A Critique on Average-Case Noise Analysis in RLWE-Based Homomorphic Encryption

Mingyu Gao **Hongren Zheng**

WAHC' 25

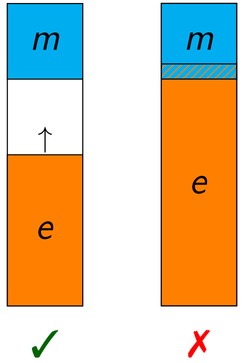
Recap: RLWE-based Homomorphic Encryption

Secret key s Message Δm Noise e

$$(as + \Delta m + e, a)$$

- Polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$
- a, s, m, e are polynomials
- Poly multiplication is coeff convolution

$$a \cdot b = \sum_{i=0}^{2N-1} \left(\sum_{j+k=i} a_j b_k \right) X^i \pmod{X^N + 1}$$

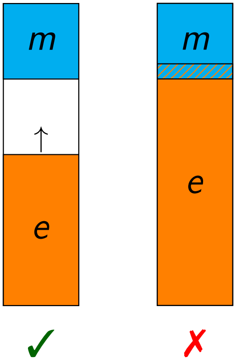


Recap: RLWE-based Homomorphic Encryption

Secret key s Message Δm Noise e

$$(as + \Delta m + e, a)$$

- Message in high bits
- Noise grows after HE operations
- Noise should never *overflow*

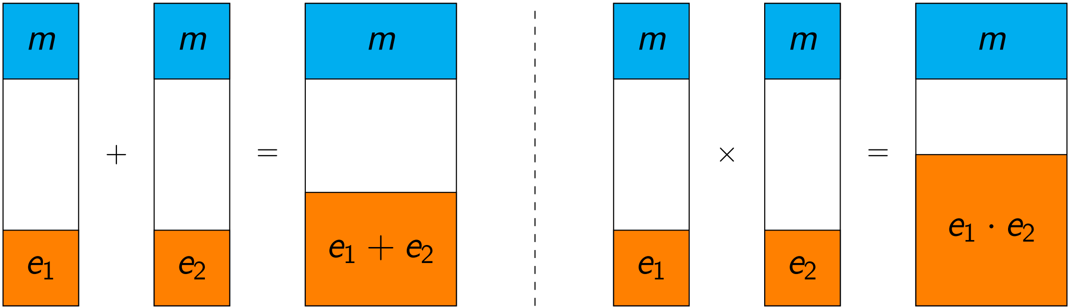


$$\text{correctness} \xleftrightarrow{\textit{tradeoff}} \text{efficiency}$$

$$\Downarrow$$

Noise Analysis

Worst-Case Noise Analysis



$+$ **is easy**

$$\|e_1 + e_2\| \leq \|e_1\| + \|e_2\|$$

$\times$ **is hard**

$$\|e_1 \cdot e_2\| \leq N \cdot \|e_1\| \cdot \|e_2\|$$

- N is *worst-case expansion factor*, very conservative and undesired
- Empirically, growth should be $C\sqrt{N}$

Average-Case Noise Analysis: Variance-Based

$$e \longrightarrow \mathrm{Var}(e) \xrightarrow[\text{Gaussian Heuristic (✗)}]{} \|e\| = 6\sigma$$

Previous Workflow

$$e \longrightarrow \mathrm{Var}(e) \xrightarrow[\text{Heavier tail}]{} \text{Larger } \|e\|$$

Our Observation

- [CCH+24]: Noises follow *Gaussian* distribution
  - Estimate the variance $\mathrm{Var}(e)$ after each step
  - Finally induce the *Gaussian* bound $\|e\|$
- Contribution 1: Invalidate the Gaussian Heuristic
  - Noises are not Gaussian after deep multiplications

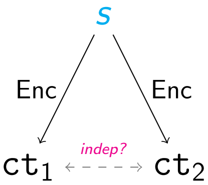
$$\mathrm{Var}(e_1 + e_2) = \mathrm{Var}(e_1) + \mathrm{Var}(e_2)$$

$$\mathrm{Var}(e_1 \cdot e_2) = N \cdot \mathrm{Var}(e_1) \cdot \mathrm{Var}(e_2)$$

