ECE 592 / CSC 591: Cryptographic Engineering and Hardware Security

Assignment 3: Hardware Design of a Quantum-Secure Cryptosystem

Instructor: Dr. Aydin Aysu
Email: aaysu@ncsu.edu
TA: Furkan Aydin (faydn@ncsu.edu)

1 Introduction and Goals

The purpose of this assignment is to develop a cryptographic hardware for a post-quantum encryption scheme. You will analyze the Ring-Binary-Learning-with-Errors encryption scheme — an efficient lattice-based public-key encryption system that provides security against quantum cryptanalysis — and you will design its hardware. Furthermore, you will optimize the design for either to minimize the area-cost or to maximize the throughput. Specifically, you are asked to design the hardware of the **decryption** block, which takes the ciphertext and a secret key input and generates the decrypted output message.

The assignment is provided to you with two files in addition to this .pdf instructions file. These are:

1) `testbench.v`

2) `reference_paper.pdf`

The first file, `testbench.v`, is the testbench of your design. This file contains 5 input test vectors (ciphertexts and secret keys). These are the inputs to your system. The `testbench.v` also contains the expected outputs corresponding to these 5 inputs. You will use these test vectors for the verification of your design. The output of a correct design should *exactly* match with the output provided in the testbench. The I/O of your design is also provided in the testbench and you cannot change it.

The second file, `reference_paper.pdf`, is a paper published at IoTPTS '16, where the algorithm of the target encryption scheme is described. You

should read the paper and analyze the algorithm details. You are expected to the design the **decryption** process by using the parameter set of **R-BinLWEEnc-II**. Please omit the description of the DECODE function. We will instead use the the one that is defined by the Lindner and Peikert, which is exactly the one we discussed in the class. In other words, you will still need to implement the threshold function but the extra shifting of $-k-\lfloor(n-3)/2\rceil$ (due to asymmetries of binary distribution) is not needed — this operation can be (and has been) moved to the encryption part of the algorithm. Therefore, the thresholding is simply converting all coefficients between q/4 and 3q/4 (not including borders) to 1, and the rest to 0.

1.1 Graded Items

You will turn in a soft copy report of your results as well as any code to the TA on Moodle. Make sure to include answers to every question in the report.

Lab reports must be in *readable* English and not raw dumps of log files. Your lab reports must be typeset and must not exceed 6 pages. You will be required to use LaTeXto generate the reports. You can use overleaf to generate the LaTeXfile. Please submit your lab report (in .pdf format) and all of your code in a .zip file on Moodle as lab3_YOUR_UNITY_ID_HERE.zip

You can use any software language you prefer to write the programs required to complete for this assignment. If you have any questions about the assignment, please first refer to the TA of the course (Anuj Dubey, aanjudu@ncsu.edu).

2 Analyze the algorithm

Please read the reference paper carefully. Please describe the parameter set requested from you, write down the security level, polynomial degrees and the coefficienct's modulo value. What is the resulting message, secret key, public key and ciphertext size? Given the algorithm description, which polynomials refer to the secret key, encoded message, decoded message, and which ones are the ciphertext polynomials?

3 Get the Hardware Specs

Form groups of two and send an email to the TA. The TA will respond to you with an optimization goal (either area-cost minimization or throughput maximization). What is the hardware optimization goal assigned to you by the

TA? Design your hardware as best as you can for the specified optimization goal, and please consider the size of the FPGA specified in the next part. Check and make sure that the output of your hardware matches those given in the testbench. Did you achieve a functionally correct design?

4 Compile and Evaluate the Hardware

Synthesize, and place and route your design on a Spartan-6 (xc6slx75–2csg484) FPGA; ISE WebPack 14.6 is recommended. What is the software and its version you are using to carry out the synthesis, place, and route processes? Did you achieve a design that is synthesized, placed, and routed with no errors? What is the hardware area-cost (slices, register, LUTs, DSPs, BRAMs, etc.) of your design? What is the maximum achievable frequency of your design? How many clock cycles it takes to process one decryption? What is the corresponding latency of your design? What is the throughput of your design (in terms of number of decryptions per second)?

5 Part 4: Conclusions

Write a summary of the assignment. Among the things to consider are: what did you learn, what are the challenges of the assignment, what are the straightforward parts, how much time did you spend, and what could be improved?

Finally, please also report the time you spent on this assignment.