INDIAN INSTITUTE OF TECHNOLOGY, GUWAHATI

Department of Computer Science and Engineering

Project Report on

Crypto Sign Synth

Submitted To

Assoc. Prof.

Dr. Chandan Karfa

Submitted By

Anuj Singh Thakur (224101008)

Nihal M. Singh (224101038)

Vaishali Chaudhari (224101055)

Shikha (224101066)

Yashvi Bipinbhai Rajvir (224101061)

For course fulfilment of CS577: C-BASED-VLSI-DESIGN

Phase 1 Report:

In this phase of the project, we focused on synthesizing the "**Dilithium**" digital signature scheme, which is strongly secure under chosen message attacks based on the hardness of lattice problems over module lattices, into hardware. Our main goals for this phase were to ensure correct hardware synthesis and to optimize the code by removing dynamic memory allocation and dynamic for loops, which cannot be directly synthesized into hardware.

Top Function: "crypto_sign"

The primary function we worked on during this phase is named "**crypto_sign**". This function is a macro and its name changes during compilation. The replaced name we used for compilation is "**pqcrystals_dilithium2_ref**" and we used the same name as our top function in the hardware synthesis process.

File Location Changes

We made changes to the source files to better accommodate the hardware synthesis process:

- **PQCgenKAT_sign.c**:

  This file was removed from the source code and added to the test bench. This change was made to streamline the hardware synthesis and testing process.

Code Changes

We made several code changes in this phase to optimize the code for hardware synthesis and testing.

- **Sign.c**

  We modified the function signature of **crypto_sign** as follows:

```
int crypto_sign(uint8_t *sm,
        size_t *smlen,
        const uint8_t *m,
        size_t mlen,
        const uint8_t *sk)
```

```
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])
```

- **test_dilithium.c**

We made the following changes in the "**test_dilithium.c**" file for efficient co-simulation:

```
//#define MLEN 59
//#define NTESTS 10000

#define NTESTS 1   // Reduced from the original due to co-simulation time
#define MLEN 3300  // Changed for compatibility with co-simulation (similar to PQCgenKAT_sign.c size)
```

Conclusion:

By making these changes to the code and ensuring compatibility with the hardware synthesis process, we have successfully completed Phase 1 of our project. Our next steps will focus on optimizing the hardware implementation for both area and latency considerations.