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 vector of bits.

**Vanilla Regev:** encryption of single bit \( \mu \in \{0,1\} \) is a vector \( c = A r + \mu \cdot \frac{1}{\sqrt{m}} \cdot \left[ \begin{array}{c} o \\ i \end{array} \right] \).

Encoding multiple bits: May seem wasteful to use a vector to encrypt a single bit. We can consider a simple variant of Regev encryption where we reuse \( A \) to encrypt multiple bits:

\[
\text{Setup}(\lambda, \ell) : \text{Sample } A \in \mathbb{Z}_q^{m \times \lambda}, \ B \leftarrow \mathbb{S}^T A + \mathbb{E} \in \mathbb{Z}_q^{\ell \times m}, \ \text{pk} : (A, B^T) \ \\
\text{sk} : S
\]

\[
\text{Encrypt}(\mu) : \text{Sample } r \in \mathbb{Z}_q^\ell \ \\
\text{output } (Ar, B^T + \mu \cdot \frac{1}{\sqrt{m}})
\]

\[
\text{Decrypt}(sk, ct) : \text{output } lct = S^T ct
\]

**Correctness:** As before: \( ct^T = B^T r + \mu \cdot \frac{1}{\sqrt{m}} = S^T A r = E^T r + \mu \cdot \frac{1}{\sqrt{m}} \)

**Security:** As before: by LWE, \((A, S^T A + E) \\sim (A, R)\) where \( A \in \mathbb{Z}_q^{m \times \lambda}, \ S \in \mathbb{Z}_q^{\ell \times \lambda}, \ E \in \mathbb{X}^m, \ R \in \mathbb{Z}_q^{\ell \times m}, \).

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

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

- Can shrink public keys to \( n^2 \) (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:

Alice: \( x \in \mathbb{Z}_q \) \rightarrow \( g^x \) \rightarrow \( B \rightarrow y \in \mathbb{Z}_q \) \leftarrow \( g^y \) \rightarrow \( k = \text{KDF}(g, g^x, g^y) \)

Bob: \( A \in \mathbb{Z}_q^{m \times n} \) \rightarrow \( S, E \leftarrow \mathbb{X}^{\ell \times n} \) \rightarrow \( B^T = S^T A + E \) \leftarrow \( B \rightarrow \)

compute \( C \leftarrow [B, B^T]_2 \) \leftarrow \( k \in \text{KDF}(A, B, C) \text{ output most significant } T \) bits of output

Main idea: exponentiation \rightarrow noisy linear combination
Correctness:
\[ S^T B_z = S^T (A S_z + E_z) = S^T A S_z + S^T E_z \pmod{q} \]

- Let both sampled from error distribution, so product is small
- if errors are B-bounded, then \( \| S^T E_z \|_2 \leq n \cdot B \)

\[ \bar{B}_z^T S_z = (S^T A + E_z) S_z = S^T A S_z + E_z S_z \pmod{q} \]

- Also bounded by \( \| E_z S_z \|_2 \leq n \cdot B \)

Hope: \( [S^T B_z] = [\bar{B}_z S_z] \)

This holds as long as \( S^T B_z \) and \( \bar{B}_z S_z \) are far from a "rounding boundary".

For simplicity, consider case where \( g \) is a power of two.

Case for \( T = 2 \)

By \( \text{LWE} \): \( (S^T A + E_z) \approx U \), where \( U \approx Z_n \)

Consider any component of \( B_z S_z = (S^T A + E_z) S_z \)

- Component is computationally indistinguishable from Uniform (\( U \))

Rounding error occurs only if \( B_z S_z \) falls into a rounding boundary.

Probability that individual component of \( B_z S_z \) falls into boundary region is

\[ \Pr [ B_z S_z ] \approx \Pr [ B_z S_z - E_z S_z ] \]

- By union bound over all \( k \) components

\[ \Pr [ B_z S_z - E_z S_z ] \leq 2^{T+1} n B^2 k \cdot k_e \]

Similar calculation shows that

\[ \Pr [ S^T B_z ] \leq 2^{T+1} n B^2 k \cdot k_e \]

If \( g \approx 2^{T+1} n B^2 k \cdot k_e \), then \( B_z S_z ] \approx [ S^T B_z - S^T E_z ] \)

- \( B_z S_z ] \approx [ S^T B_z - S^T E_z ] \) 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): \( (A, B_t^T \approx S^T A + E_t, B_t^T \approx A S_z + E_z, \ [S^T B_z]) \)

\[ \approx \text{LWE} \]

\[ (A, U_t^T = S^T A + E_t, U_t = S^T U_t] \] \( \approx \) \( (\text{LWE}) \) \( (A, U_t^T = S^T A + E_t, U_t = S^T U_t] \)

\[ \approx (\text{LWE}) \]

\[ (A, B_t^T = S^T A + E_t, U_t = S^T U_t] \] \( \approx \) \( (\text{LWE}) \) \( (A, B_t^T = S^T A + E_t, U_t = S^T U_t] \)

Thus, under \( \text{LWE} \), distribution of shared key is computationally close to uniform random even given the public messages.