Report

Team Name:	**The Mavs**
Chandrabhushan Reddy	**200101027**
Manideepak Gannoju	**200101032**
Shashank	**200102005**
Sathvika Kalangi	**200101048**
Rajeev Anand	**200102096**

Modifications Made:

1) The dilithium namespace has been defined over all the functions which is causing synthesization error. So we've commented out the namespaces in 2 files in which it is present.

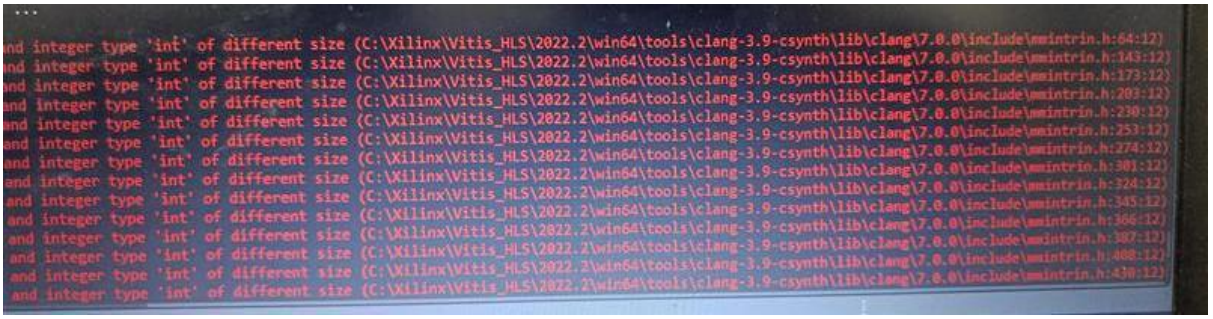
sign.h:

```c
#ifndef SIGN_H
#define SIGN_H

#include <stddef.h>
#include <stdint.h>
#include "params.h"
#include "polyvec.h"
#include "poly.h"

//#define challenge DILITHIUM_NAMESPACE(_challenge)
void challenge(poly *c, const uint8_t seed[SEEDBYTES]);

//#define crypto_sign_keypair DILITHIUM_NAMESPACE(_keypair)
int crypto_sign_keypair(uint8_t *pk, uint8_t *sk);

//#define crypto_sign_signature DILITHIUM_NAMESPACE(_signature)
int crypto_sign_signature(uint8_t *sig, size_t *siglen,
                          const uint8_t *m, size_t mlen,
                          const uint8_t *sk);

//#define crypto_sign DILITHIUM_NAMESPACE()
int crypto_sign(uint8_t *sm, size_t *smlen,
                const uint8_t *m, size_t mlen,
                const uint8_t *sk)

//#define crypto_sign_verify DILITHIUM_NAMESPACE(_verify)
int crypto_sign_verify(const uint8_t *sig, size_t siglen,
                       const uint8_t *m, size_t mlen,
                       const uint8_t *pk);

//#define crypto_sign_open DILITHIUM_NAMESPACE(_open)
int crypto_sign_open(uint8_t *m, size_t *mlen,
                     const uint8_t *sm, size_t smlen,
                     const uint8_t *pk);

#endif
```

api.h:

```
//#define crypto_sign_keypair DILITHIUM_NAMESPACE(_keypair)
int crypto_sign_keypair(unsigned char *pk, unsigned char *sk);

//#define crypto_sign DILITHIUM_NAMESPACE()
int crypto_sign(unsigned char *sm, unsigned long long *smlen,
                const unsigned char *msg, unsigned long long len,
                const unsigned char *sk);

//#define crypto_sign_open DILITHIUM_NAMESPACE(_open)
int crypto_sign_open(unsigned char *m, unsigned long long *mlen,
                     const unsigned char *sm, unsigned long long smlen,
                     const unsigned char *pk);
```

2) The function randombytes() in the randombytes.c file which is being used in our target source file (sign.c) is causing “clang” compilation errors.



So we removed randombytes.c and randombytes.h from our source files and instead used an another similar function of randombytes() present in rng.c
So we’ve commented out the randombytes.h header file in sign.c and added rng.h header file.

