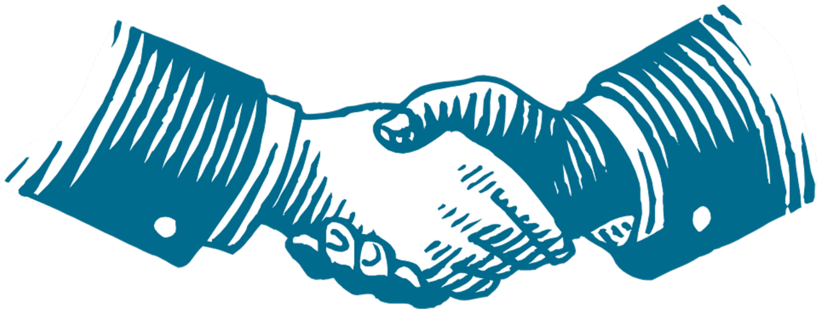
When HEAAN Meets FV:
a New Somewhat Homomorphic Encryption with Reduced Memory Overhead



Hao Chen
Facebook
USA

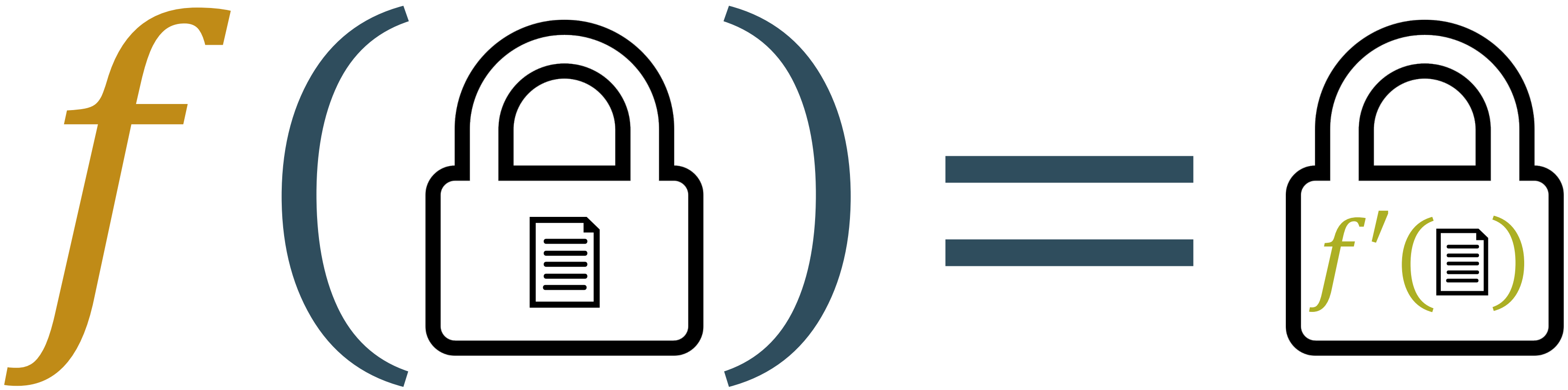
Ilia Iliashenko
Ciphermode Labs;
imec-COSIC, KU Leuven
Belgium

Kim Laine
Microsoft Research
USA

IMA International Conference on Cryptography and Coding

December 15, 2021

Fully/somewhat homomorphic encryption



Fully HE (FHE): f' is arbitrary.

Somewhat HE (SHE): f' has a limited depth.

FHE/SHE schemes are exact

Ciphertext ct encrypts a message m.

$$\text{Decrypt}(ct) = m$$

The results of correct decryption are useless for an attacker.
Every ciphertext has noise and it is removed by decryption.

Approximate HE (HEAAN/CKKS)

Idea: consider ciphertext noise as a part of a message.

Ciphertext ct encrypts a message m.

Decryption leaves some noise

$$\mathrm{Decrypt}(ct) = m + e \simeq m.$$

Decryption results always leak the noise and can be used for key recovery. (Li-Micciancio'20).

FHE/SHE versus AHE

FHE/SHE

- inefficient for arithmetic on complex or real numbers
- batching capacity is limited

+ small encryption parameters for simple functions
+ no decryption leakage

AHE

+ efficient for arithmetic on complex or real numbers
+ huge batching capacity

- large encryption parameters even for simple functions
- decryption leakage

Is there an HE scheme with the best of the two worlds?

