CS577 - C BASED VLSI DESIGN

ADDURI SAI SRI DATTA - 190101003
GOLI AANANDA VARDHAN - 180101026
KAJAL KHOBRAGADE - 224101028
PATHLAVATH SRIKANTH - 190101060
GYAN RATNA - 224156016

ZIP FILE NAME :

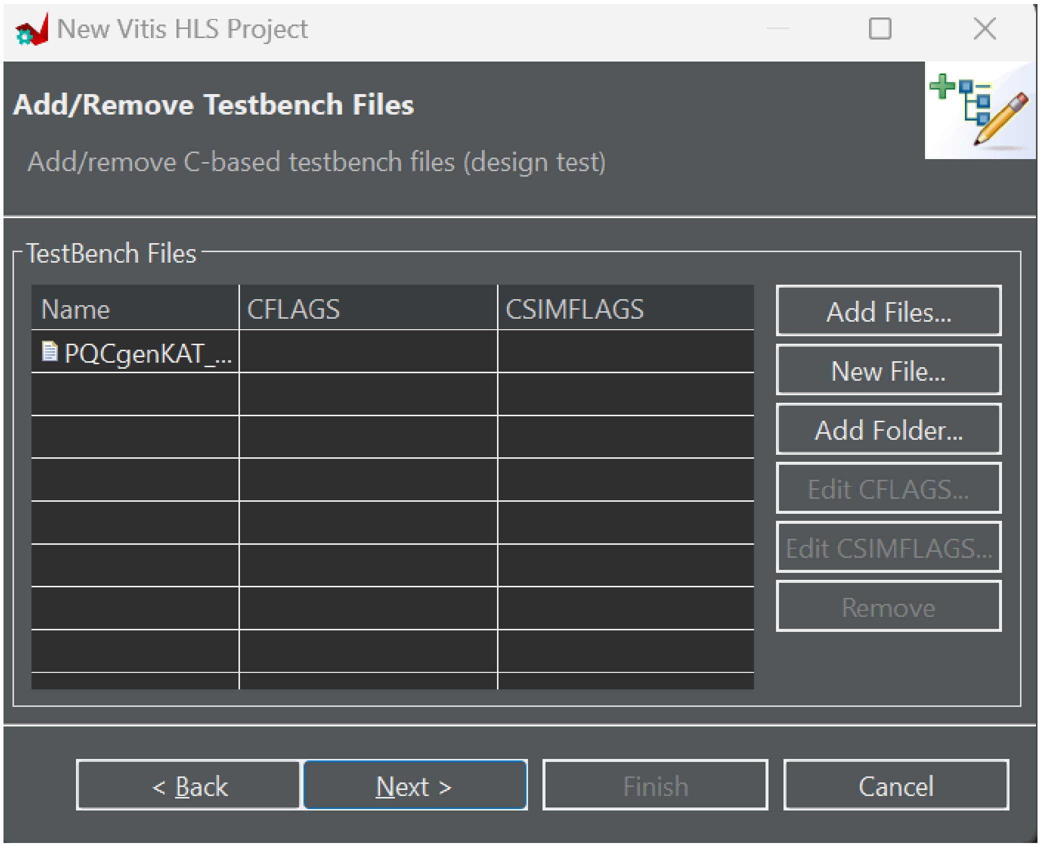
Our Top function was crypto_kem_enc and it is available in the file “kem.c”

Target Device : xc7a200t-fbg676-2

Product Family : artix7

Modifications Made:

1) “PQCgenKAT kem.c” out of all files available, was placed under Testbench and all other files are placed under the source.



New Vitis HLS Project

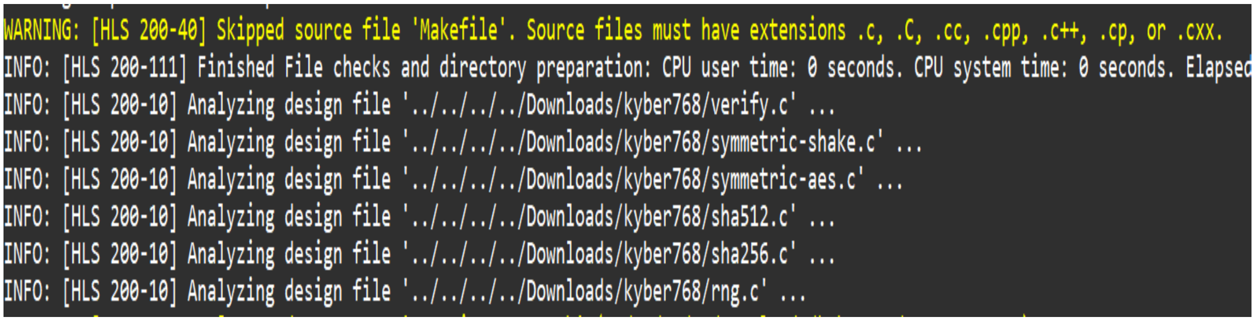
Add/Remove Testbench Files

Add/remove C-based testbench files (design test)

