

const

+aead_chacha20poly1305
_ABYTES
+aead_chacha20poly1305
_IETF_ABYTES
+aead_chacha20poly1305
_IETF_KEYBYTES
+aead_chacha20poly1305
_IETF_NPUBBYTES
+aead_chacha20poly1305
_IETF_NSECBYTES
+aead_chacha20poly1305
_KEYBYTES
+aead_chacha20poly1305
_NPUBBYTES
+aead_chacha20poly1305
_NSECBYTES
+aead_xchacha20poly1305
_IETF_ABYTES
+aead_xchacha20poly1305
_IETF_KEYBYTES
...

ParagonIE_Sodium_Crypto32

+ const aead_xchacha20poly1305
_IETF_NSECBYTES
+ const aead_xchacha20poly1305
_IETF_NPUBBYTES
+ const box_curve25519xsalsa20poly1305
_SEEDBYTES
+ const box_curve25519xsalsa20poly1305
_PUBLICKEYBYTES
+ const box_curve25519xsalsa20poly1305
_SECRETKEYBYTES
+ const box_curve25519xsalsa20poly1305
_BEFORENMBYTES
+ const box_curve25519xsalsa20poly1305
_NONCEBYTES
+ const box_curve25519xsalsa20poly1305
_MACBYTES
+ const box_curve25519xsalsa20poly1305
_BOXZEROBYTES
+ const box_curve25519xsalsa20poly1305
_ZEROBYTES
et 13 de plus...

+ static aead_xchacha20poly1305
_ietf_decrypt(\$message=",
\$ad=", \$nonce=", \$key=")
+ static aead_xchacha20poly1305
_ietf_encrypt(\$message=",
\$ad=", \$nonce=", \$key=")
+ static auth(\$message,
\$key)
+ static auth_verify
(\$mac, \$message, \$key)
+ static box(\$plaintext,
\$nonce, \$keypair)
+ static box_beforenm
(\$sk, \$pk)
+ static box_keypair()
+ static box_seed_keypair
(\$seed)
+ static box_keypair
_from_secretkey_and
_publickey(\$sKey, \$pKey)
+ static box_secretkey
(\$keypair)
et 13 de plus...
static scalarmult_throw
_if_zero(\$q)