PQCgenKAT_sign.c | sign.c | api.h

sign.c > ...

```c
#include <stdint.h>
#include "params.h"
#include "sign.h"
#include "packing.h"
#include "polyvec.h"
#include "poly.h"
//#include "randombytes.h"
#include "rng.h"
#include "symmetric.h"
#include "fips202.h"

```

3) For simulation and co-simulation to work we've replaced the variable size arguments of arrays present in the crypto_sign function and replaced them with the actual array sizes which are being initialised in the "PQCgenKAT_sign.c" testbench file.

sign.c:

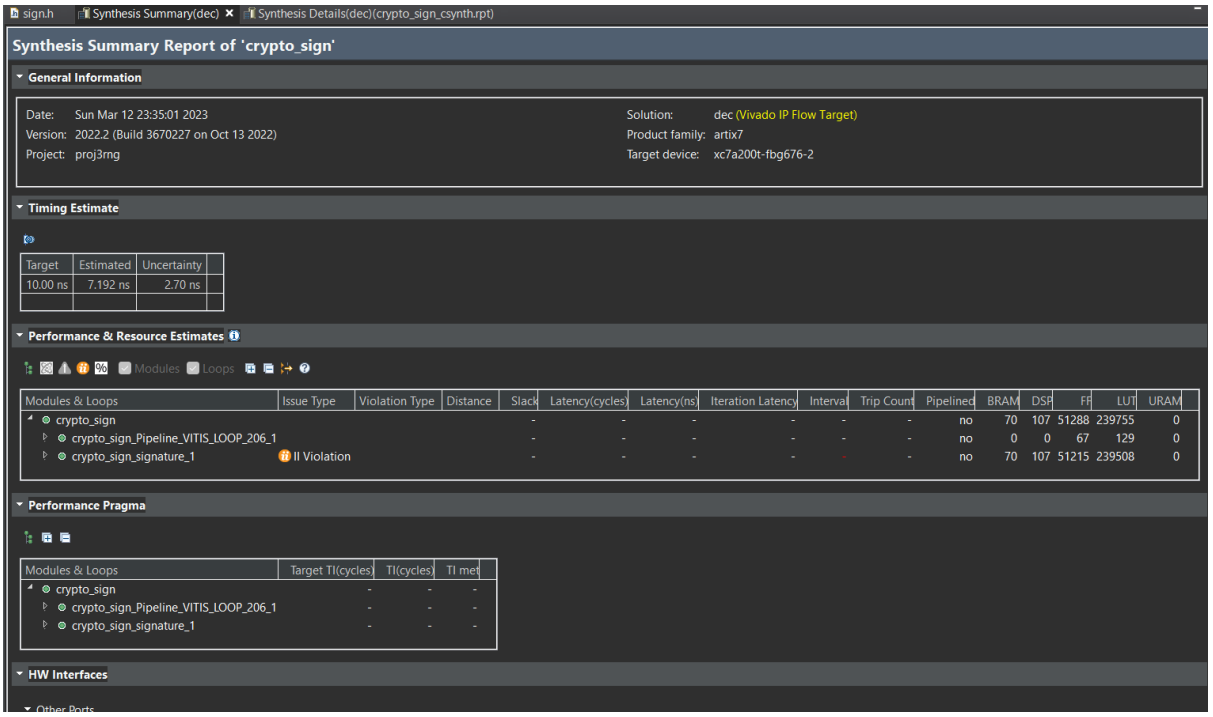
```c
int crypto_sign(uint8_t sm[3300+CRYPTO_BYTES],
                size_t *smlen,
                const uint8_t m[3300],
                size_t mlen,
                const uint8_t sk[CRYPTO_SECRETKEYBYTES])
{
  size_t i;

  for(i = 0; i < mlen; ++i)
    sm[CRYPTO_BYTES + mlen - 1 - i] = m[mlen - 1 - i];
  crypto_sign_signature(sm, smlen, sm + CRYPTO_BYTES, mlen, sk);
  *smlen += mlen;
  return 0;
}
```

sign.h:

```
//#define crypto_sign DILITHIUM_NAMESPACE()
int crypto_sign(uint8_t sm[3300+CRYPTO_BYTES], size_t *smlen,
                const uint8_t m[3300], size_t mlen,
                const uint8_t sk[CRYPTO_SECRETKEYBYTES]);
```

