Conclusion

Food for thought

- Traditional security notions don’t necessarily apply as-is to FHE
  - Usually giving out decryptions gives the adversary no advantage in IND-CPA
  - But it can on LWE-based schemes
- Attacks against the real cryptosystems (BGV, BFV, TFHE, CKKS, …) are more nuanced
  - Details in the respective papers

References

- On the Security of Homomorphic Encryption on Approximate Numbers
  - Baiyu Li and Daniele Micciancio, EUROCRYPT 2021 (ePrint)
- Attacks Against the INDCPA-D Security of Exact FHE Schemes
  - Jung Hee Cheon et al, ACM CCS 2024 (ePrint)