**Probable next steps:**

When I profile the VOLE implementation using Xcode instruments, I realized that there is a bottleneck in the following function:

* Lpn\_mtx\_indices
  + rng: &mut AesRng
  + rand\_core::Block\_rng::generate and set
* AesRng::from\_seed(seed)