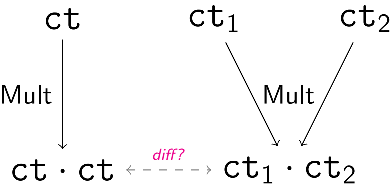
$$\Downarrow ✗$$

$$\|e_1 \cdot e_2\| = \sqrt{N} \cdot \|e_1\| \cdot \|e_2\|$$

Dependencies



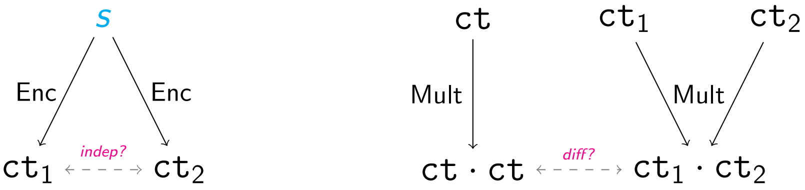
Common Dependencies



Ciphertext Dependencies

- Contribution 2: Study *dependencies* in noise analysis
- Previously, use Independence Heuristic because dependencies are hard
- Two types of dependencies
  - Common dependencies: All $\mathtt{ct}$ share secret key s
  - Ciphertext dependencies: $\mathtt{ct} \cdot \mathtt{ct}$ *v.s.* $\mathtt{ct}_1 \cdot \mathtt{ct}_2$

Dependencies



Common Dependencies   Ciphertext Dependencies

- Contribution 2: Study *dependencies* in noise analysis
- Previously, use Independence Heuristic because dependencies are hard
- Two types of dependencies
  - Common dependencies: All $\mathtt{ct}$ share secret key s
  - Ciphertext dependencies: $\mathtt{ct} \cdot \mathtt{ct}$ *v.s.* $\mathtt{ct}_1 \cdot \mathtt{ct}_2$
- Contribution 3: Find flaws in OpenFHE empirical formula
  - Root cause: Gaussian Heuristic + Independence Heuristic
  - Special cases will violate both

Section 1

Technical Details

Noise in BFV

- Polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(X^N + 1)$, N power of 2
- Noise $e \leftarrow \mathcal{N}(0, \sigma^2)$ with Gaussian coefficients
- Secret key $s \leftarrow \{-1, 0, 1\}$ with uniform ternary coefficients

$$
\begin{aligned}
\mathtt{pk} &= (-as + e_{\mathtt{pk}}, a) \\
\mathtt{ct} &= u_{\mathtt{ct}} \cdot \mathtt{pk} + (\Delta m + e_{\mathtt{ct}}, e'_{\mathtt{ct}}) \\
\mathtt{ct}(s) &= \Delta m + \underbrace{e_{\mathtt{ct}} + u_{\mathtt{ct}} \cdot e_{\mathtt{pk}} + e'_{\mathtt{ct}} \cdot s}_{\text{Noise } v}
\end{aligned}
$$

- Common dependencies: secret key s and noise in public key $e_{\mathtt{pk}}$
- Ciphertext dependencies: ciphertext specific $u_{\mathtt{ct}}$ and $e_{\mathtt{ct}}$

BFV Multiplication

BFV $\mathtt{ct}$ in $\mathcal{R}/Q\mathcal{R}$. Multiplication happens in $\mathcal{R}$.

$$
\begin{aligned}
\mathtt{ct}_1(s) &= \Delta m_1 + v_1 + h_1 Q \\
h_1 Q &\approx c_1 \boxed{s} \\
h_1 &\approx \mu_{\mathtt{ct}_1} \boxed{s} \\
(\mathtt{ct}_1 \otimes \mathtt{ct}_2)(s) &= v_1 h_2 + v_2 h_1 + \cdots \\
&= \boxed{s^2} \cdot (\mu_{\mathtt{ct}_2} e_{\mathtt{ct}_1}) + \cdots
\end{aligned}
$$

BFV Multiplication

BFV $\texttt{ct}$ in $\mathcal{R}/Q\mathcal{R}$. Multiplication happens in $\mathcal{R}$.

