ParagonIE_Sodium_Core_Util
+ static compare(\$left,
\$right, \$len=null)
+ static declareScalarType (&\$mixedVar=null, \$type
='void', \$argumentIndex=0)
+ static intToChr(\$int)
+ static memcmp(\$left,
\$right)
+ static strlen(\$str) + static substr(\$str,
\$start=0, \$length=null)
+ static verify_16(\$a, \$b)
+ static verify_32(\$a, \$b)
+ static xorStrings(
\$a, \$b)
static hash_update (&\$hs, \$data)
Δ
ParagonIE_Sodium_Core
_ChaCha20
L static rotate(f)(fn)
+ static rotate(\$v, \$n) + static stream(\$len
=64, \$nonce=", \$key=")
+ static ietfStream(
\$len, \$nonce=", \$key=")
+ static ietfStreamXorlc (\$message, \$nonce=",
\$key=", \$ic=")
+ static streamXorIc
(\$message, \$nonce='', \$key='', \$ic='')
<u> </u>
ParagonIE_Sodium_Core
_HChaCha20
+ static hChaCha20(\$in =", \$key=", \$c=null)
static hChaCha20Bytes
(array \$ctx)
Α
ParagonIE_Sodium_Core
XChaCha20
+ static stream(\$len =64, \$nonce=", \$key=")
+ static ietfStream(
\$len=64, \$nonce='',
\$key=")
+ static streamXorlc (\$message, \$nonce=",
\$key=", \$ic=")
+ static ietfStreamXorlc
(\$message, \$nonce='', \$key='', \$ic='')
\ \
Ť
XChaCha20