TestBench Files

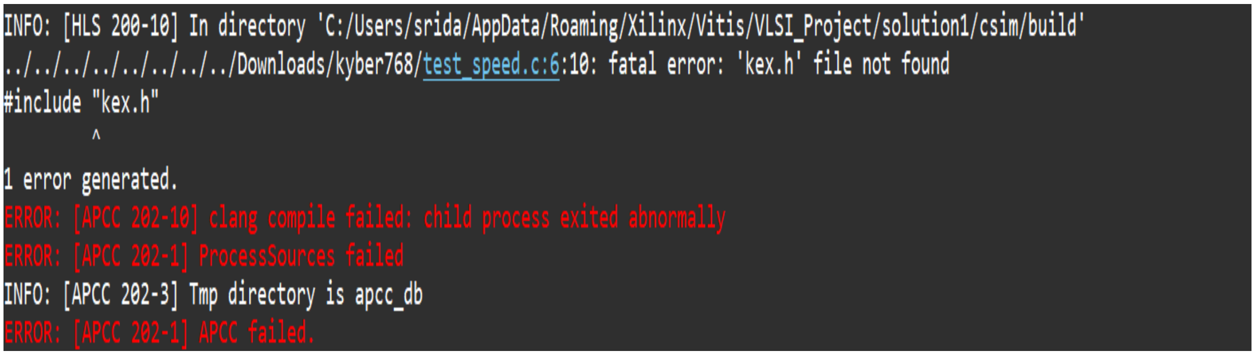
Name	CFLAGS	CSIMFLAGS
PQCgenKAT_...		

2) On synthesizing a warning stating that “Makefile” was skipped and the source file must contain files with extension .c, .cpp, etc. only appeared, so we detached “Makefile” from the source files.



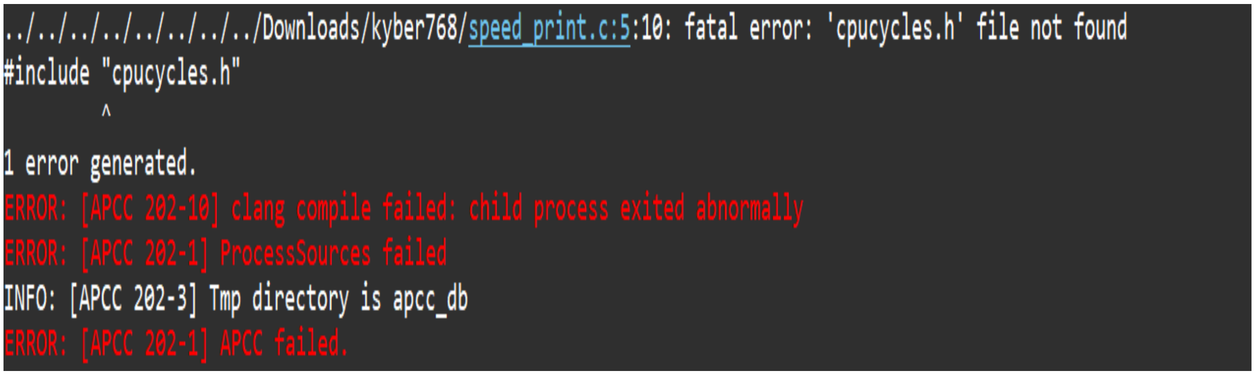
```
WARNING: [HLS 200-40] Skipped source file 'Makefile'. Source files must have extensions .c, .C, .cc, .cpp, .c++, .cp, or .cxx.
INFO: [HLS 200-111] Finished File checks and directory preparation: CPU user time: 0 seconds. CPU system time: 0 seconds. Elapsed
INFO: [HLS 200-10] Analyzing design file '../../../../Downloads/kyber768/verify.c' ...
INFO: [HLS 200-10] Analyzing design file '../../../../Downloads/kyber768/symmetric-shake.c' ...
INFO: [HLS 200-10] Analyzing design file '../../../../Downloads/kyber768/symmetric-aes.c' ...
INFO: [HLS 200-10] Analyzing design file '../../../../Downloads/kyber768/sha512.c' ...
INFO: [HLS 200-10] Analyzing design file '../../../../Downloads/kyber768/sha256.c' ...
INFO: [HLS 200-10] Analyzing design file '../../../../Downloads/kyber768/rng.c' ...
```

3) On synthesizing again, an error stating that test_speed.c attempted to access “kex.h” which is not present, so we removed this file.