$$
\begin{aligned}
\texttt{ct}_1(s) &= \Delta m_1 + v_1 + h_1 Q \\
h_1 Q &\approx c_1 \boxed{s} \\
h_1 &\approx \mu_{\texttt{ct}_1} \boxed{s} \\
(\texttt{ct}_1 \otimes \texttt{ct}_2)(s) &= v_1 h_2 + v_2 h_1 + \cdots \\
&= \boxed{s^2} \cdot \left(\mu_{\texttt{ct}_2} e_{\texttt{ct}_1}\right) + \cdots \\
\left(\bigotimes_i^k \texttt{ct}_i\right)(s) &= \boxed{s^k} \cdot \left(\prod \mu_{\texttt{ct}_i} e_{\texttt{ct}_j}\right) + \cdots
\end{aligned}
$$

Assume relinearize after each multiplication
but introduces negligible noise

BFV Multiplication

BFV $\texttt{ct}$ in $\mathcal{R}/Q\mathcal{R}$. Multiplication happens in $\mathcal{R}$.

$$
\begin{aligned}
\texttt{ct}_1(s) &= \Delta m_1 + v_1 + h_1 Q \\
h_1 Q &\approx c_1 \boxed{s} \\
h_1 &\approx \mu_{\texttt{ct}_1} \boxed{s} \\
(\texttt{ct}_1 \otimes \texttt{ct}_2)(s) &= v_1 h_2 + v_2 h_1 + \cdots \\
&= \boxed{s^2} \cdot \left(\mu_{\texttt{ct}_2} e_{\texttt{ct}_1}\right) + \cdots \\
\left(\bigotimes_i^k \texttt{ct}_i\right)(s) &= \boxed{s^k} \cdot \left(\prod \mu_{\texttt{ct}_i} e_{\texttt{ct}_j}\right) + \cdots \\
\texttt{ct}^k(s) &= \boxed{s^k \mu_{\texttt{ct}}^{k-1}} \cdot e_{\texttt{ct}} + \cdots
\end{aligned}
$$

Assume relinearize after each multiplication
but introduces negligible noise

BFV Multiplication

BFV $\texttt{ct}$ in $\mathcal{R}/Q\mathcal{R}$. Multiplication happens in $\mathcal{R}$.

$$\texttt{ct}_1(s) = \Delta m_1 + v_1 + h_1 Q$$
$$h_1 Q \approx c_1 \boxed{s}$$
$$h_1 \approx \mu_{\texttt{ct}_1} \boxed{s}$$
$$(\texttt{ct}_1 \otimes \texttt{ct}_2)(s) = v_1 h_2 + v_2 h_1 + \cdots$$
$$= \boxed{s^2} \cdot \left(\mu_{\texttt{ct}_2} e_{\texttt{ct}_1}\right) + \cdots$$
$$\left(\bigotimes_i^k \texttt{ct}_i\right)(s) = \boxed{s^k} \cdot \left(\prod \mu_{\texttt{ct}_i} e_{\texttt{ct}_j}\right) + \cdots$$
$$\texttt{ct}^k(s) = \boxed{s^k \mu_{\texttt{ct}}^{k-1}} \cdot e_{\texttt{ct}} + \cdots$$

Assume relinearize after each multiplication
but introduces negligible noise

k-way multiplication contains high degree terms

- s^k in noise *generally*
- $\mu_{\texttt{ct}}^{k-1}$ in noise in specific circuit

BFV Multiplication

BFV $\texttt{ct}$ in $\mathcal{R}/Q\mathcal{R}$. Multiplication happens in $\mathcal{R}$.

