

ParagonIE_Sodium_Crypto
<ul style="list-style-type: none"> <li>+ const aead_chacha20poly1305_KEYBYTES</li> <li>+ const aead_chacha20poly1305_NSECBYTES</li> <li>+ const aead_chacha20poly1305_NPUBBYTES</li> <li>+ const aead_chacha20poly1305_ABBYTES</li> <li>+ const aead_chacha20poly1305_IETF_KEYBYTES</li> <li>+ const aead_chacha20poly1305_IETF_NSECBYTES</li> <li>+ const aead_chacha20poly1305_IETF_NPUBBYTES</li> <li>+ const aead_chacha20poly1305_IETF_ABBYTES</li> <li>+ const aead_xchacha20poly1305_IETF_KEYBYTES</li> <li>+ const aead_xchacha20poly1305_IETF_NSECBYTES</li> <li>et 23 de plus...</li> </ul>
<ul style="list-style-type: none"> <li>+ static aead_xchacha20poly1305_ietf_decrypt( \$message=", \$ad=", \$nonce=", \$key=")</li> <li>+ static aead_xchacha20poly1305_ietf_encrypt( \$message=", \$ad=", \$nonce=", \$key=")</li> <li>+ static auth(\$message, \$key)</li> <li>+ static auth_verify(\$mac, \$message, \$key)</li> <li>+ static box(\$plaintext, \$nonce, \$keypair)</li> <li>+ static box_beforenm(\$sk, \$pk)</li> <li>+ static box_keypair()</li> <li>+ static box_seed_keypair(\$seed)</li> <li>+ static box_keypair_from_secretkey_and_publickey(\$sKey, \$pKey)</li> <li>+ static box_secretkey(\$keypair)</li> <li>et 13 de plus...</li> <li># static scalarmult_throw_if_zero(\$q)</li> </ul>