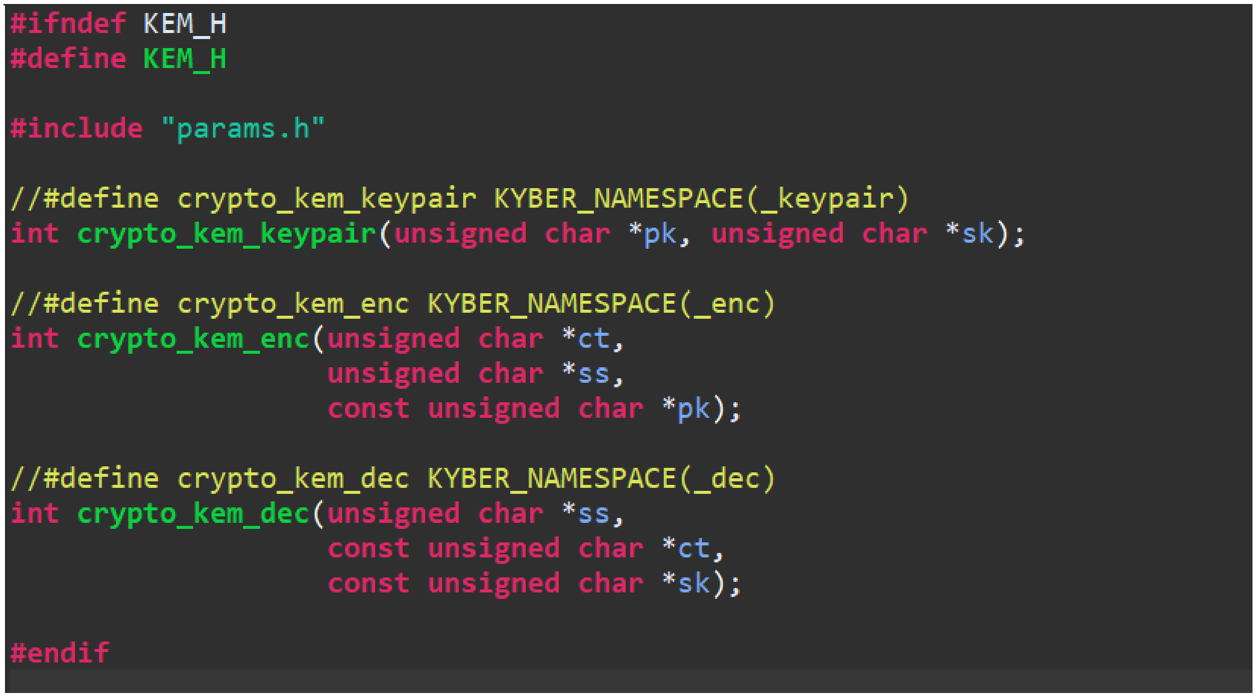
```
INFO: [HLS 200-10] In directory 'C:/Users/srida/AppData/Roaming/Xilinx/Vitis/VLSI_Project/solution1/csim/build'
../../../../../../../../Downloads/kyber768/test_speed.c:6:10: fatal error: 'kex.h' file not found
#include "kex.h"
         ^
1 error generated.
ERROR: [APCC 202-10] clang compile failed: child process exited abnormally
ERROR: [APCC 202-1] ProcessSources failed
INFO: [APCC 202-3] Tmp directory is apcc_db
ERROR: [APCC 202-1] APCC failed.
```

4) On synthesizing again, an error stating that speed_print.c attempted to access “kex.h” which is not present, so we removed this file.

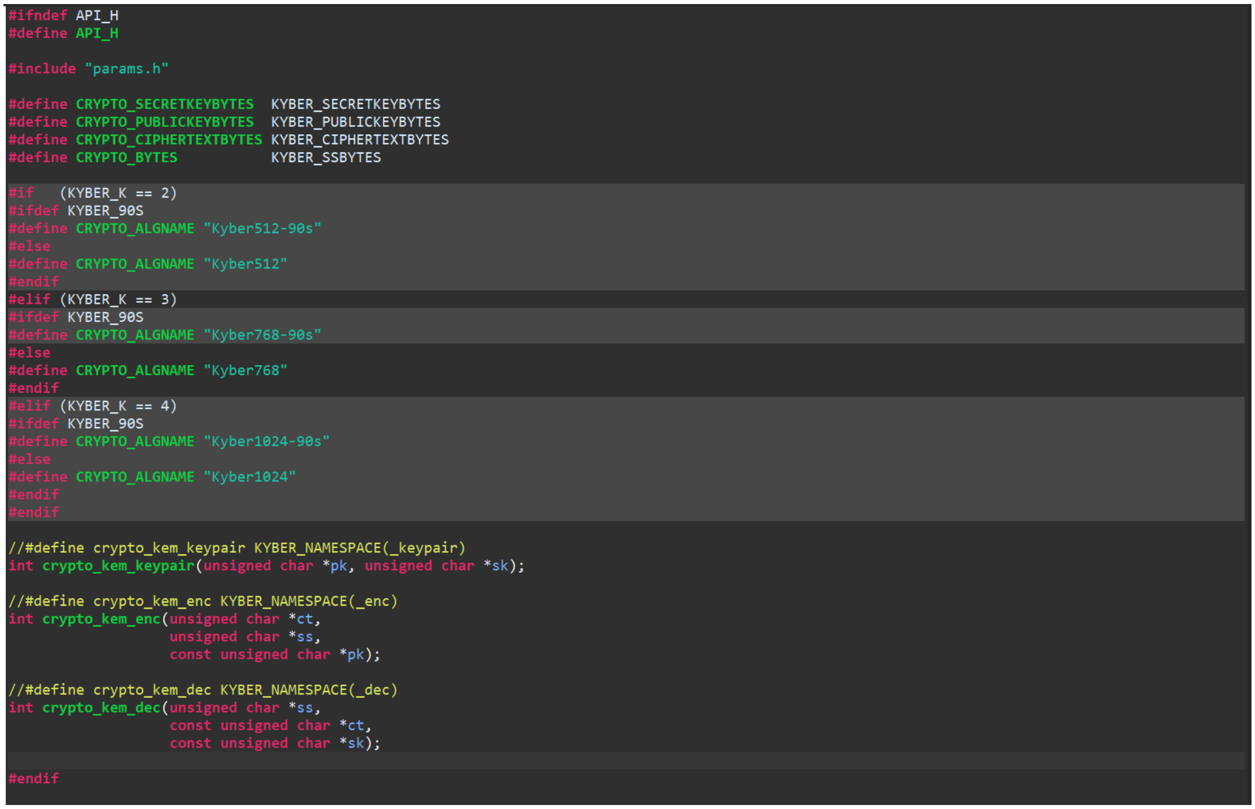


```
../../../../../../../../Downloads/kyber768/speed_print.c:5:10: fatal error: 'cpucycles.h' file not found
#include "cpucycles.h"
         ^
1 error generated.
ERROR: [APCC 202-10] clang compile failed: child process exited abnormally
ERROR: [APCC 202-1] ProcessSources failed
INFO: [APCC 202-3] Tmp directory is apcc_db
ERROR: [APCC 202-1] APCC failed.
```

5) When we tried to synthesize it generated an error stating that it couldn’t find the top function. Possible reasons include a typo or static declaration so we comment out #define in kem.h and api.h files.

