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 Curve25519_H const L # static \$base # static \$base2 # static \$d static \$d2 # static \$sqrtm1 # static \$invsqrtamd # # static \$sqrtadm1 static \$onemsqd # # static \$sqdmone ParagonIE_Sodium_Core _Curve25519 + 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 _Fe \$Z) et 27 de plus... ParagonIE_Sodium_Core X25519 + static fe_cswap(ParagonIE Sodium_Core_Curve25519 Fe \$f, ParagonIE_Sodium Core_Curve25519_Fe \$g, \$b=0)

_Core_Curve25519_Fe \$g, \$b=0)
+ static edwards_to_montgomery
(ParagonIE_Sodium_Core_Curve25519
_Fe \$edwardsY, ParagonIE_Sodium
_Core_Curve25519_Fe \$edwardsZ)
+ static crypto_scalarmult
_curve25519_ref10_base(\$n)

