Search R-LWE Problem: Given samples $(a, b = as + e)$, determine s.

(a: random; e: random short)

Decision R-LWE Problem: Given samples either of form $(a, b = as + e) \in R_p \times R_p$

or uniformly random in $R_p \times R_p$

determine which.

Ring-LWE Public Key Cryptosystem

Public Setup: R_p (n and p), moderately large $k \in \mathbb{Z}$.

"small" = coeffs in $\{0, 1, -1\}$

Alice

Bob

Private Key: $s \in R_p$, small, random

Public Key: $(a, b = as + e_1) \in R_p \times R_p$

where $a \in R_p$ random

$e_1 \in R_p$ small, random

$\xleftarrow[\text{public key}]{(a,b)}$

Message: $0 < m < \frac{p}{k}$

Encryption:

$r \in R_p$ random small (ephemeral key)

$e_2, e_3 \in R_p$ random small

$v = ar + e_2$

$w = br + e_3 + km$

$\xrightarrow[\text{ciphertext}]{(v,w)}$

Decryption:

$w - vs$

$= km + br + e_3 - ars - se_2$

$= km + r(as + e_1) + e_3 - ars - se_2$

$= km + \underbrace{re_1 + e_3 - se_2}_{\text{small}}$

round to nearest multiple of k.

$\to km$