SHE scheme from BCIV'18

Version of the RLWE-based scheme of Fan and Vercauteren (aka FV)

Ciphertext space: $R_q^2 = (\mathbb{Z}[X]/\langle q, X^n + 1\rangle)^2, q \in \mathbb{Z}$

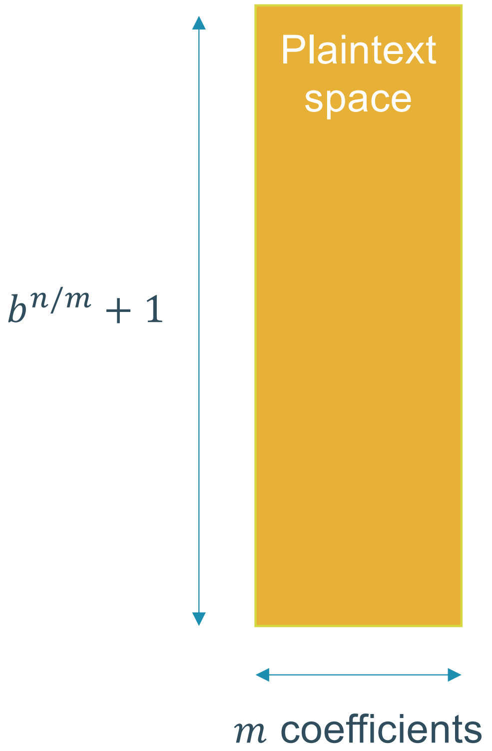
Plaintext space: $R_{X^m+b} = \mathbb{Z}[X]/\langle X^m + b, X^n + 1\rangle$, m, n are powers of two ($m = 0$ in FV)

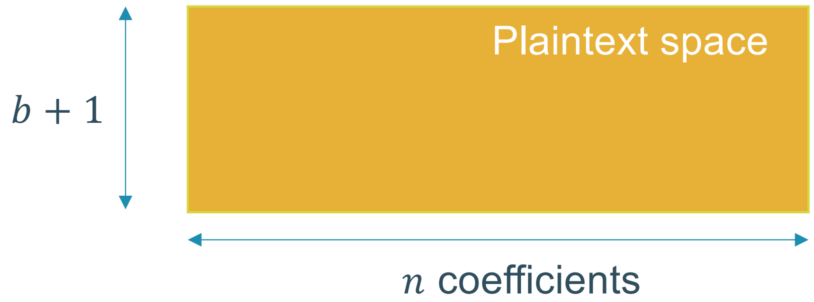
- $R_{X^m+b} \cong \mathbb{Z}[X]/\left\langle X^m + b, b^{n/m} + 1\right\rangle$
  natively supports polynomials with large coefficients
- If $\exists\alpha: b = \alpha^m \bmod \left(b^{n/m} + 1\right)$, then