Results:

1) Synthesis Report:



sign.h | Synthesis Summary(dec) | Synthesis Details(dec)(crypto_sign_csynth.rpt)

Synthesis Summary Report of 'crypto_sign'

General Information

Date: Sun Mar 12 23:35:01 2023
Version: 2022.2 (Build 3670227 on Oct 13 2022)
Project: proj3rng
Solution: dec (Vivado IP Flow Target)
Product family: artix7
Target device: xc7a200t-fbg676-2

Timing Estimate

Target	Estimated	Uncertainty
10.00 ns	7.192 ns	2.70 ns

Performance & Resource Estimates

Modules Loops

Modules & Loops	Issue Type	Violation Type	Distance	Slack	Latency(cycles)	Latency(ns)	Iteration Latency	Interval	Trip Count	Pipelined	BRAM	DSP	FF	LUT	URAM
crypto_sign				-	-	-	-	-	-	no	70	107	51288	239755	0
crypto_sign_Pipeline_VITIS_LOOP_206_1				-	-	-	-	-	-	no	0	0	67	129	0
crypto_sign_signature_1	II Violation			-	-	-	-	-	-	no	70	107	51215	239508	0

Performance Pragma

Modules & Loops	Target TI(cycles)	TI(cycles)	TI met
crypto_sign	-	-	-
crypto_sign_Pipeline_VITIS_LOOP_206_1	-	-	-
crypto_sign_signature_1	-	-	-

HW Interfaces

Other Ports

2) Simulation Report:

