

ParagonIE_Sodium_Crypto

```
+ const aead_chacha20poly1305
  _KEYBYTES
+ const aead_chacha20poly1305
  _NSECBYTES
+ const aead_chacha20poly1305
  _NPUBBYTES
+ const aead_chacha20poly1305
  _ABYTES
+ const aead_chacha20poly1305
  _IETF_KEYBYTES
+ const aead_chacha20poly1305
  _IETF_NSECBYTES
+ const aead_chacha20poly1305
  _IETF_NPUBBYTES
+ const aead_chacha20poly1305
  _IETF_ABYTES
+ const aead_xchacha20poly1305
  _IETF_KEYBYTES
+ const aead_xchacha20poly1305
  _IETF_NSECBYTES
et 23 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)
```

Crypto