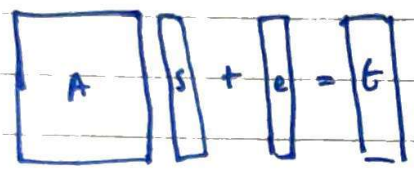
LWE encryption

first we generate a public key and a private key (Alice generates)

Bob



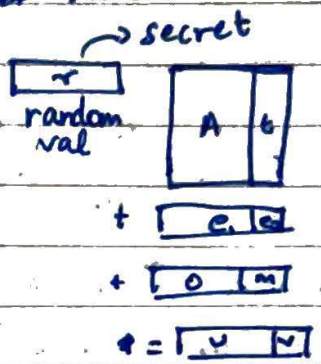

A is random

(s, e) small coefficients

public key $\leftarrow (A, t)$ } Concatenation

$s \rightarrow$ private key

Alice




Alice uses Bobs public key and does $R \times At$ then adds $e_1$ and $e_2$ and the message m she provides the encrypted text of u and v

u and v sent to Bob to recompute the message m

$v = rxt + e_2 + m$

$= r(As + e) + e_2 + m$

$= r(As) + e' + m$

$e'$ ↪ small noise

$us = (rA + e_1)s$

$= rAs + e'$

$x \; v - m$

so Alice can decrypt to obtain

$v - us = m + e'$

obtain the message by removing the noise somehow

→ for each bit of message you need to send large sizes of At