crypto_sign_csim.log:

```
sign.h  crypto_sign_csim.log  PQCsignKAT_2544.req
INFO: [SIM 2] *************** CSIM start ***************
INFO: [SIM 4] CSIM will launch GCC as the compiler.
   Compiling(apcc) ../../../../../../../../Sem6/VLSI/dilithium2rng/dilithium2/PQCgenKAT_sign.c in debug mode
INFO: [HLS 200-10] Running 'C:/Xilinx/Vitis_HLS/2022.2/bin/unwrapped/win64.o/apcc.exe'
INFO: [HLS 200-10] For user 'manideepak' on host 'desktop-aab3m4s' (Windows NT_amd64 version 6.2) on Sun Mar 12 23:40:36 +0530 2023
INFO: [HLS 200-10] In directory 'C:/Users/manid/AppData/Roaming/Xilinx/Vitis/proj3rng/dec/csim/build'
INFO: [APCC 202-3] Tmp directory is apcc_db
INFO: [APCC 202-1] APCC is done.
INFO: [HLS 200-112] Total CPU user time: 1 seconds. Total CPU system time: 0 seconds. Total elapsed time: 3.184 seconds; peak allocated memory: 6.602 MB.
   Compiling(apcc) ../../../../../../../../Sem6/VLSI/dilithium2rng/dilithium2/symmetric-shake.c in debug mode
INFO: [HLS 200-10] Running 'C:/Xilinx/Vitis_HLS/2022.2/bin/unwrapped/win64.o/apcc.exe'
INFO: [HLS 200-10] For user 'manideepak' on host 'desktop-aab3m4s' (Windows NT_amd64 version 6.2) on Sun Mar 12 23:40:42 +0530 2023
INFO: [HLS 200-10] In directory 'C:/Users/manid/AppData/Roaming/Xilinx/Vitis/proj3rng/dec/csim/build'
INFO: [APCC 202-3] Tmp directory is apcc_db
INFO: [APCC 202-1] APCC is done.
INFO: [HLS 200-112] Total CPU user time: 0 seconds. Total CPU system time: 0 seconds. Total elapsed time: 1.253 seconds; peak allocated memory: 6.930 MB.
   Compiling(apcc) ../../../../../../../../Sem6/VLSI/dilithium2rng/dilithium2/symmetric-aes.c in debug mode
INFO: [HLS 200-10] Running 'C:/Xilinx/Vitis_HLS/2022.2/bin/unwrapped/win64.o/apcc.exe'
INFO: [HLS 200-10] For user 'manideepak' on host 'desktop-aab3m4s' (Windows NT_amd64 version 6.2) on Sun Mar 12 23:40:46 +0530 2023
INFO: [HLS 200-10] In directory 'C:/Users/manid/AppData/Roaming/Xilinx/Vitis/proj3rng/dec/csim/build'
INFO: [APCC 202-3] Tmp directory is apcc_db
INFO: [APCC 202-1] APCC is done.
INFO: [HLS 200-112] Total CPU user time: 1 seconds. Total CPU system time: 0 seconds. Total elapsed time: 1.325 seconds; peak allocated memory: 5.281 MB.
   Compiling(apcc) ../../../../../../../../Sem6/VLSI/dilithium2rng/dilithium2/sign.c in debug mode
INFO: [HLS 200-10] Running 'C:/Xilinx/Vitis_HLS/2022.2/bin/unwrapped/win64.o/apcc.exe'
INFO: [HLS 200-10] For user 'manideepak' on host 'desktop-aab3m4s' (Windows NT_amd64 version 6.2) on Sun Mar 12 23:40:49 +0530 2023
INFO: [HLS 200-10] In directory 'C:/Users/manid/AppData/Roaming/Xilinx/Vitis/proj3rng/dec/csim/build'
INFO: [APCC 202-3] Tmp directory is apcc_db
INFO: [APCC 202-1] APCC is done.
INFO: [HLS 200-112] Total CPU user time: 0 seconds. Total CPU system time: 0 seconds. Total elapsed time: 1.476 seconds; peak allocated memory: 5.324 MB.
   Compiling(apcc) ../../../../../../../../Sem6/VLSI/dilithium2rng/dilithium2/rounding.c in debug mode
INFO: [HLS 200-10] Running 'C:/Xilinx/Vitis_HLS/2022.2/bin/unwrapped/win64.o/apcc.exe'
INFO: [HLS 200-10] For user 'manideepak' on host 'desktop-aab3m4s' (Windows NT_amd64 version 6.2) on Sun Mar 12 23:40:53 +0530 2023
INFO: [HLS 200-10] In directory 'C:/Users/manid/AppData/Roaming/Xilinx/Vitis/proj3rng/dec/csim/build'
INFO: [APCC 202-3] Tmp directory is apcc_db
INFO: [APCC 202-1] APCC is done.
INFO: [HLS 200-112] Total CPU user time: 0 seconds. Total CPU system time: 0 seconds. Total elapsed time: 1.182 seconds; peak allocated memory: 5.309 MB.
   Compiling(apcc) ../../../../../../../../Sem6/VLSI/dilithium2rng/dilithium2/rng.c in debug mode
INFO: [HLS 200-10] Running 'C:/Xilinx/Vitis_HLS/2022.2/bin/unwrapped/win64.o/apcc.exe'
INFO: [HLS 200-10] For user 'manideepak' on host 'desktop-aab3m4s' (Windows NT_amd64 version 6.2) on Sun Mar 12 23:40:57 +0530 2023
INFO: [HLS 200-10] In directory 'C:/Users/manid/AppData/Roaming/Xilinx/Vitis/proj3rng/dec/csim/build'
INFO: [APCC 202-3] Tmp directory is apcc_db
INFO: [APCC 202-1] APCC is done.
INFO: [HLS 200-112] Total CPU user time: 0 seconds. Total CPU system time: 0 seconds. Total elapsed time: 1.445 seconds; peak allocated memory: 6.629 MB.
```

Output Files Generated: (Which are specified in the “PQCgenKAT_sign.c” testbench file)