$$\texttt{ct}_1(s) = \Delta m_1 + v_1 + h_1 Q$$

$$h_1 Q \approx c_1 \boxed{s} \qquad h_1 Q \approx c_t s^t$$

$$h_1 \approx \mu_{\texttt{ct}_1} \boxed{s}$$

$$(\texttt{ct}_1 \otimes \texttt{ct}_2)(s) = v_1 h_2 + v_2 h_1 + \cdots$$

$$= \boxed{s^2} \cdot \left(\mu_{\texttt{ct}_2} e_{\texttt{ct}_1}\right) + \cdots$$

$$\left(\bigotimes_i^k \texttt{ct}_i\right)(s) = \boxed{s^k} \cdot \left(\prod \mu_{\texttt{ct}_i} e_{\texttt{ct}_j}\right) + \cdots$$

$$\texttt{ct}^k(s) = \boxed{s^k \mu_{\texttt{ct}}^{k-1}} \cdot e_{\texttt{ct}} + \cdots$$

Assume relinearize after each multiplication
but introduces negligible noise

k-way multiplication contains high degree terms

- s^k in noise *generally*
- $\mu_{\texttt{ct}}^{k-1}$ in noise in specific circuit
- Lazy relinearize makes degree higher

BFV Multiplication

BFV ct in $\mathcal{R}/Q\mathcal{R}$. Multiplication happens in $\mathcal{R}$.

$$\mathtt{ct}_1(s) = \Delta m_1 + v_1 + h_1 Q$$

$$h_1 Q \approx c_1 \boxed{s} \qquad\qquad h_1 Q \approx c_t s^t$$

$$h_1 \approx \mu_{\mathtt{ct}_1} \boxed{s}$$

$$(\mathtt{ct}_1 \otimes \mathtt{ct}_2)(s) = v_1 h_2 + v_2 h_1 + \cdots$$

$$= \boxed{s^2} \cdot (\mu_{\mathtt{ct}_2} e_{\mathtt{ct}_1}) + \cdots$$

$$\left(\bigotimes_i^k \mathtt{ct}_i \right)(s) = \boxed{s^k} \cdot \left(\prod \mu_{\mathtt{ct}_i} e_{\mathtt{ct}_j} \right) + \cdots$$

$$\mathtt{ct}^k(s) = \boxed{s^k \mu_{\mathtt{ct}}^{k-1}} \cdot e_{\mathtt{ct}} + \cdots$$

Assume relinearize after each multiplication
but introduces negligible noise

k-way multiplication contains high degree terms

- s^k in noise *generally*
- $\mu_{\mathtt{ct}}^{k-1}$ in noise in specific circuit
- Lazy relinearize makes degree higher

Need to study distribution of

- Product of Gaussians: $\prod f_i$
- Power of one Gaussian: f^k
- Mixed Product of Gaussians: $\prod f_i^{k_i}$

Are they Gaussian?

$\Rightarrow$ Study the Kurtosis!

Kurtosis/Bound of Gaussian

Definition (Kurtosis)

The **Kurtosis** of a zero-mean random variable X is defined as

$$\mathrm{Kurt}(X) = \frac{\mathbb{E}[X^4]}{(\mathbb{E}[X^2])^2} = \frac{\mathbb{E}[X^4]}{\mathrm{Var}(X)^2}$$

- Kurtosis measures *tailedness* [Wes14]
- Gaussian has *constant* Kurt $= 3$

$$\mathrm{Kurt}(\mathcal{N}(0,\sigma^2)) = \frac{3\sigma^4}{(\sigma^2)^2} = 3$$

- Usually bound X using $B = 6\sigma$

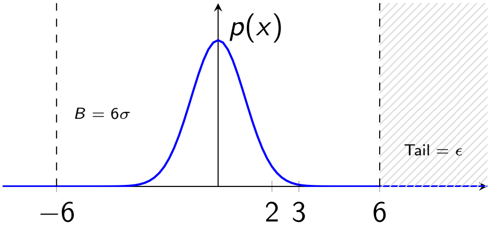
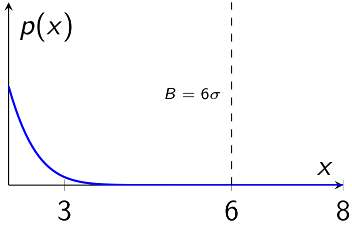


Figure: Gaussian Distribution with 6σ Bound

$$P(|X| > B) = \mathtt{erfc}\left(\frac{B}{\sigma\sqrt{2}}\right) \approx 2^{-28} = \epsilon$$

