I am interested in exploring noir to make some aes proofs as they are used in TLS. I notice that the standard lib has support for AES in CBC mode. The mode I would like to use is Galois Counter Mode which is a subset of the Counter Mode. What would be the best approach to add these modes? Would it be best to start from scratch in noir? Or would it be reasonable to open a PR to the standard library? Would love some insight or feedback from the maintainers.