$$R_{X^m+b} \cong \mathbb{Z}[e^{\pi i/m}]/\langle b^{n/m} + 1\rangle$$

natively supports cyclotomic integers

FV allows less operations on number encodings

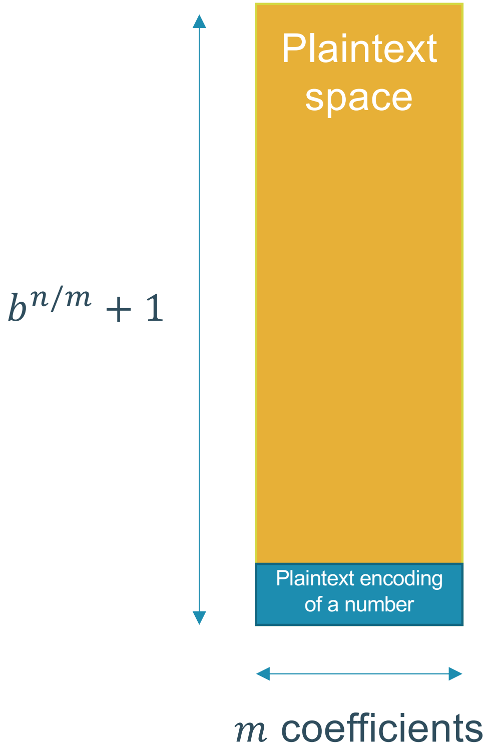


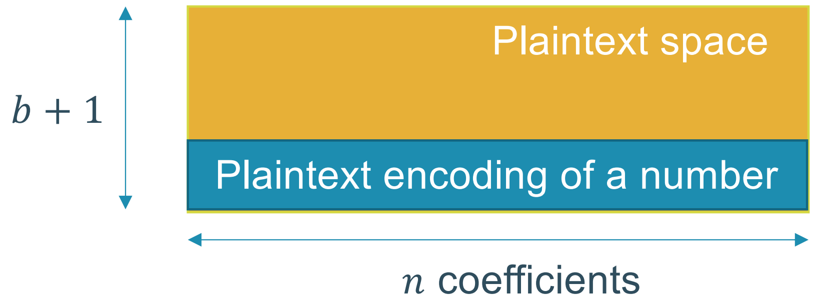


FV: $R_{b+1} = \mathbb{Z}[X]/\langle b+1, X^n + 1\rangle,\ t \in \mathbb{Z}$

BCIV: $R_{X^m+b} \cong \mathbb{Z}[X]/\langle X^m + b, b^{n/m} + 1\rangle$

FV allows less operations on number encodings

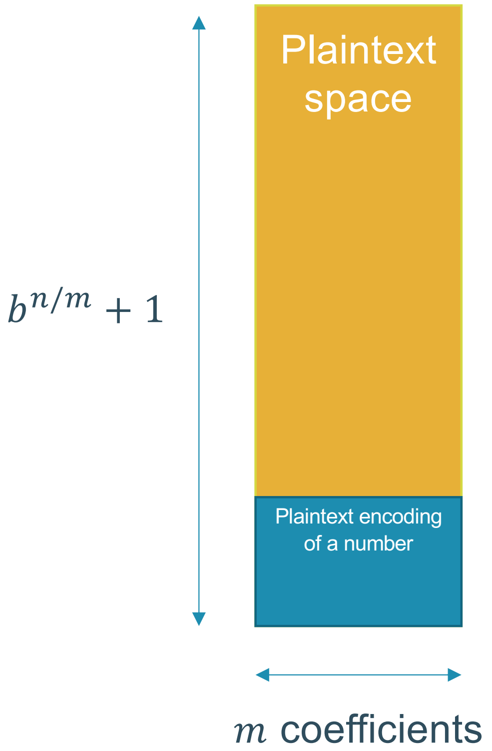


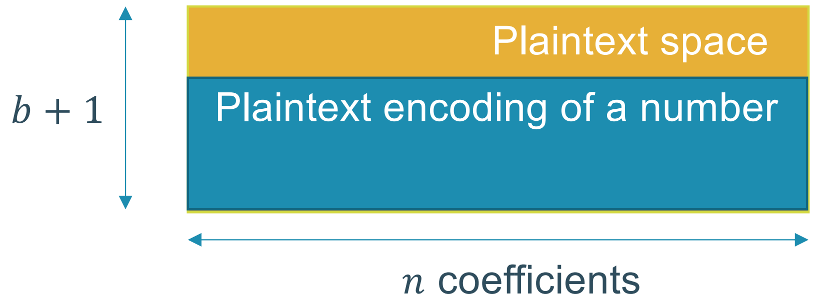


FV: $R_{b+1} = \mathbb{Z}[X]/\langle b+1, X^n + 1 \rangle,\ t \in \mathbb{Z}$

BCIV: $R_{X^m+b} \cong \mathbb{Z}[X]/\langle X^m + b, b^{n/m} + 1 \rangle$

FV allows less operations on number encodings

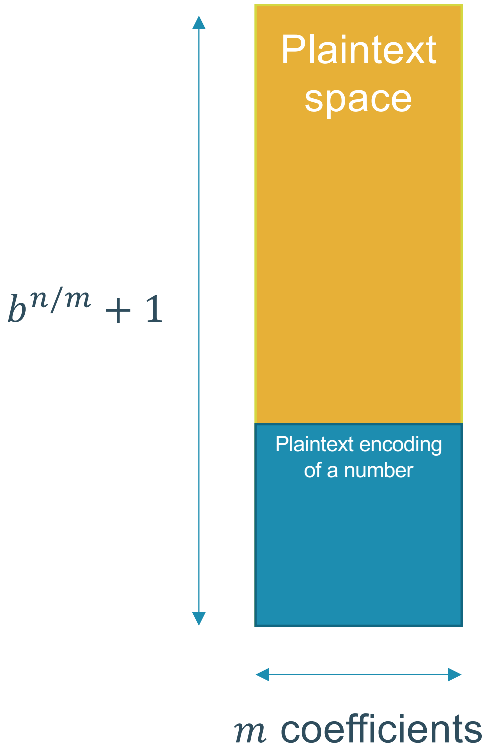




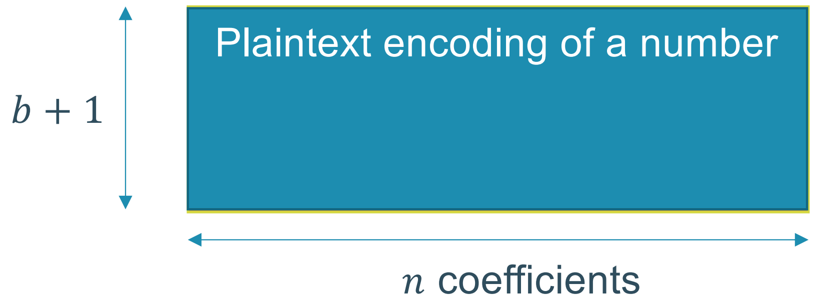
FV: $R_{b+1} = \mathbb{Z}[X]/\langle b + 1, X^n + 1\rangle$, $t \in \mathbb{Z}$