Kurtosis and Bound

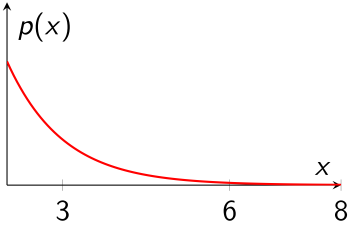


Gaussian Distribution

$p(x) \sim \exp(-x^2)$

$\text{Kurt} = 3$

$B = 6\sigma$

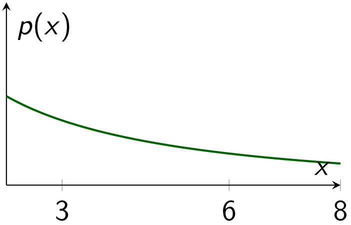


Laplace Distribution

$p(x) \sim \exp(-|x|)$

$\text{Kurt} = 6$

$B = 23.3\sigma$



Generalized Gaussian Distribution

$p(x) \sim \exp(-|x|^{0.5})$

$\text{Kurt} = 25.2$

$B = 43.5\sigma$

- Trend: Tail decays slower $\searrow$, Tail heavier $\nearrow$, Kurtosis $\nearrow$, Bound $\nearrow$
- Kurtosis $\ggg 3 \quad \Rightarrow \quad$ not Gaussian

B derived with the same failing probability ϵ

Main Theorems

Let $f_i \leftarrow \mathcal{N}(0,1)$ be independent Gaussian polynomials

Theorem ($\prod$ Indep)

$F = \prod_i^k f_i$

$$\mathrm{Kurt}(F) = 3 + 3\frac{2^k - 2}{N}$$

Theorem ($\prod$ Same)

$F = f^k$

$$\mathrm{Kurt}(F) = 3 + 3\frac{\binom{2k}{k} - 2}{N}$$

Theorem (Mixed $\prod$)

$F = \prod f_i^{k_i}$

$$\mathrm{Kurt}(F) = 3 + 3\frac{\prod \binom{2k_i}{k_i} - 2}{N}$$

- k is multiplication depth; N is ring dimension
- For practical $N = 2^{16}$, $k > 16$ (or $k > 10$) $\Rightarrow$ Kurt > 6 $\Rightarrow$ F not Gaussian

$\boxed{\textit{Noises are not Gaussian!}}$

in deep multiplications

Main Theorems

Let $f_i \leftarrow \mathcal{N}(0,1)$ be independent Gaussian polynomials

Theorem ($\prod$ Indep)

$F = \prod_i^k f_i$

$$\mathrm{Kurt}(F) = 3 + 3\frac{2^k - 2}{N}$$

Theorem ($\prod$ Same)

$F = f^k$

$$\mathrm{Kurt}(F) = 3 + 3\frac{\binom{2k}{k} - 2}{N}$$

Theorem (Mixed $\prod$)

$F = \prod f_i^{k_i}$

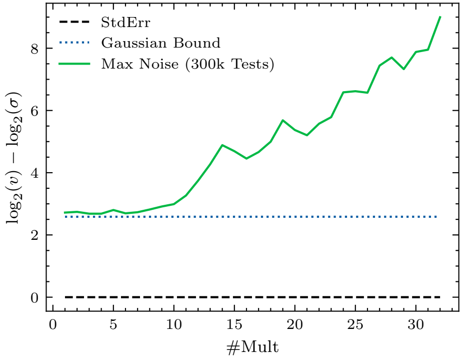
$$\mathrm{Kurt}(F) = 3 + 3\frac{\prod \binom{2k_i}{k_i} - 2}{N}$$

- Remark 1: When $N \to \infty$, Kurt $\to 3$
  - It becomes Gaussian!
  - Exactly Central Limit Theorem
  - But here N is *finite*, so CLT fails
- Remark 2: When k small, Kurt ≈ 3
  - Illusion that noises are *always* Gaussian
  - Past experiments only done for small k
- Remark 3: There is no widely-known name for these distributions