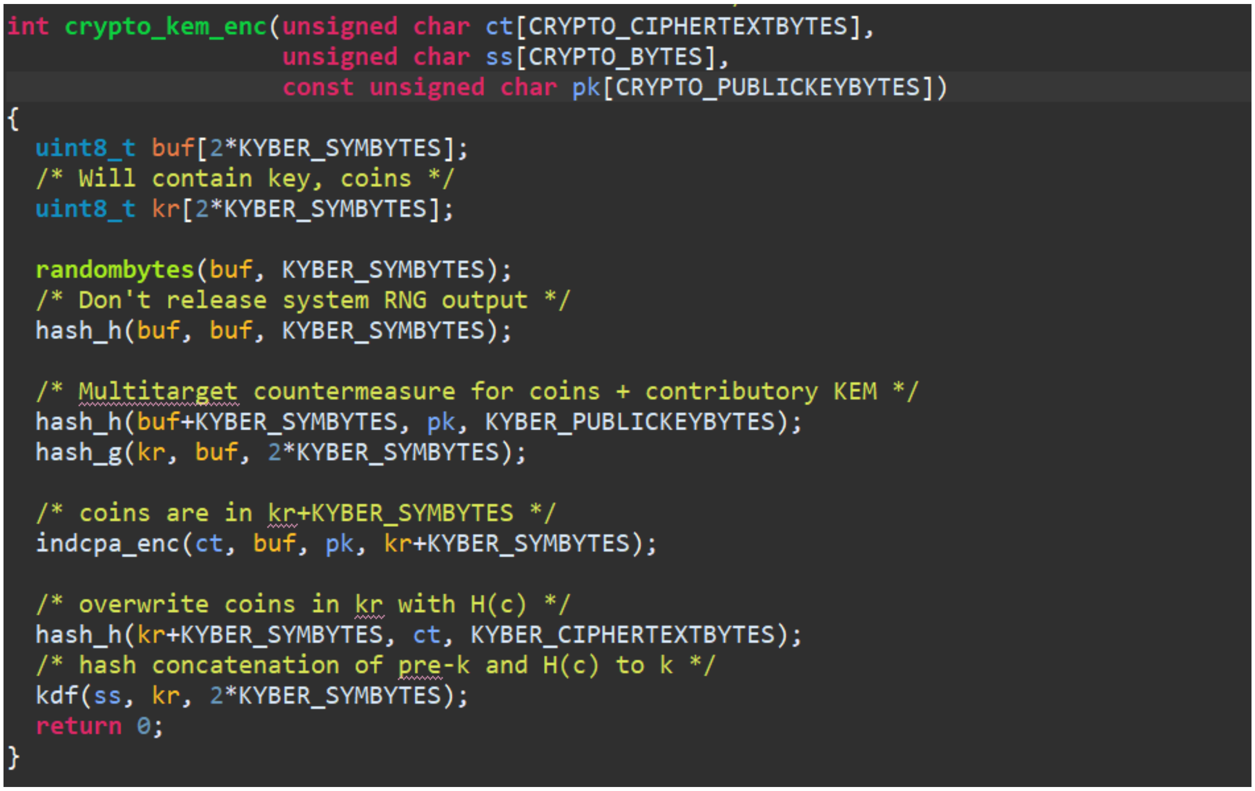


```
#ifndef KEM_H
#define KEM_H

#include "params.h"

//#define crypto_kem_keypair KYBER_NAMESPACE(_keypair)
int crypto_kem_keypair(unsigned char *pk, unsigned char *sk);

//#define crypto_kem_enc KYBER_NAMESPACE(_enc)
int crypto_kem_enc(unsigned char *ct,
                   unsigned char *ss,
                   const unsigned char *pk);

//#define crypto_kem_dec KYBER_NAMESPACE(_dec)
int crypto_kem_dec(unsigned char *ss,
                   const unsigned char *ct,
                   const unsigned char *sk);

#endif
```