BCIV: $R_{X^m+b} \cong \mathbb{Z}[X]/\langle X^m + b, b^{n/m} + 1\rangle$

FV allows less operations on number encodings



BCIV: $R_{X^m+b} \cong \mathbb{Z}[X]/\langle X^m + b, b^{n/m} + 1\rangle$



FV: $R_{b+1} = \mathbb{Z}[X]/\langle b + 1, X^n + 1\rangle$, $t \in \mathbb{Z}$

HEAAN

Version of the RLWE-based scheme of Fan and Vercauteren (aka FV)

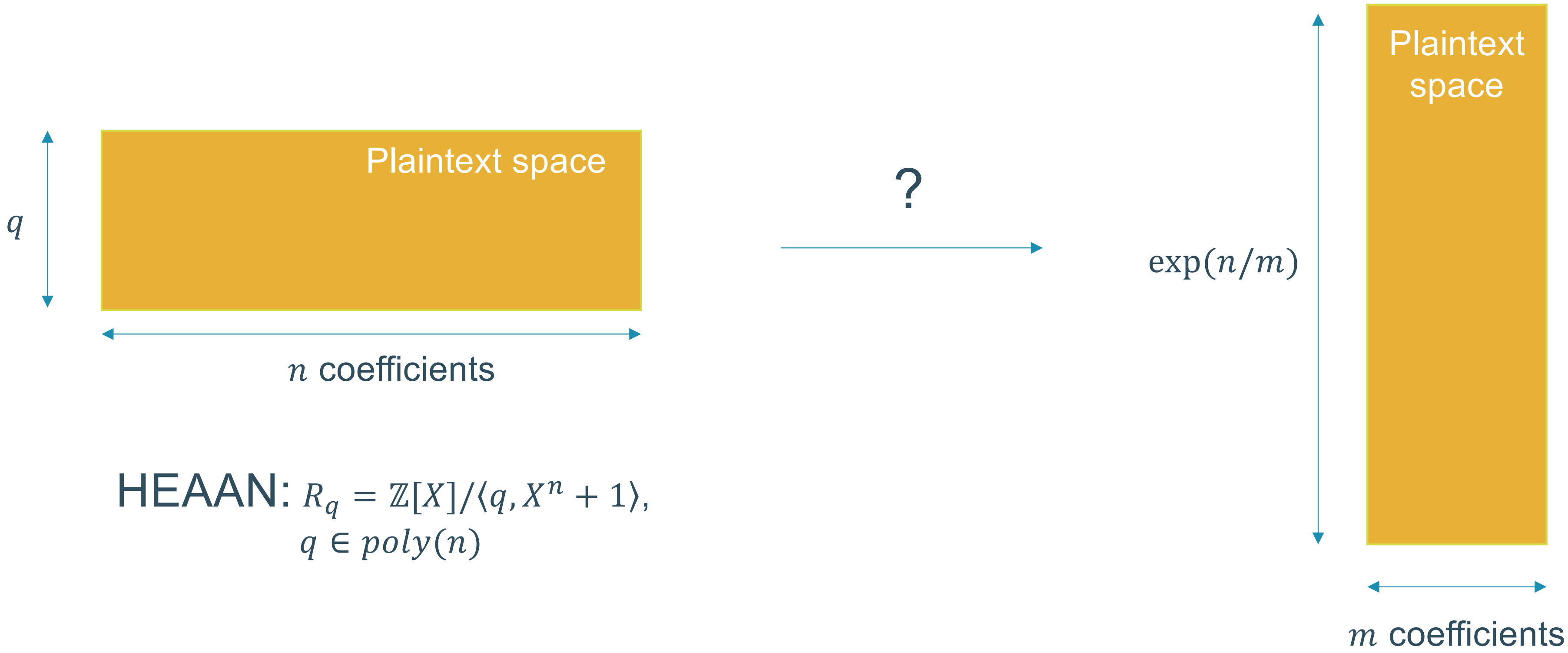
Ciphertext space: $R_q^2 = (\mathbb{Z}[X]/\langle q, X^n + 1\rangle)^2, q \in \mathbb{Z}$

Plaintext space: $R_q = \mathbb{Z}[X]/\langle q, X^n + 1\rangle \cong \mathbb{Z}[e^{\pi i/n}]/\langle q\rangle$
natively supports cyclotomic integers