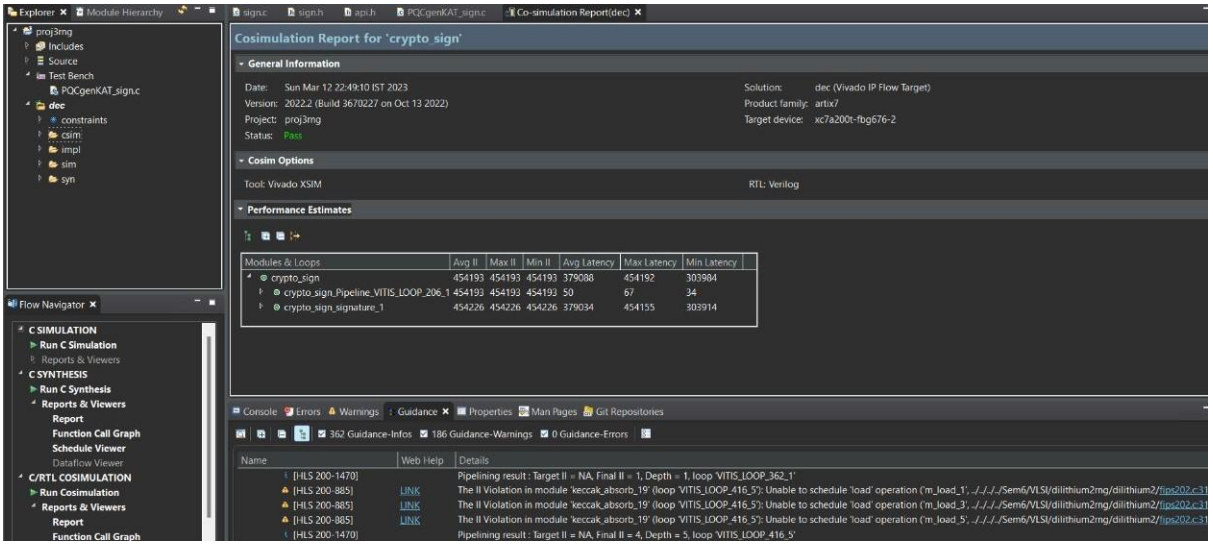
PQCsignKAT_2544.req: (Request File)

```
sign.h  crypto_sign_csim.log  PQCsignKAT_2544.req
count = 0
seed = 061550234D158C5EC95595FE04EF7A25767F2E24CC2BC479D09D86DC9ABCFDE7056A8C266F9EF97ED08541DBD2E1FFA1
mlen = 33
msg = D81C4D8D734FCBFBEADE3D3F8A039FAA2A2C9957E835AD55B22E75BF57BB556AC8
pk =
sk =
smlen =
sm =

count = 1
seed = 64335BF29E5DE62842C941766BA129B0643B5E7121CA26CFC190EC7DC3543830557FDD5C03CF123A456D48EFEA43C868
mlen = 66
msg = 225D5CE2CEAC61930A07503FB59F7C2F936A3E075481DA3CA299A80F8C5DF9223A073E7B90E02EBF98CA2227EBA38C1AB2568209E46DBA961869C6F83983B17DCD49
pk =
sk =
smlen =
sm =
```

