## 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)



+ROUNDS

## ParagonIE\_Sodium\_Core Salsa20

- + 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)