- $m/2$ complex numbers can be encoded into one plaintext
  - $\text{Pack}_{p,m}\colon \mathbb{C}^{m/2} \to R_q$
  - $\text{Unpack}_{p,m}\colon R_q \to \mathbb{C}^{m/2}$

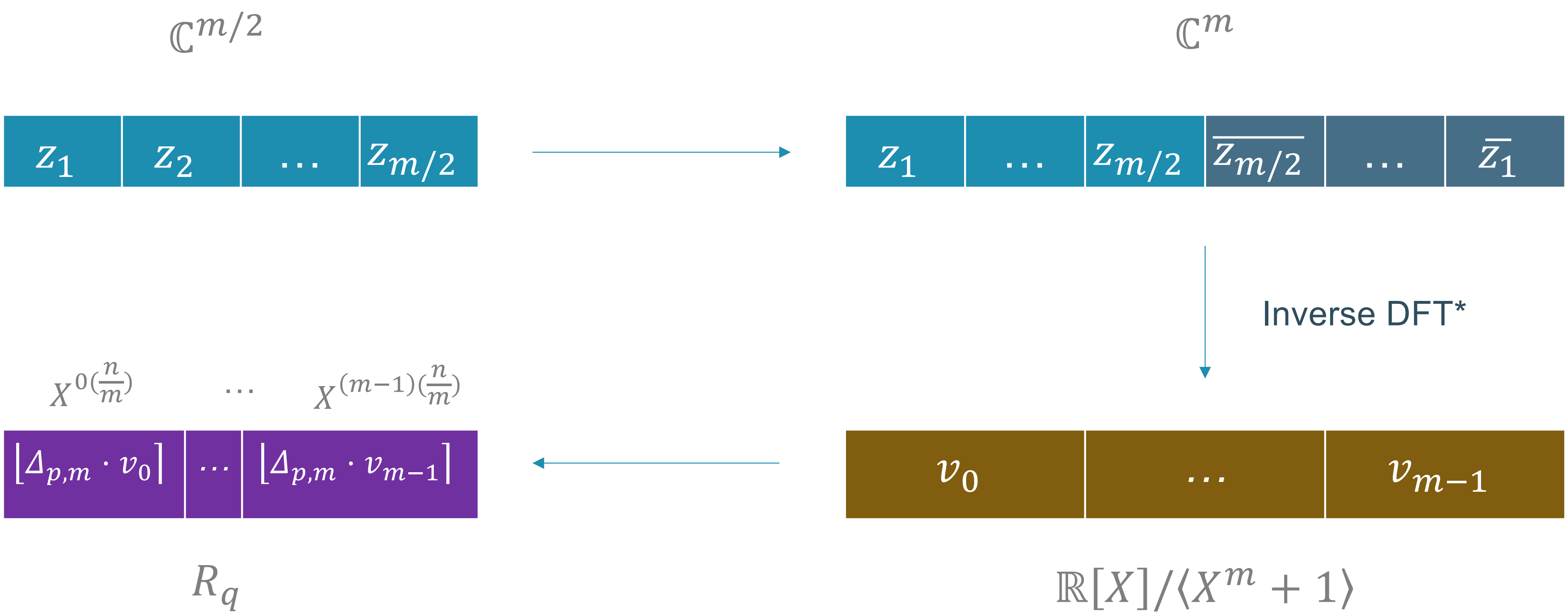
$$\left|\text{Unpack}_{p,m}\left(\text{Pack}_{p,m}(\mathbf{z})\right) - \mathbf{z}\right|_\infty < \frac{1}{p}$$