Experimental Results

Gaussian bound fails $\Rightarrow$ Noises not Gaussian

- x-axis: mul-depth k
- Calculate the variance σ^2 thus StdErr σ
- Sample 300k times and record max noise
- Normalize to 0 to see the difference
- y-axis: max noise v.s. StdErr
  - $\log_2(v/\sigma) = \log_2(v) - \log_2(\sigma)$
  - *In logarithm scale!*
- Gaussian bound: 6σ

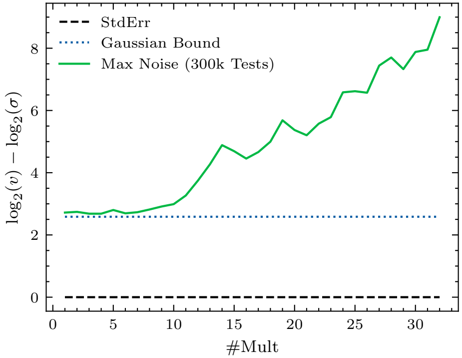


$$e_1 \to e_1 e_2 \longrightarrow \cdots \longrightarrow \prod^{32} e_i$$

Experimental Results

Gaussian bound fails $\Rightarrow$ Noises not Gaussian

- 8 bit overflow $\Rightarrow$ 256σ deviation
- If Gaussian, happens with prob 2^{-47282}
- When k small, noises are Gaussian-like
  - $\text{Kurt} = 3 + 3\frac{2^k - 2}{N}$
  - k small $\Rightarrow$ $\text{Kurt} \approx 3$
- Caused *illusion* that noises are Gaussian!



$$e_1 \to e_1 e_2 \longrightarrow \cdots \longrightarrow \prod^{32} e_i$$

Curve not smooth because of independent samples

Case study: How dependencies affact the variance

We also calculate the variance

Theorem ($\prod$ Indep)

$$Var\left(\prod f_i\right) = N^{k-1}$$

Theorem ($\prod$ Same)

$$Var\left(f^k\right) = k!N^{k-1}$$

Theorem (Mixed $\prod$)

$$Var\left(\prod f_i^{k_i}\right) = \prod k_i!N^{k-1}$$

BFV $\mathtt{ct}$ independent product

$$\mathrm{Var}\left(\left(\bigotimes_i^k \mathtt{ct}_i\right)(s) = \boxed{s^k} \cdot \left(\prod \mu_{\mathtt{ct}_i} e_{\mathtt{ct}_j}\right) + \cdots\right) \approx k! \cdot N^{2k-1} \cdot \mathrm{Var}(s)^k \cdots$$

We are able to exactly derive $k!$ while [BMCM23] used experimental correction factor

$$\boxed{\textit{Common dependencies} \quad \Rightarrow \quad \textit{Variance} \nearrow}$$

Case study: How dependencies affact the variance

We also calculate the variance

Theorem ($\prod$ Indep)

$$Var\left(\prod f_i\right) = N^{k-1}$$

Theorem ($\prod$ Same)

$$Var\left(f^k\right) = k!N^{k-1}$$

Theorem (Mixed $\prod$)

$$Var\left(\prod f_i^{k_i}\right) = \prod k_i!N^{k-1}$$

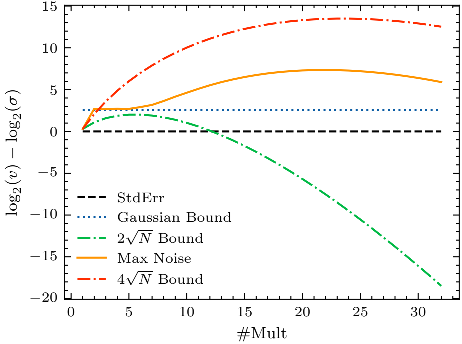
BFV ct dependent product *v.s.* independent product

$$\frac{\mathrm{Var}\left(\mathtt{ct}^k(s) = \boxed{s^k \mu_{\mathtt{ct}}^{k-1}} \cdot e_{\mathtt{ct}} + \cdots\right)}{\mathrm{Var}\left(\left(\bigotimes_i^k \mathtt{ct}_i\right)(s) = \boxed{s^k} \cdot \left(\prod \mu_{\mathtt{ct}_i} e_{\mathtt{ct}_j}\right) + \cdots\right)} \approx (k-1)!$$

$$\boxed{\textit{Ciphertext dependencies} \quad \Rightarrow \quad \textit{Variance} \nearrow}$$

