Lecture 11

Tuesday, October 8, 2024 6:09 PM

References

- Van Dijk, Marten, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. "Fully homomorphic encryption over the integers." In *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pp. 24-43. Springer Berlin Heidelberg, 2010.
- Slides https://shaih.github.io/pubs/IHE-Columbia-Theory-Seminar.ppt

Bootstrapping GSW

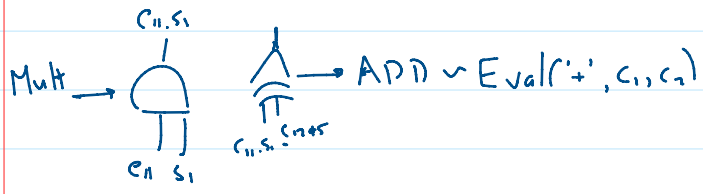
$Eval(ek, C_{Dec}, ct_1, \ldots, ct_\ell)$

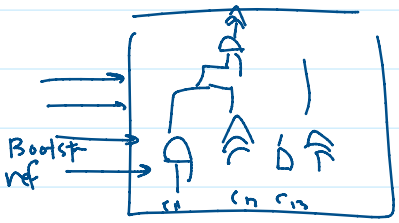
$Eval((Pk), \pi, (\overline{SK}), ct_1, \ldots, ct_m)$

$Dec(C, s) = \underline{C} \cdot s = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ \vdots & & & \\ c_{n1} & \cdots & - & c_{nn} \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$

$= (c_{11} \cdot s_1) + c_{12} \cdot s_2 \ldots -$

Decryption operation can Homo. evaluated in GSW





But $ek = (ct_{s_1}, \ldots, ct_{s_n}) = (Enc(s, s_1), Enc(s, s_2) \ldots, Enc(s, s_n))$

$Eval(ek, C_{Dec}, ct_{s_1}, ct_{s_2}, \ldots, ct_{s_n}) = \hat{C} \neq C$ → "fresh" ciphertext s.t.

$Dec(s, C) = Dec(s, \hat{C})$