HEAAN plaintext space is constrained as in FV



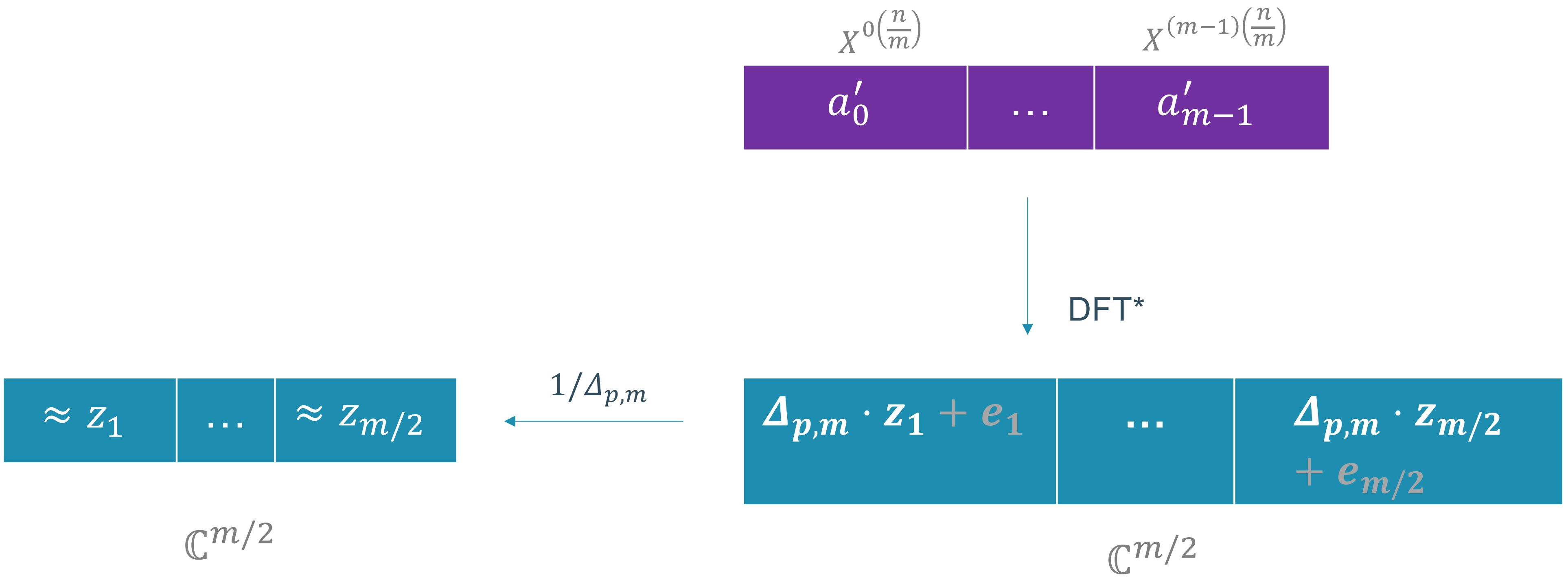
HEAAN: $R_q = \mathbb{Z}[X]/\langle q, X^n + 1\rangle$,
$q \in poly(n)$