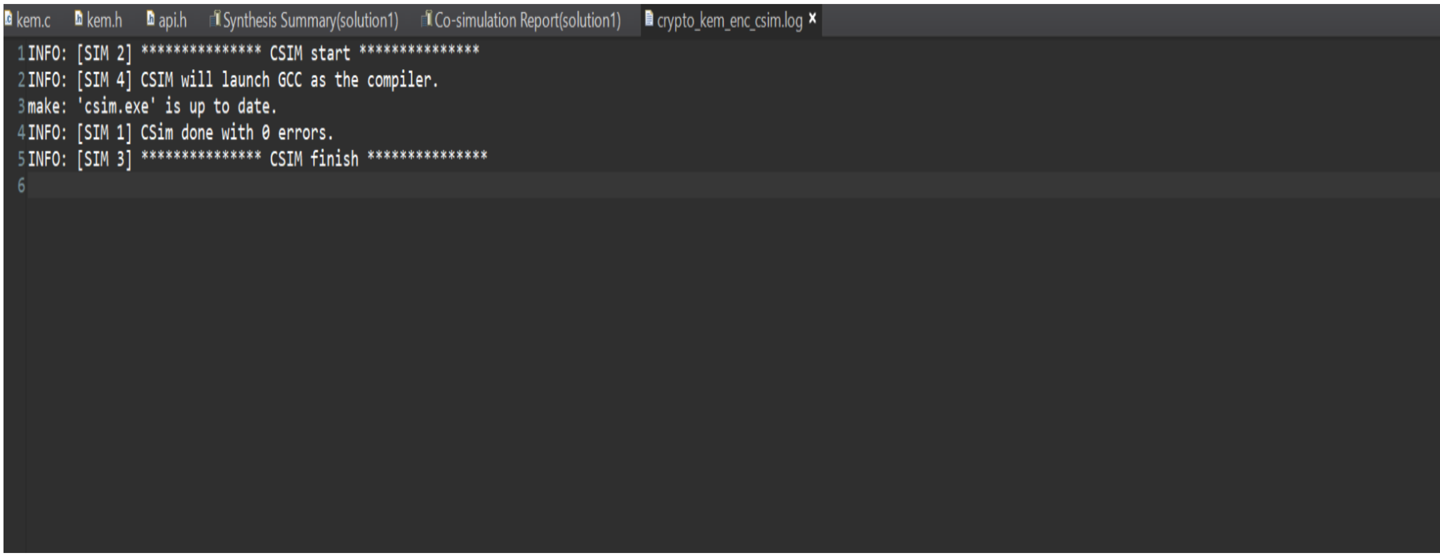
```
#ifndef API_H
#define API_H

#include "params.h"

#define CRYPTO_SECRETKEYBYTES  KYBER_SECRETKEYBYTES
#define CRYPTO_PUBLICKEYBYTES  KYBER_PUBLICKEYBYTES
#define CRYPTO_CIPHERTEXTBYTES KYBER_CIPHERTEXTBYTES
#define CRYPTO_BYTES           KYBER_SSBYTES

#if   (KYBER_K == 2)
#ifdef KYBER_90S
#define CRYPTO_ALGNAME "Kyber512-90s"
#else
#define CRYPTO_ALGNAME "Kyber512"
#endif
#elif (KYBER_K == 3)
#ifdef KYBER_90S
#define CRYPTO_ALGNAME "Kyber768-90s"
#else
#define CRYPTO_ALGNAME "Kyber768"
#endif
#elif (KYBER_K == 4)
#ifdef KYBER_90S
#define CRYPTO_ALGNAME "Kyber1024-90s"
#else
#define CRYPTO_ALGNAME "Kyber1024"
#endif
#endif

//#define crypto_kem_keypair KYBER_NAMESPACE(_keypair)
int crypto_kem_keypair(unsigned char *pk, unsigned char *sk);

//#define crypto_kem_enc KYBER_NAMESPACE(_enc)
int crypto_kem_enc(unsigned char *ct,
                   unsigned char *ss,
                   const unsigned char *pk);

//#define crypto_kem_dec KYBER_NAMESPACE(_dec)
int crypto_kem_dec(unsigned char *ss,
                   const unsigned char *ct,
