



NOTE: This assumes a relatively long-enough master secret like  $> 80$  bits. This is employed mainly to guarantee the forward secrecy.