$\mathrm{Pack}_{p,m}\colon \mathbb{C}^{m/2} \to R_q$



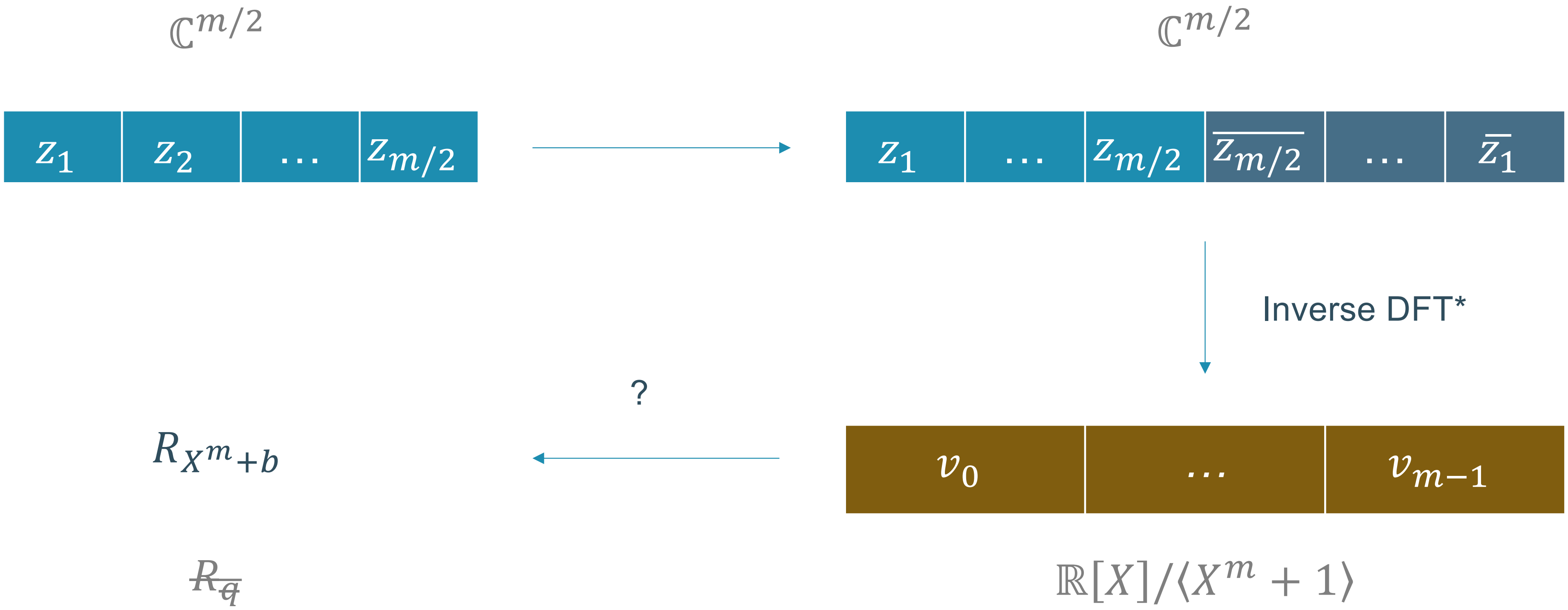
*with primitive $2m$-th roots of unity

$\text{Unpack}_{p,m}: R_q \rightarrow \mathbb{C}^{m/2}$



*with primitive $2m$-th roots of unity

$\text{Pack}_{p,m}\colon \mathbb{C}^{m/2} \to R_{X^m+b}$ for BCIV



*with primitive $2m$-th roots of unity

BCIV encoding of real polynomials

If $\exists \alpha: b = \alpha^m \bmod \left(b^{n/m} + 1\right)$, then

$$e^{\pi i/m} \mapsto \alpha^{-1} X$$

yields the isomorphism

$$\mathbb{Z}[e^{\pi i/m}]/\langle b^{n/m} + 1\rangle \cong R_{X^m + b}$$

$$\uparrow$$

1. multiply by $\Delta_{p,m}$,
2. round coefficientwise
3. map $X \mapsto e^{\pi i/m}$

$$\mathbb{R}[X]/\langle X^m + 1\rangle$$

Asymptotic comparison

To support computation of **multiplicative depth** L
with starting **precision** p
on $m/2$ complex **numbers**
of **absolute value** B.

HEAAN: $q \in \Theta\left(m^{L+1} p^{L+1} B^{2^L} n^{L+1}\right)$

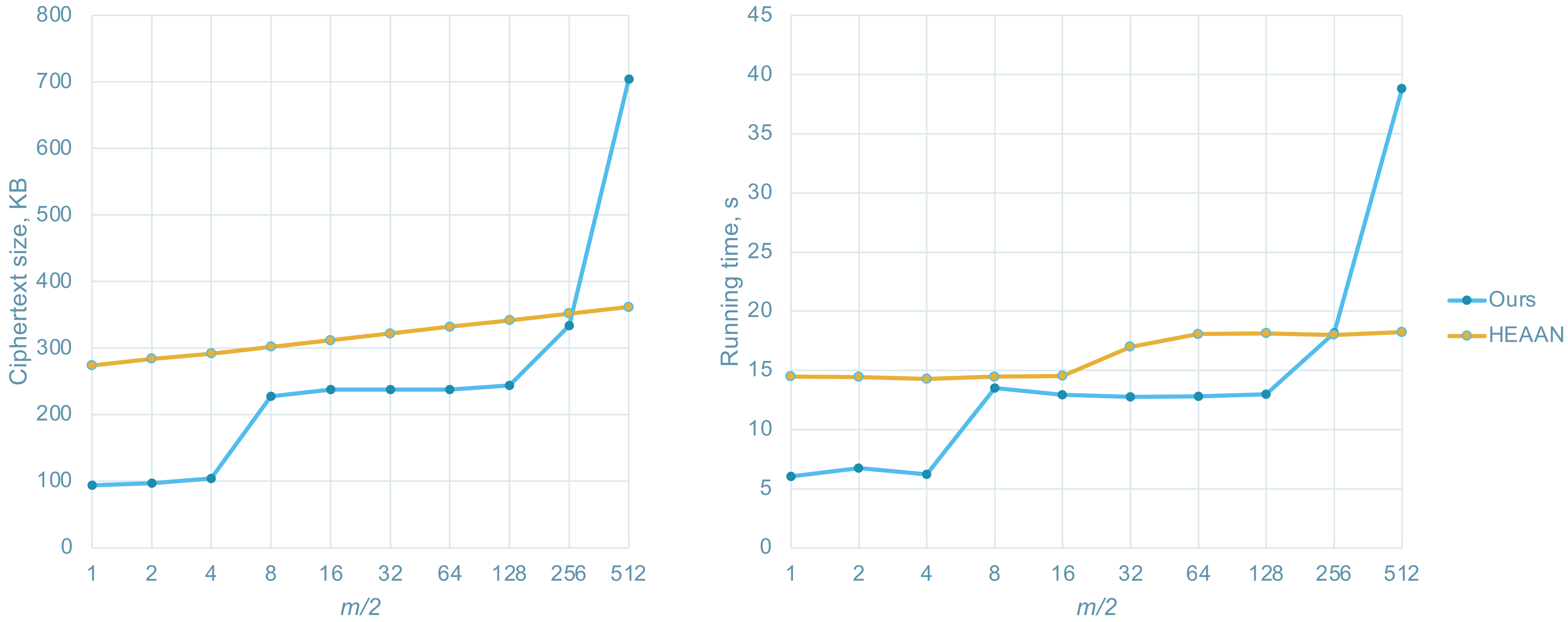
OUR scheme: $q \in \Theta\left(m^{\frac{m}{n}(2^{L+1}-1)(L+2)} (pB)^{\frac{m}{n}2^L(L+2)} n^{L+1.5}\right)$