                   const unsigned char *sk);

#endif
```

6) The argument in the crypto_kem_enc were dynamic which led to variable definition of size so we give a static size.

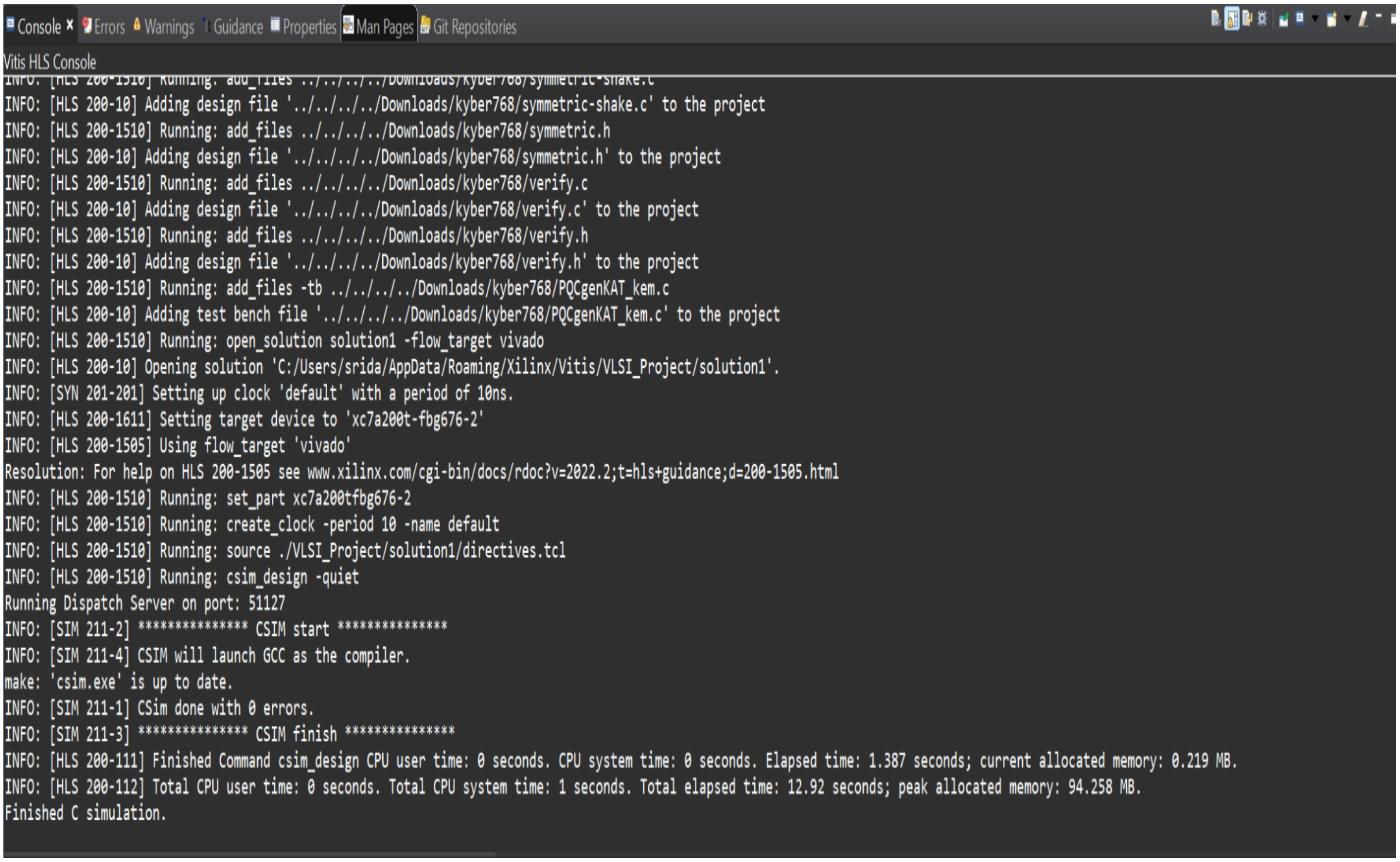


```
int crypto_kem_enc(unsigned char ct[CRYPTO_CIPHERTEXTBYTES],
                   unsigned char ss[CRYPTO_BYTES],
                   const unsigned char pk[CRYPTO_PUBLICKEYBYTES])
{
  uint8_t buf[2*KYBER_SYMBYTES];
  /* Will contain key, coins */
  uint8_t kr[2*KYBER_SYMBYTES];

  randombytes(buf, KYBER_SYMBYTES);
  /* Don't release system RNG output */
  hash_h(buf, buf, KYBER_SYMBYTES);

  /* Multitarget countermeasure for coins + contributory KEM */
  hash_h(buf+KYBER_SYMBYTES, pk, KYBER_PUBLICKEYBYTES);
  hash_g(kr, buf, 2*KYBER_SYMBYTES);

  /* coins are in kr+KYBER_SYMBYTES */
  indcpa_enc(ct, buf, pk, kr+KYBER_SYMBYTES);

  /* overwrite coins in kr with H(c) */
  hash_h(kr+KYBER_SYMBYTES, ct, KYBER_CIPHERTEXTBYTES);
  /* hash concatenation of pre-k and H(c) to k */
  kdf(ss, kr, 2*KYBER_SYMBYTES);
  return 0;
}
```

