

de-
bug
prints
?
?
rng.h
randombytes.h
??

??
?

Categoría	Ficheros (.c/.h)	Descripción Funcional
Núcleo del esquema	makem, indcpa api kyber_wrapper verify	indcpakem
Matemáticas	poly, polyvec ntt, reduce cbd	R_q $q = 3329$
Hashing	fips202, sha, symmetric	
Sistema	randombytes params	

??
?

Categoría	Ficheros (.c/.h)	Descripción Funcional
Núcleo del esquema	makem, SABER_indcpa	SABER_indcpakem
	api	
	saber_wrapper	
	verify	
Matemáticas	poly, pack_unpack	R_q
	poly_mul	
	cbd	
Hashing	fips202	
Sistema	randombytes	
	SABER_params	

?
?

?? ?		
Categoría	Ficheros (.c/.h)	Descripción Funcional
Núcleo del esquema	code, hqc	codehqc
	api	
	hqc_wrapper	
	parsing	
Matemáticas	reed_solomon, reed_muller	
	gf, gf2x, fft	
	vector	
Hashing	fips202, shake_ds, shake_prng	
Sistema	randombytes	
	parameters, domains	
wrap- per		
?		
?		
AlgorithmWrapper.h		
??		
link- ing		
buffers		