At SKALE we need to implement a Hash(Keccack) based-cipher - the reason is we need to be able to decrypt in Solidity smart contract as a part of a fraud claim.

t the moment we are using an ad-hock counter-based CIPHER that I cooked up - essentially XORING plaintext with consequitive hashes of COUNTER | KEY

Can anyone point to a spec on a simple HASH-based cipher that is cheap and easy to do in Solidity?