Result of RTL C-Simulation:

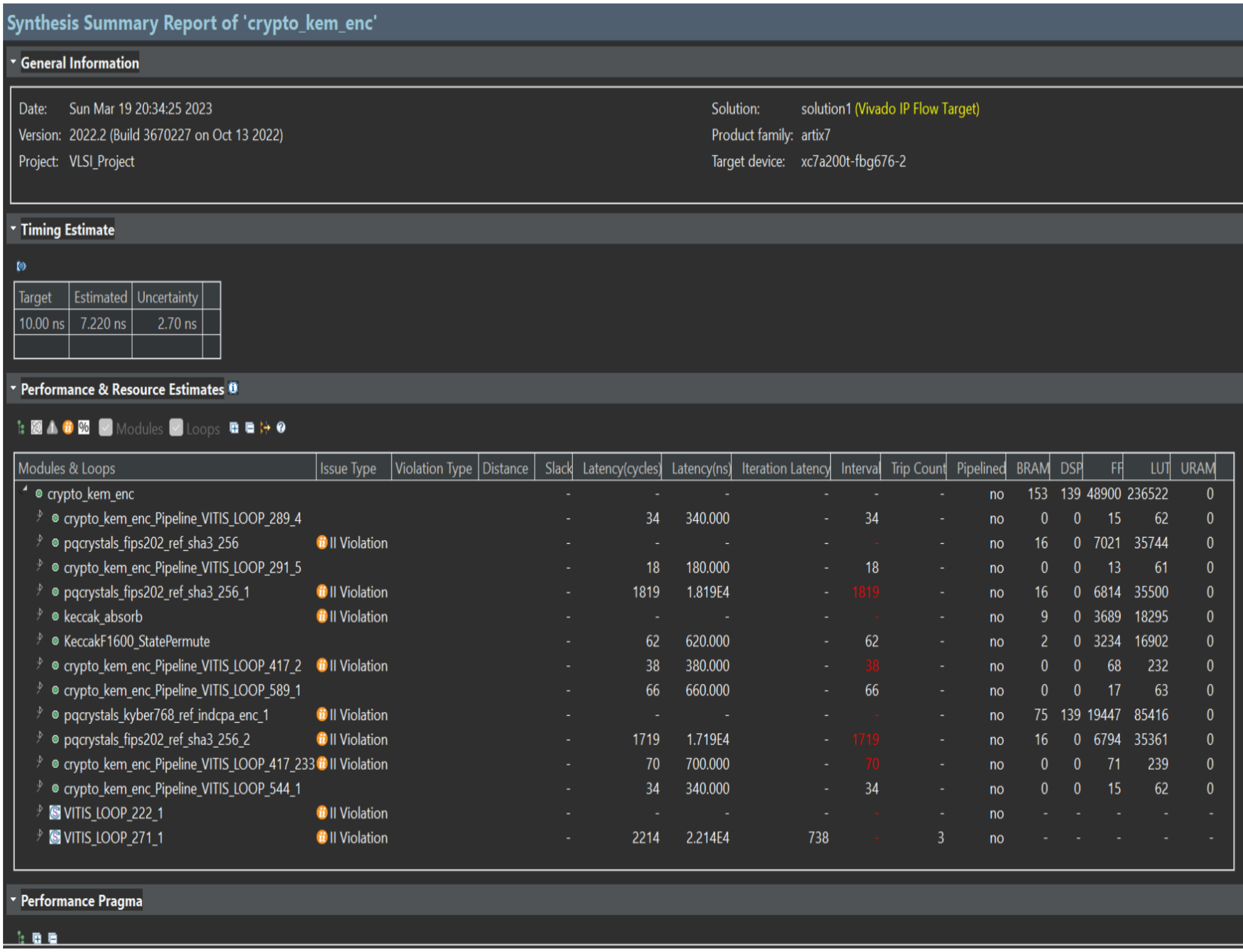


```
INFO: [SIM 2] *************** CSIM start ***************
INFO: [SIM 4] CSIM will launch GCC as the compiler.
make: 'csim.exe' is up to date.
INFO: [SIM 1] CSim done with 0 errors.
INFO: [SIM 3] *************** CSIM finish ***************
```



```
INFO: [HLS 200-1510] Running: add_files ../../../../Downloads/kyber768/symmetric-shake.c
INFO: [HLS 200-10] Adding design file '../../../../Downloads/kyber768/symmetric-shake.c' to the project
INFO: [HLS 200-1510] Running: add_files ../../../../Downloads/kyber768/symmetric.h
INFO: [HLS 200-10] Adding design file '../../../../Downloads/kyber768/symmetric.h' to the project
INFO: [HLS 200-1510] Running: add_files ../../../../Downloads/kyber768/verify.c
INFO: [HLS 200-10] Adding design file '../../../../Downloads/kyber768/verify.c' to the project
INFO: [HLS 200-1510] Running: add_files ../../../../Downloads/kyber768/verify.h
INFO: [HLS 200-10] Adding design file '../../../../Downloads/kyber768/verify.h' to the project
INFO: [HLS 200-1510] Running: add_files -tb ../../../../Downloads/kyber768/PQCgenKAT_kem.c
INFO: [HLS 200-10] Adding test bench file '../../../../Downloads/kyber768/PQCgenKAT_kem.c' to the project
INFO: [HLS 200-1510] Running: open_solution solution1 -flow_target vivado
INFO: [HLS 200-10] Opening solution 'C:/Users/srida/AppData/Roaming/Xilinx/Vitis/VLSI_Project/solution1'.
INFO: [SYN 201-201] Setting up clock 'default' with a period of 10ns.
INFO: [HLS 200-1611] Setting target device to 'xc7a200t-fbg676-2'
INFO: [HLS 200-1505] Using flow_target 'vivado'
Resolution: For help on HLS 200-1505 see www.xilinx.com/cgi-bin/docs/rdoc?v=2022.2;t=hls+guidance;d=200-1505.html
INFO: [HLS 200-1510] Running: set_part xc7a200tfbg676-2
INFO: [HLS 200-1510] Running: create_clock -period 10 -name default
INFO: [HLS 200-1510] Running: source ./VLSI_Project/solution1/directives.tcl
INFO: [HLS 200-1510] Running: csim_design -quiet
Running Dispatch Server on port: 51127
INFO: [SIM 211-2] *************** CSIM start ***************
INFO: [SIM 211-4] CSIM will launch GCC as the compiler.
make: 'csim.exe' is up to date.
INFO: [SIM 211-1] CSim done with 0 errors.
INFO: [SIM 211-3] *************** CSIM finish ***************
INFO: [HLS 200-111] Finished Command csim_design CPU user time: 0 seconds. CPU system time: 0 seconds. Elapsed time: 1.387 seconds; current allocated memory: 0.219 MB.
INFO: [HLS 200-112] Total CPU user time: 0 seconds. Total CPU system time: 1 seconds. Total elapsed time: 12.92 seconds; peak allocated memory: 94.258 MB.
Finished C simulation.
```

Result of RTL C-Synthesis:



Synthesis Summary Report of 'crypto_kem_enc'

General Information

Date: Sun Mar 19 20:34:25 2023

Version: 2022.2 (Build 3670227 on Oct 13 2022)

Project: VLSI_Project

Solution: solution1 (Vivado IP Flow Target)