Test the Empirical Formula in OpenFHE

- OpenFHE used $2\sqrt{N}$ *empirical* expansion factor
  - Originally tested using $e \cdot e'$ and $e \cdot s$
- Works for e^k, $\prod e_i$, $\prod s_i$
- Fails for s^k and modulus switching error
  - Does not affect security because of other loose factors
- Contacted OpenFHE and fixed in v1.3.1
  - Use $4\sqrt{N}$ for these special cases



s^k

Implications and Open Questions

- Software needs to track common dependencies and ciphertext dependencies
  - If they want to do average-case noise analysis
  - Means an *application-specific* analysis and parameter generation
  - Agrees with the Application-Aware security model [AAMP24]
  - Compiler can help here!

- What is the true distribution of the noises?
  - Noise analysis needs the bound!
  - We only calculated the kurtosis

$$\text{Kurt} \xrightarrow{\quad ? \quad} \text{Bound } B$$

- How can ciphertext dependencies be used for attack?
  - Recent attacks[1] [GNSJ24, CCP$^+$24, CSBB24] exploited such dependencies in addition $(+)$
  - We are able to analyse dependencies in multiplication $(\times)$.

[1] or misconfiguration as argued in [AAMP24]

Informal Comments on CKKS Average-Case Noise Analysis

- The major term[2] in CKKS noise is

$$m_1 \cdot m_2 \cdot m_3 \cdots (e_{\mathtt{ct}})$$

- We know little about messages m_i (otherwise security implications)
- Previous works assume m_i are *uniform in range* $[-1, 1]$
  - Assumption is not practical
- Need distribution analysis and range analysis depending on applications
- No good ways to do average-case
- Maybe we can only use worst-case analysis, or empirical results

[2] Especially for OpenFHE "reduced error" implementation

Summary

- Noises are not Gaussian after deep multiplications
- Dependencies greatly affect the variance and kurtosis of the noise
- Find flaws in empirical formula in OpenFHE

Thank you!

Questions?

References I

Andreea Alexandru, Ahmad Al Badawi, Daniele Micciancio, and Yuriy Polyakov.
Application-aware approximate homomorphic encryption: Configuring FHE for practical use.
Cryptology ePrint Archive, Report 2024/203, 2024.

Beatrice Biasioli, Chiara Marcolla, Marco Calderini, and Johannes Mono.
Improving and automating BFV parameters selection: An average-case approach.
Cryptology ePrint Archive, Report 2023/600, 2023.

Anamaria Costache, Benjamin R. Curtis, Erin Hales, Sean Murphy, Tabitha Ogilvie, and Rachel Player.
On the precision loss in approximate homomorphic encryption.
In Claude Carlet, Kalikinkar Mandal, and Vincent Rijmen, editors, *SAC 2023*, volume 14201 of *LNCS*, pages 325–345. Springer, Cham, August 2024.

References II

Jung Hee Cheon, Hyeongmin Choe, Alain Passelègue, Damien Stehlé, and Elias Suvanto.
Attacks against the IND-CPA^{D} security of exact FHE schemes.
In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie, editors, *ACM CCS 2024*, pages 2505–2519. ACM Press, October 2024.

Marina Checri, Renaud Sirdey, Aymen Boudguiga, and Jean-Paul Bultel.
On the practical CPA^{D} security of "exact" and threshold FHE schemes and libraries.
In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part III*, volume 14922 of *LNCS*, pages 3–33. Springer, Cham, August 2024.

Qian Guo, Denis Nabokov, Elias Suvanto, and Thomas Johansson.
Key recovery attacks on approximate homomorphic encryption with non-worst-case noise flooding countermeasures.
In Davide Balzarotti and Wenyuan Xu, editors, *USENIX Security 2024*. USENIX Association, August 2024.

References III

Peter H Westfall.
Kurtosis as peakedness, 1905–2014. rip.
The American Statistician, 68(3):191–195, 2014.