SEAL Ciphertext Serialization

Assumptions:
uint64_t: 8 bytes
double: 8 bytes
byte: 8 bits

# Octet	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	
1	SEAL HEADER, always 0xA15E		header size (bytes)	SEAL Major Version	SEAL Minor Version	comp_mode_type	future use		Size of SEAL Header: 16 Bytes
2	size of entire serialized object including header								
…	serialized ciphertext data								
…	...								
…	...								
…	...								

serialized ciphertext data:

3	params_id_type …								params_id_type decribes parameters that are hashed with blake2b hash function (HashOutputSize=4*uint64)
4	… params_id_type …								
5	… params_id_type …								
6	… params_id_type								
7	is_ntt	# bytes in uint64 … (= 8)							
8	... # bytes in uint64	poly modulus degree (uint64)							
9	… poly_modulus_degree	coeff_modulus_size (uint64)							
10	… coeff_modulus_size	scale (double)							
11	… scale	data							

data (concrete):

consists of serialization of DynArray<ct_coeff_type>

11	empty	size of DynArray / number of elements							data array of uint64
…		ciphertext coefficient …							
…		… ciphertext coefficient …							
…		… ciphertext coefficient …							
…		… ciphertext coefficient …							
…		… ciphertext coefficient …							
…		… ciphertext coefficient							
…		…							
…		empty							

data (seed): has_seed_marker() == true <==> (data_.size() && (size_ == 2)) ? (data(1)[0] == 0xFFFFFFFFFFFFFFFFULL) : false

11	empty	size of DynArray / number of elements							data array of uint64
…		ciphertext coefficient …							
…		… ciphertext coefficient …							
…		… ciphertext coefficient …							
…		… ciphertext coefficient …							
…		… ciphertext coefficient							
…		prng_type	seed						UniformRandomGeneratorInfo prng:_type: shake256 and blake2xb are supported seed has constant length of 8*uint64
…		seed							
…		seed							
		seed							
		seed							
		seed							
		seed							
		seed							
		empty							

Notes

Seal uses compression on each component individually instead of compressing all components together, eg. seed is compressed independently from ciphertext coefficients if compression is turned on