Now, we will see how to use LWE to obtain a key agreement protocol

We start with an amortized version of Regev's PKE scheme where each ciphertext encrypts a <u>vector</u> of bits

<u>Vanilla Regev:</u> encryption of single bit $\mu \in \{0,1\}$ is a vector $c = Ar + \mu \cdot \lfloor \frac{q}{2} \rceil \cdot \begin{bmatrix} 0^n \\ 1 \end{bmatrix}$

Encrypting multiple bits: May seem wasteful to use a vector to encrypt a <u>single</u> bit. We can consider a simple variant of Regev encryption where we <u>reuse</u> A to encrypt multiple bits:

amortized Regev

<u>Setup</u>$(1^\lambda, 1^\ell)$: sample $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$

$S \xleftarrow{R} \mathbb{Z}_q^{n \times \ell}$ $\qquad B^T \leftarrow S^T A + E^T \in \mathbb{Z}_q^{\ell \times m}$ $\qquad$ pk: (A, B^T)

$E \xleftarrow{R} \chi^{m \times \ell}$ $\qquad$ sk: S

ℓ secret keys concatenated together

<u>Encrypt</u>$(pk, \mu \in \{0,1\}^\ell)$: sample $r \xleftarrow{R} \{0,1\}^m$

output $(Ar, B^T r + \mu \cdot \lfloor \frac{q}{2} \rfloor)$

<u>Decrypt</u>(sk, ct): output $\lfloor ct_2 - S^T ct_1 \rceil_2$

<u>Correctness</u>: As before: $ct_2 - S^T ct_1 = B^T r + \mu \cdot \lfloor \frac{q}{2} \rfloor - S^T A r = E^T r + \mu \cdot \lfloor \frac{q}{2} \rfloor$

<u>Security</u>: As before: by LWE, $(A, S^T A + E^T) \overset{c}{\approx} (A, R)$ where $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$, $S \xleftarrow{R} \mathbb{Z}_q^{n \times \ell}$, $E \leftarrow \chi^{m \times \ell}$, $R \xleftarrow{R} \mathbb{Z}_q^{\ell \times m}$

↳ in particular, apply a hybrid argument and argue for each row of S (and corresponding row of $S^T A + E^T$)

Public keys are large: if $m = n \log q$, then public key has size $n^2 \log q$ – for instance: $n \sim 600$, $q \sim 2^{12}$ $\quad$ ($\sim$ 550 KB)

↳ Can shrink public keys to n^2 $\quad$ (Will leave as exercise; hint: sample secret key from error distribution)

↳ Can shrink further using ring LWE ($O(n)$ public key size)

Lattice-based key exchange. Recall Diffie-Hellman:

<u>Alice</u>		<u>Bob</u>
$x \xleftarrow{R} \mathbb{Z}_p$	$\xrightarrow{g^x}$	$y \xleftarrow{R} \mathbb{Z}_p$
	$\xleftarrow{g^y}$	

$k \leftarrow \mathrm{KDF}(g, g^x, g^y, g^{xy})$

$\longrightarrow$

<u>Alice</u>		<u>Bob</u>
$A \xleftarrow{R} \mathbb{Z}_q^{n \times n}$		
$S_1, E_1 \leftarrow \chi^{n \times k_1}$		
$B_1^T \leftarrow S_1^T A + E_1^T$		
	$\xrightarrow{A,\ B_1}$	
		$S_2, E_2 \leftarrow \chi^{n \times k_2}$
		$B_2 \leftarrow A S_2 + E_2$
	$\xleftarrow{B_2}$	
compute $C \leftarrow \lceil S_1^T B_2 \rfloor$		compute $C \leftarrow \lceil B_1^T S_2 \rfloor_{2^T}$

in practice: A is very large (but random)

↳ derive from a PRG and Alice sends PRG seed

(relies on random oracle heuristic)

↳ output most significant T bits of output

$k \leftarrow \mathrm{KDF}(A, B_1, B_2, C)$

↳ $C \in \{0,1\}^{k_1 \times k_2}$

<u>Main idea:</u> exponentiation $\longrightarrow$ noisy linear combination

<u>Correctness</u>: $S_1^T B_2 = S_1^T(AS_2 + E_2) = S_1^T A S_2 + \underline{S_1^T E_2} \pmod q$

↳ both sampled from error distribution, so product is small

if errors are B-bounded, then $\|S_1^T E_2\|_\infty \le n \cdot B^2$

$B_1^T S_2 = (S_1^T A + E_1^T) S_2 = S_1^T A S_2 + \underline{E_1^T S_2} \pmod q$

