2018-09-25

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

HElib

- dot product （inner product）

  $u = [1,2,3,4]$ $\quad$ $\mathrm{v} = [1,2,3,4]$

  $u \cdot v = 1 * 1 + 2 * 2 + 3 * 3 + 4 * 4 = 30$

1. Encrypting each elements
2. Packing into coefficients
3. Packing into subfields(so-called CRT-based packing)

[https://www.slideshare.net/ssuser4c5f79/h-elib]

HElib

- dot product （inner product）

  $u = [1,2,3,4]$ $\quad$ $v = [1,2,3,4]$

  $u \cdot v = 1 * 1 + 2 * 2 + 3 * 3 + 4 * 4 = 30$

Paremeters

1. $m \in Z^+$ defines $\Phi_m(x)$
2. $p : prime\ number, integer\ r$ defines $Z_{p^r}[x]$

[https://www.slideshare.net/ssuser4c5f79/h-elib]

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab