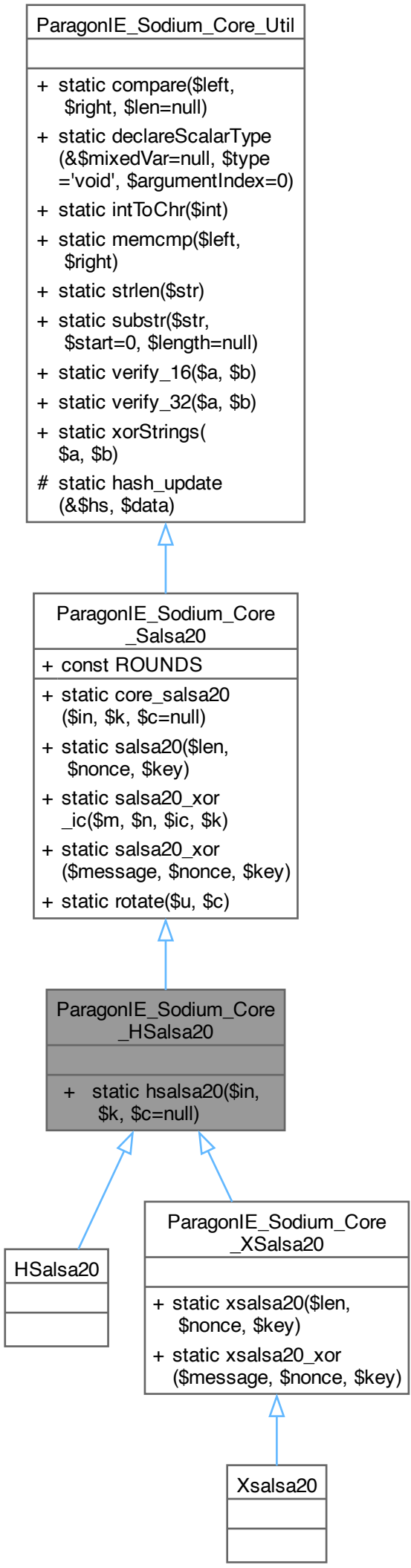
ParagonIE_Sodium_Core_Util
+ static compare($left, $right, $len=null)
+ static declareScalarType (&$mixedVar=null, $type ='void', $argumentIndex=0)
+ static intToChr($int)
+ static memcmp($left, $right)
+ static strlen($str)
+ static substr($str, $start=0, $length=null)
+ static verify_16($a, $b)
+ static verify_32($a, $b)
+ static xorStrings($a, $b)
# static hash_update (&$hs, $data)
ParagonIE_Sodium_Core _Salsa20
+ const ROUNDS
+ static core_salsa20 ($in, $k, $c=null)
+ static salsa20($len, $nonce, $key)
+ static salsa20_xor _ic($m, $n, $ic, $k)
+ static salsa20_xor ($message, $nonce, $key)
+ static rotate($u, $c)
ParagonIE_Sodium_Core _HSalsa20
+ static hsalsa20($in, $k, $c=null)
HSalsa20
ParagonIE_Sodium_Core _XSalsa20
+ static xsalsa20($len, $nonce, $key)
+ static xsalsa20_xor ($message, $nonce, $key)
Xsalsa20