	2 kB	15.6 MB	0.03 ms	13 ms
[AAPS11]	18.5 kB	-	10 ms	-
This work	0.9 kB	35 kB	0.5 ms	2 ms

Table: Parameters are taken for 128-bit security, and for SHE schemes, with a single multiplication allowed.

Open problems

- Reduce the number of bootstrapping ciphertexts
- Demonstrate a practical application

Open problems

- Reduce the number of bootstrapping ciphertexts
- Demonstrate a practical application

Thank you for your attention!

References I


Frederik Armknecht, Daniel Augot, Ludovic Perret, and Ahmad-Reza Sadeghi.
On constructing homomorphic encryption schemes from coding theory.
In IMA International Conference on Cryptography and Coding, pages 23–40. Springer, 2011.


Dan Boneh, Eu-Jin Goh, and Kobbi Nissim.
Evaluating 2-DNF formulas on ciphertexts.
In Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2, pages 325–341. Springer, 2005.


Andrej Bogdanov and Chin Ho Lee.
Homomorphic encryption from codes.
Cryptology ePrint Archive, Report 2011/622, 2011.
https://eprint.iacr.org/2011/622.

References II


Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène.
Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds.
In Jung Hee Cheon and Tsuyoshi Takagi, editors, ASIACRYPT 2016, Part I, volume 10031 of LNCS, pages 3–33. Springer, Heidelberg, December 2016.


Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène.
TFHE: Fast fully homomorphic encryption over the torus.
Journal of Cryptology, 33(1):34–91, January 2020.


Xuan-Thanh Do, Dang-Truong Mac, and Quoc-Huy Vu.
zk-snarks from codes with rank metrics.
In IMA International Conference on Cryptography and Coding, pages 99–119. Springer, 2023.

References III


Craig Gentry.
Fully homomorphic encryption using ideal lattices.
In Proceedings of the forty-first annual ACM symposium on Theory of computing, pages 169–178, 2009.


Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich.
Identity-based encryption from codes with rank metric.
In Jonathan Katz and Hovav Shacham, editors, CRYPTO 2017, Part III, volume 10403 of LNCS, pages 194–224. Springer, Heidelberg, August 2017.


Valérie Gauthier, Ayoub Otmani, and Jean-Pierre Tillich.
A distinguisher-based attack of a homomorphic encryption scheme relying on reed-solomon codes.
Cryptology ePrint Archive, Report 2012/168, 2012.
https://eprint.iacr.org/2012/168.

References IV

Philippe Gaborit, Olivier Ruatta, and Julien Schrek.
On the complexity of the rank syndrome decoding problem.
CoRR, abs/1301.1026, 2013.

Carlos Aguilar Melchor, Pierre-Louis Cayrel, Philippe Gaborit, and Fabien Laguillaumie.
A new efficient threshold ring signature scheme based on coding theory.
IEEE Transactions on Information Theory, 57(7):4833–4842, 2011.

Khoa Nguyen, Hanh Tang, Huaxiong Wang, and Neng Zeng.
New code-based privacy-preserving cryptographic constructions.
In Steven D. Galbraith and Shiho Moriai, editors, ASIACRYPT 2019, Part II, volume 11922 of LNCS, pages 25–55. Springer, Heidelberg, December 2019.

References V


Jacques Stern.
A new identification scheme based on syndrome decoding.
In Douglas R. Stinson, editor, CRYPTO'93, volume 773 of LNCS, pages 13–21. Springer, Heidelberg, August 1994.


Vahid Yousefipoor and Taraneh Eghlidos.
An efficient post-quantum attribute-based encryption scheme based on rank metric codes for cloud computing.
IEEE Access, 2023.


Zhuoran Zhang, Zheng Zhang, and Fangguo Zhang.
Inner-product functional encryption from random linear codes: Trial and challenges.
In Provable and Practical Security: 15th International Conference, ProvSec 2021, Guangzhou, China, November 5–8, 2021, Proceedings 15, pages 259–276. Springer, 2021.