Product family: artix7

Target device: xc7a200t-fbg676-2

Timing Estimate

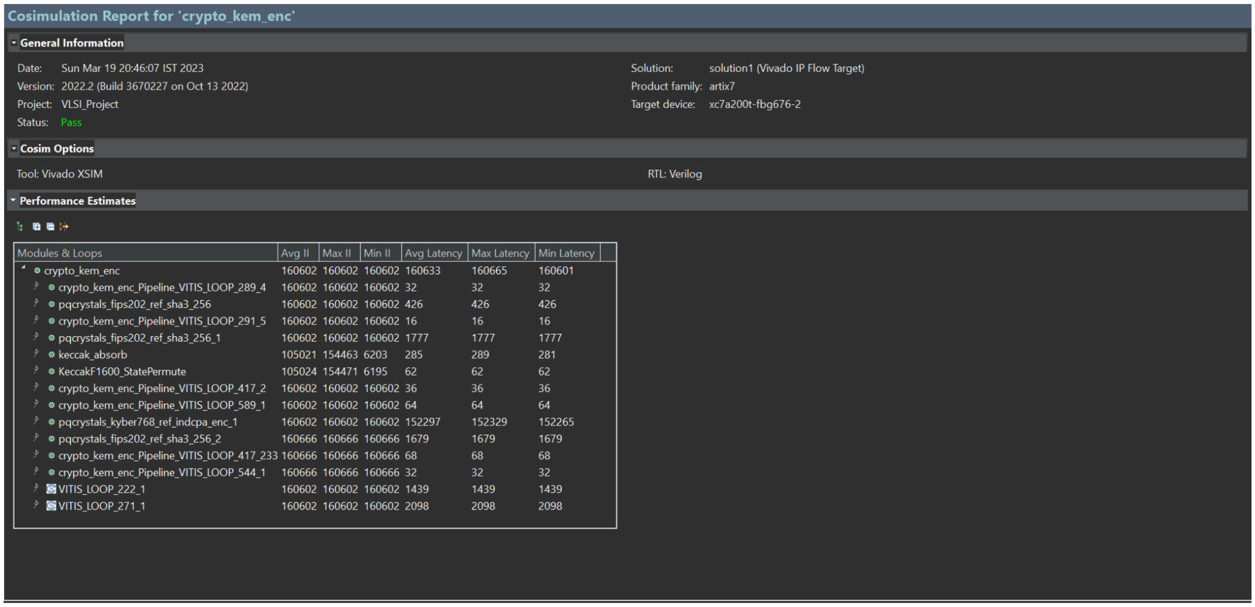
Target	Estimated	Uncertainty
10.00 ns	7.220 ns	2.70 ns

Performance & Resource Estimates

Modules & Loops	Issue Type	Violation Type	Distance	Slack	Latency(cycles)	Latency(ns)	Iteration Latency	Interval	Trip Count	Pipelined	BRAM	DSP	FF	LUT	URAM
crypto_kem_enc				-	-	-	-	-	-	no	153	139	48900	236522	0
crypto_kem_enc_Pipeline_VITIS_LOOP_289_4				-	34	340.000	-	34	-	no	0	0	15	62	0
pqcrystals_fips202_ref_sha3_256	II Violation			-	-	-	-	-	-	no	16	0	7021	35744	0
crypto_kem_enc_Pipeline_VITIS_LOOP_291_5				-	18	180.000	-	18	-	no	0	0	13	61	0
pqcrystals_fips202_ref_sha3_256_1	II Violation			-	1819	1.819E4	-	1819	-	no	16	0	6814	35500	0
keccak_absorb	II Violation			-	-	-	-	-	-	no	9	0	3689	18295	0
KeccakF1600_StatePermute				-	62	620.000	-	62	-	no	2	0	3234	16902	0
crypto_kem_enc_Pipeline_VITIS_LOOP_417_2	II Violation			-	38	380.000	-	38	-	no	0	0	68	232	0
crypto_kem_enc_Pipeline_VITIS_LOOP_589_1				-	66	660.000	-	66	-	no	0	0	17	63	0
pqcrystals_kyber768_ref_indcpa_enc_1	II Violation			-	-	-	-	-	-	no	75	139	19447	85416	0
pqcrystals_fips202_ref_sha3_256_2	II Violation			-	1719	1.719E4	-	1719	-	no	16	0	6794	35361	0
crypto_kem_enc_Pipeline_VITIS_LOOP_417_233	II Violation			-	70	700.000	-	70	-	no	0	0	71	239	0
crypto_kem_enc_Pipeline_VITIS_LOOP_544_1				-	34	340.000	-	34	-	no	0	0	15	62	0
VITIS_LOOP_222_1	II Violation			-	-	-	-	-	-	no	-	-	-	-	-
VITIS_LOOP_271_1	II Violation			-	2214	2.214E4	738	-	3	no	-	-	-	-	-

Performance Pragma

Result of RTL Co-Simulation:



Cosimulation Report for 'crypto_kem_enc'

General Information

Date: Sun Mar 19 20:46:07 IST 2023
Version: 2022.2 (Build 3670227 on Oct 13 2022)
Project: VLSI_Project
Status: Pass

Solution: solution1 (Vivado IP Flow Target)
Product family: artix7
Target device: xc7a200t-fbg676-2

Cosim Options

Tool: Vivado XSIM

RTL: Verilog

Performance Estimates

Modules & Loops	Avg II	Max II	Min II	Avg Latency	Max Latency	Min Latency
crypto_kem_enc	160602	160602	160602	160633	160665	160601
crypto_kem_enc_Pipeline_VITIS_LOOP_289_4	160602	160602	160602	32	32	32
pqcrystals_fips202_ref_sha3_256	160602	160602	160602	426	426	426
crypto_kem_enc_Pipeline_VITIS_LOOP_291_5	160602	160602	160602	16	16	16
pqcrystals_fips202_ref_sha3_256_1	160602	160602	160602	1777	1777	1777
keccak_absorb	105021	154463	6203	285	289	281
KeccakF1600_StatePermute	105024	154471	6195	62	62	62
crypto_kem_enc_Pipeline_VITIS_LOOP_417_2	160602	160602	160602	36	36	36
crypto_kem_enc_Pipeline_VITIS_LOOP_589_1	160602	160602	160602	64	64	64
pqcrystals_kyber768_ref_indcpa_enc_1	160602	160602	160602	152297	152329	152265
pqcrystals_fips202_ref_sha3_256_2	160666	160666	160666	1679	1679	1679
crypto_kem_enc_Pipeline_VITIS_LOOP_417_233	160666	160666	160666	68	68	68
crypto_kem_enc_Pipeline_VITIS_LOOP_544_1	160666	160666	160666	32	32	32
VITIS_LOOP_222_1	160602	160602	160602	1439	1439	1439
VITIS_LOOP_271_1	160602	160602	160602	2098	2098	2098