

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_Core32_Util



ParagonIE_Sodium_Core32_Curve25519_H
static \$base # static \$base2 # static \$d # static \$d2 # static \$sqrtm1



ParagonIE_Sodium_Core32_Curve25519
+ static fe_0() + static fe_1() + static fe_copy(ParagonIE _Sodium_Core32_Curve25519_Fe \$f) + static fe_isnegative (ParagonIE_Sodium_Core32 _Curve25519_Fe \$f) + static fe_neg(ParagonIE _Sodium_Core32_Curve25519 _Fe \$f) + static fe_invert(Paragon IE_Sodium_Core32_Curve25519 _Fe \$Z) + static fe_pow22523 (ParagonIE_Sodium_Core32 _Curve25519_Fe \$z) + static fe_sub(ParagonIE _Sodium_Core32_Curve25519 _Fe \$f, ParagonIE_Sodium _Core32_Curve25519_Fe \$g) + static ge_add(ParagonIE _Sodium_Core32_Curve25519 _Ge_P3 \$p, ParagonIE_Sodium _Core32_Curve25519_Ge_Cached \$q) + static ge_madd(ParagonIE _Sodium_Core32_Curve25519 _Ge_P1p1 \$R, ParagonIE_Sodium _Core32_Curve25519_Ge_P3 \$p, ParagonIE_Sodium_Core32_Curve25519 _Ge_Precomp \$q) et 15 de plus...



ParagonIE_Sodium_Core32_Ed25519
+ const KEYPAIR_BYTES + const SEED_BYTES
+ static keypair() + static secretkey(\$keypair) + static publickey(\$keypair) + static pk_to_curve25519(\$pk) + static sk_to_pk(\$sk) + static sign_detached (\$message, \$sk)



ParagonIE_Sodium_Core32_X25519
+ static edwards_to_montgomery (ParagonIE_Sodium_Core32 _Curve25519_Fe \$edwardsY, ParagonIE_Sodium_Core32_Curve25519 _Fe \$edwardsZ) + static crypto_scalarmult _curve25519_ref10_base(\$n)