PQCsignKAT_2544.rsp: (Response File)

```
sign.h  crypto_sign_csim.log  PQCsignKAT_2544.req  PQCsignKAT_2544.rsp
# Dilithium2

count = 0
seed = 061550234D158C5EC95595FE04EF7A25767F2E24CC2BC479D09D86DC9ABCFDE7056A8C266F9EF97ED08541DBD2E1FFA1
mlen = 33
msg = D81C4D8D734FCBFBEADE3D3F8A039FAA2A2C9957E835AD55B22E75BF57BB556AC8
pk = 1C0EE1111B08003F28E65E8B3BDEB037CF8F221DFCDAF5950EDB38D506D85BEFEA58E9EA74E74E865732B2AC3430BF90C4AA8FDCC4AA33BE606137070424B0FBA4A11A501E20EC68FC58ECE335F9AE78F1E
sk = 1C0EE1111B08003F28E65E8B3BDEB037CF8F221DFCDAF5950EDB38D506D85BEFEB60E7FB7708849FEDB54F41A68314805A5C0766ACC9F338A46B29EAAC00087AD561C09A9B820B9EB1984C894463A7DFB5D2
smlen = 2453
sm = 8514E7E52D965C3966052FF4EE66F817CAB304AD67793144299 3E237B7B1A4757C67CB9313583364CE57FBDAC0F9F1E2781E112A94C2C750007AE1504F9325CB583EA14207E32CE31969AB2E6CB61CCBCAA

count = 1
seed = 64335BF29E5DE62842C941766BA129B0643B5E7121CA26CFC190EC7DC3543830557FDD5C03CF123A456D48EFEA43C868
mlen = 66
msg = 225D5CE2CEAC61930A07503FB59F7C2F936A3E075481DA3CA299A80F8C5DF9223A073E7B90E02EBF98CA2227EBA38C1AB2568209E46DBA961869C6F83983B17DCD49
pk = B541C1E92CEADD904A09EC08AD306D974734A077868471E58D077187C46604CFB2B2E16B4936E6304399B3E1CD82F85E4935D66BBA7235304C4AD3EF394BFAC122B7F0538D1F897E1E89C5F07C0F7E348EF
sk = B541C1E92CEADD904A09EC08AD306D974734A077868471E58D077187C46604CF4CB2F611ACE7E4234B75B74B2E51366BFACD2715FFAA595B4FF575958CF219C5F5E863619C812448277ACAA7050F345B2EE
smlen = 2486
sm = 33BE9EF1E287701E474466FDD99BBF61B4A019C4F790834FD6EC19DC2A6702ABD5787EE8C2091C77D4851C4A9533355331E29C2993A0CA643F7E99A612C76A4721C749AFB8B6A70095159689F11D40B41E6
```

3) Co-Simulation Report:


Explorer
Module Hierarchy
proj3rng
Includes
Source
Test Bench
PQCgenKAT_sign.c
dec
constraints
csim
impl
sim
syn
Flow Navigator
C SIMULATION
Run C Simulation
Reports & Viewers
C SYNTHESIS
Run C Synthesis
Reports & Viewers
Report
Function Call Graph
Schedule Viewer
Dataflow Viewer
C/RTL COSIMULATION
Run Cosimulation
Reports & Viewers
Report
Function Call Graph
sign.c
sign.h
api.h
PQCgenKAT_sign.c
Co-simulation Report(dec)
Cosimulation Report for 'crypto_sign'
General Information
Date: Sun Mar 12 22:49:10 IST 2023
Version: 2022.2 (Build 3670227 on Oct 13 2022)
Project: proj3rng
Status: Pass
Solution: dec (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_sign
454193 454193 454193 379088 454192 303984
crypto_sign_Pipeline_VITIS_LOOP_206_1
454193 454193 454193 50 67 34
crypto_sign_signature_1
454226 454226 454226 379034 454155 303914
Console
Errors
Warnings
Guidance
Properties
Man Pages
Git Repositories
362 Guidance-Infos
186 Guidance-Warnings
0 Guidance-Errors
Name
Web Help
Details
[HLS 200-1470]
Pipelining result : Target II = NA, Final II = 1, Depth = 1, loop 'VITIS_LOOP_362_1'
[HLS 200-885]
LINK
The II Violation in module 'keccak_absorb_19' (loop 'VITIS_LOOP_416_5'): Unable to schedule 'load' operation ('m_load_1', ../../../../Sem6/VLSI/dilithium2rng/dilithium2/fips202.c:31
[HLS 200-885]
LINK
The II Violation in module 'keccak_absorb_19' (loop 'VITIS_LOOP_416_5'): Unable to schedule 'load' operation ('m_load_3', ../../../../Sem6/VLSI/dilithium2rng/dilithium2/fips202.c:31
[HLS 200-885]
LINK
The II Violation in module 'keccak_absorb_19' (loop 'VITIS_LOOP_416_5'): Unable to schedule 'load' operation ('m_load_5', ../../../../Sem6/VLSI/dilithium2rng/dilithium2/fips202.c:31
[HLS 200-1470]
Pipelining result : Target II = NA, Final II = 4, Depth = 5, loop 'VITIS_LOOP_416_5'