Our scheme is better
if $m/n = 2^{-L-1}$ and $B > (m\sqrt{n})^{2^{1-L}}$

→

- Shallow circuits with $m \simeq n/4$
- Deep circuits with $m = n/2^{L+1}$

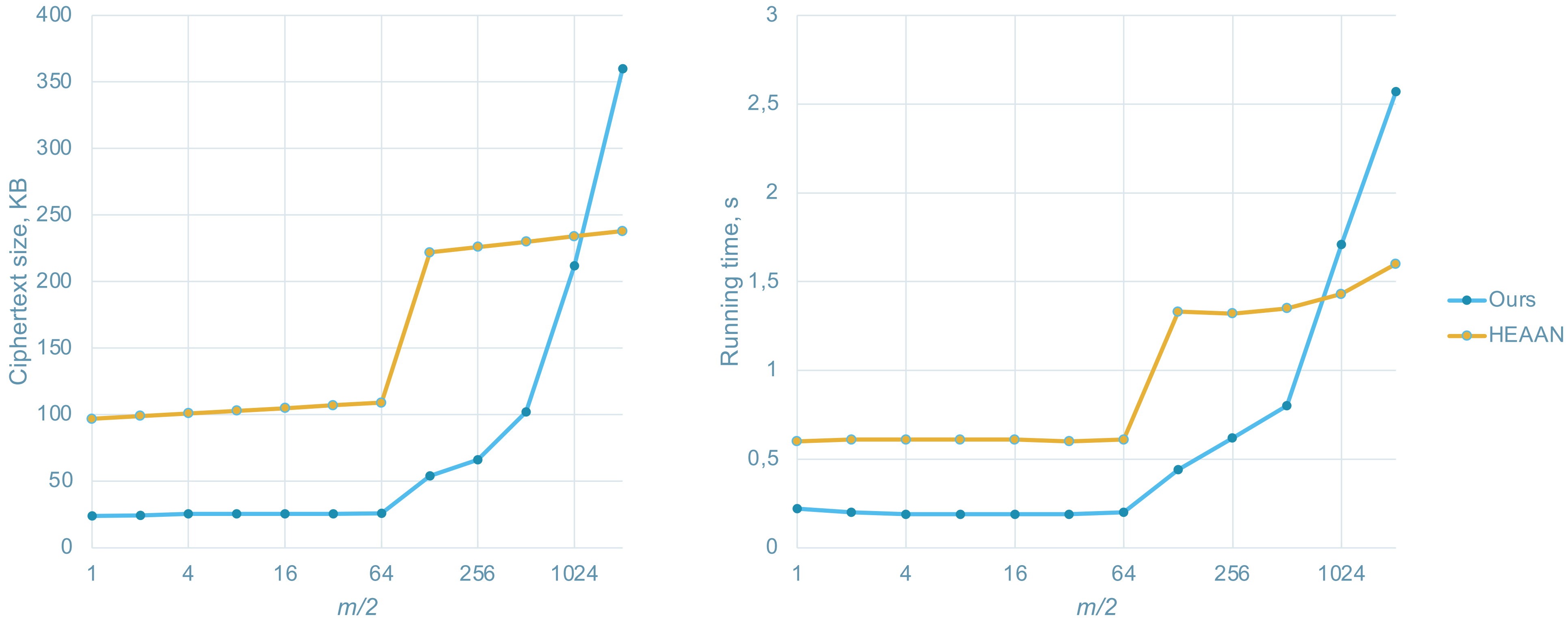
Practical comparison: logistic regression



$B = 2.1$

Output precision 2^7

Practical comparison: x^{16}



$B = 2.1$

Output precision 2^7

Conclusion

- New SHE scheme natively supporting complex vectors
- No decryption leakage
- Better computational and memory overhead than in HEAAN when
  - circuits are shallow (e.g. simple statistics)
  - packing capacity is small (e.g. small data stream to be handled online)

Future work

- Implement in RNS (residue number system)
- Find an analog of HEAAN's Rescale operation

Thank you