Lecture 9

Tuesday, October 1, 2024 7:20 PM

References

- Gentry, Craig, Amit Sahai, and Brent Waters. "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based." In *Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, pp. 75-92. Springer Berlin Heidelberg, 2013.
- MIT Lecture Notes https://65610.csail.mit.edu/2024/lec/l08-fhe.pdf
- MIT Lecture Notes https://65610.csail.mit.edu/2024/lec/l09-fhe2.pdf

Bootstrapping

- For a given HE scheme $\mathcal{E}$, we generate (pk, sk).
- Encrypt sk with pk, obtain $\overline{sk}$
- Given ct, encrypt it using pk to get $\overline{ct}$
- Recall in HE, we have

$$Eval(pk, \pi, ct_1, \ldots, ct_n)$$

$$Eval(pk, DEC_{\mathcal{E}}, \overline{ct}, \overline{sk}) = ct$$

$DEC_{\mathcal{E}}(\pi(ct_1, \ldots, ct_n)) = \overline{ct}$, $\overline{ct}, \overline{sk}$