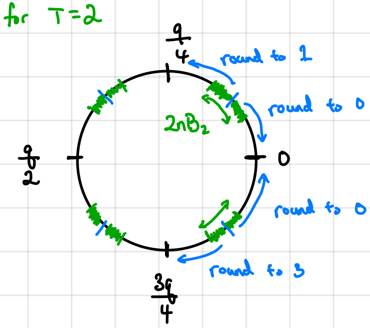
↳ also bounded by $\|E_1 S_2\|_\infty \le n B^2$

<u>Hope</u>: $\lceil S_1^T B_2 \rfloor = \lceil B_1^T S_2 \rfloor$

This holds as long as $S_1^T B_2$ and $B_1^T S_2$ are far from a "rounding boundary"

For simplicity, consider case where q is a power of two

Case for $T=2$



By LWE: $(S_1^T A + E_1^T) \overset{c}{\approx} U$ where $U \xleftarrow{R} \mathbb{Z}_q^{k_1 \times n}$

Consider any component of $B_1 S_2 = (S_1^T A + E_1^T) S_2$

↳ Component is computationally indistinguishable from Uniform$(\mathbb{Z}_q)$

holds as long as at least one element in each row of $(S_1^T A + E_1^T)$ is invertible, which holds with prob. $1 - \text{negl}(n)$ for random matrix

(but components might be correlated)

Rounding error occurs only if $B_1^T S_2$ falls into a rounding boundary

Probability that individual component of $B_1^T S_2$ falls into boundary region is $\le \dfrac{2^T \cdot 2nB^2}{q} = \dfrac{2^{T+1} n B^2}{q}$

By union bound over all $k_1 k_2$ components

$$\Pr\left[\lceil B_1^T S_2 \rfloor_{2^T} \ne \lceil B_1^T S_2 - E_1 S_2 \rfloor_{2^T}\right] \le \frac{2^{T+1} n B^2 k_1 k_2}{q}$$

Similar calculation shows that

$$\Pr\left[\lceil S_1^T B_2 \rfloor_{2^T} \ne \lceil S_1^T B_2 - S_1^T E_2 \rfloor_{2^T}\right] \le \frac{2^{T+1} n B^2 k_1 k_2}{q}$$

If $q \gg 2^{T+1} \cdot n B^2 k_1 k_2$, then $\lceil B_1^T S_2 \rfloor_{2^T} = \lceil B_1^T S_2 - E_1 S_2 \rfloor_{2^T} = \lceil S_1^T A S_2 \rfloor_{2^T}$

$= \lceil S_1^T B_2 - S_1^T E_2 \rfloor_{2^T} = \lceil S_1^T B_2 \rfloor_{2^T}$ and Alice, Bob agree on the shared key

Can reduce error rates via a key reconciliation mechanism [See FrodoKEM for details]

Security (against passive eavesdroppers): $(\overbrace{A,\ B_1^T = S_1^T A + E_1^T,\ B_2 = AS_2 + E_2}^{\text{public messages}},\ \overbrace{\lceil S_1^T B_2 \rfloor_{2^T}}^{\text{shared key}})$

$$\overset{c}{\approx} \quad \text{(LWE)}$$

$$(A,\ B_1^T = S_1^T A + E_1^T,\ U_2,\ \lceil S_1^T U_2 \rfloor_{2^T}) \quad \text{where } U_2 \xleftarrow{R} \mathbb{Z}_q^{n \times k_2}$$

$$\overset{s}{\approx} \quad (\text{as long as } q > 2^{T+1} \cdot B \cdot n k_1)$$

$$(A,\ B_1^T = S_1^T A + E^T,\ U_2,\ \lceil S_1^T U_2 + \tilde{E}^T \rfloor_{2^T}) \quad \text{where } \tilde{E} \leftarrow \chi^{n \times k_1}$$

$$\overset{c}{\approx} \quad (\text{LWE and } q \text{ is power of two})$$

$$(A,\ U_1,\ U_2,\ U_3) \quad \text{where } U_1 \xleftarrow{R} \mathbb{Z}_q^{k_1 \times n},\ U_2 \xleftarrow{R} \mathbb{Z}_q^{n \times k_2},\ U_3 \xleftarrow{R} \mathbb{Z}_{2^T}^{k_1 \times k_2}$$

$$\overset{c}{\approx} \quad (\text{LWE})$$

$$(A,\ B_1^T = S_1^T A + E_1^T,\ B_2 = AS_2 + E_2,\ U_3)$$

Thus, under LWE, distribution of shared key is computationally close to uniform random even given the public messages.