

ParagonIE_Sodium_Core_Util
<pre> + 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) </pre>



ParagonIE_Sodium_Core_Curve25519_H
<pre> + const L # static \$base # static \$base2 # static \$d # static \$d2 # static \$sqrtm1 # static \$invsqrtamd # static \$sqrtadm1 # static \$onemsqd # static \$sqdmone </pre>



ParagonIE_Sodium_Core_Curve25519
<pre> + static fe_0() + static fe_1() + static fe_copy(ParagonIE _Sodium_Core_Curve25519_Fe \$f) + static fe_frombytes(\$s) + static fe_isnegative (ParagonIE_Sodium_Core _Curve25519_Fe \$f) + static fe_mul(ParagonIE _Sodium_Core_Curve25519 _Fe \$f, ParagonIE_Sodium _Core_Curve25519_Fe \$g) + static fe_neg(ParagonIE _Sodium_Core_Curve25519 _Fe \$f) + static fe_sq(ParagonIE _Sodium_Core_Curve25519 _Fe \$f) + static fe_sq2(ParagonIE _Sodium_Core_Curve25519 _Fe \$f) + static fe_invert(Paragon IE_Sodium_Core_Curve25519 _Fe \$Z) et 27 de plus... </pre>



ParagonIE_Sodium_Core_Ed25519
<pre> + const KEYPAIR_BYTES + const SEED_BYTES + const SCALAR_BYTES + static keypair() + static secretkey(\$keypair) + static publickey(\$keypair) + static pk_to_curve25519(\$pk) + static sk_to_pk(\$sk) + static sign_detached (\$message, \$sk) + static scalar_complement(\$s) + static scalar_random() + static scalar_negate(\$s) + static scalar_add(\$a, \$b) + static scalar_sub(\$x, \$y) </pre>



ParagonIE_Sodium_Core_Ristretto255
<pre> + const crypto_core_ristretto255 _HASHBYTES + const HASH_SC_L + const CORE_H2C_SHA256 + const CORE_H2C_SHA512 + static fe_cneg(ParagonIE _Sodium_Core_Curve25519 _Fe \$f, \$b) + static fe_abs(ParagonIE _Sodium_Core_Curve25519 _Fe \$f) + static ristretto255 _sqrt_ratio_m1(ParagonIE _Sodium_Core_Curve25519 _Fe \$u, ParagonIE_Sodium _Core_Curve25519_Fe \$v) + static ristretto255 _point_is_canonical(\$s) + static ristretto255 _frombytes(\$s, \$skipCanonical Check=false) + static ristretto255 _p3_tobytes(ParagonIE _Sodium_Core_Curve25519 _Ge_P3 \$h) + static ristretto255 _elligator(ParagonIE _Sodium_Core_Curve25519 _Fe \$t) + static ristretto255 _from_hash(\$h) + static is_valid_point(\$p) + static ristretto255 _add(\$p, \$q) et 14 de plus... # static h2c_string_to _hash_sha256(\$hLen, \$ctx, \$msg) # static h2c_string_to _hash_sha512(\$hLen, \$ctx, \$msg) # static _string_to_element (\$ctx, \$msg, \$hash_alg) </pre>