Hardware Implementation of Post-Processing Modules for Quantum Key Distribution using 2×2 NTT Butterfly Architecture

Sourabh Tyagi, B.Tech ECE, VIT-AP University

Abstract
This project presents the hardware implementation of two critical post-processing modules—Sifting and Privacy Amplification (PA)—for Quantum Key Distribution (QKD) systems. QKD ensures unconditional security in cryptographic communication by leveraging the principles of quantum mechanics. In this work, a Sifting block was designed to filter valid bits based on quantum basis comparison and calculate Quantum Bit Error Rate (QBER), while the PA block compresses sifted keys using a 2×2 Number Theoretic Transform (NTT) butterfly architecture. The Barrett reduction technique was employed for modulo operations in the PA block. The simulation results demonstrate correct functional behavior and low-latency performance in real-time QKD post-processing. The output signals were validated using testbenches and waveform analysis. The developed architecture ensures scalability and efficiency, making it suitable for high-speed FPGA-based quantum cryptographic applications.

1. Introduction

Quantum Key Distribution (QKD) offers an unbreakable method of secure communication by exploiting the principles of quantum mechanics. While quantum channels are used to exchange raw keys, post-processing is essential to extract a usable secret key. This involves Sifting, Error Correction, and Privacy Amplification (PA). In this project, we focus on implementing the Sifting and PA blocks in hardware using Verilog HDL, aiming to achieve real-time processing with low latency and high throughput.

Initially, the project was explored through C/C++ to understand logical flow and arithmetic operations. The design was then migrated to Verilog for FPGA synthesis. Vivado Design Suite was used for RTL design, simulation, and analysis. The **Sifting Block** compares Alice's and Bob's basis choices to retain matching key bits and compute the Quantum Bit Error Rate (QBER). The **PA Block** reduces the information available to an eavesdropper by compressing the sifted key using the Number

Privacy Amplification Block (2×2 NTT Butterfly)

Privacy Amplification (PA) is the final stage in a QKD post-processing pipeline. Its objective is to compress the sifted key into a shorter, secret key that removes any partial information potentially known by an eavesdropper (Eve). In this work, PA is implemented using Universal Hashing, based on the MMH-MH algorithm accelerated by the Number Theoretic Transform (NTT). The PA block was built using a **2×2 Number Theoretic Transform (NTT) Butterfly** structure, designed entirely in Verilog. It performs modular polynomial multiplication using twiddle factors and implements **Barrett reduction** for efficient modulus computation. Modules such as mult_gen_0, c_add_0, and barret.v were used to realize the datapath.

Objective:

- Reduce Eve's knowledge of the key
- Output a smaller, high-entropy key
- Support real-time operation on FPGA

Method:
Input: sifted_key from the Sifting block
Hash function:

- Apply MMH (Multilinear Modular Hashing)
- Followed by MH (Modular Hashing) with additional compression
- The MMH stage leverages the NTT for fast polynomial multiplication in a modular ring
- Final result: a compressed key with negligible information leakage.

Toolchain and Simulation

All hardware modules were simulated using **Vivado Design Suite 2018.2**, and testbenches were written to validate the design. Output waveforms were analyzed to ensure logical correctness and timing integrity

Results

- **RTL Schematic of Sifting Block**

Theoretic Transform (NTT), specifically a 2×2 butterfly architecture for efficient modular polynomial multiplication.

Barrett reduction was integrated for modular operations, and all modules were verified using waveform simulations. The implementation demonstrates functional accuracy, minimal resource utilization, and real-time performance suitable for secure FPGA-based QKD systems

2. Methodology

This project focused on designing and implementing two major post-processing blocks for Quantum Key Distribution (QKD) systems—**Sifting** and **Privacy Amplification (PA)**—directly using **Verilog HDL** for FPGA-based real-time execution.

Sifting Block

In a **QKD system**, sifting is the **first post-processing stage**. It retains key bits only when **Alice and Bob's measurement bases match**, ensuring both share a consistent bitstream. It also computes the **Quantum Bit Error Rate (QBER)** by comparing valid bits from both parties.

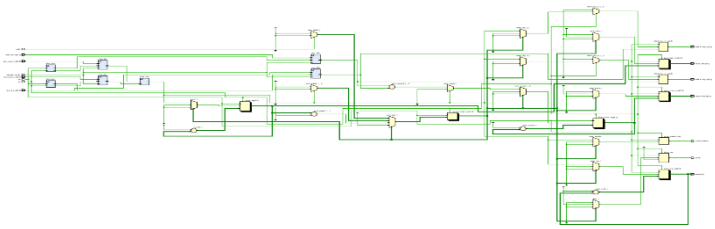
This module was fully designed in **Verilog HDL** for **real-time FPGA execution**.

❖ **Key Functions:**

- Compare basis_a and basis_b
- If matched → retain key_a
- Compute QBER by comparing key_a with key_b

❖ **Modules Used:**

- **comparator** — basis and bit equality check
- **counter** — tracks bit position
- **dff** — flip-flop registers
- **lfsr8** — pseudo-random bit generator
- **mux2to1** — selects valid bits
- **qkd_sifting_bram** — stores sifted bits
- **reg_mem** — internal memory access
- **sifting_core_tb** — testbench for verification



❖ **Sifting Hardware Output**

```
 Starting Simulation...
SIFTED at Addr=0 | ABit=0 BBit=1 | AB=1 BB=1
SIFTED at Addr=1 | ABit=0 BBit=1 | AB=0 BB=0
SIFTED at Addr=2 | ABit=1 BBit=0 | AB=1 BB=1
DISCARDED          | ABit=0 BBit=1 | AB=1 BB=0 (basis mismatch)
SIFTED at Addr=3 | ABit=1 BBit=0 | AB=1 BB=1
DISCARDED          | ABit=1 BBit=0 | AB=0 BB=1 (basis mismatch)
SIFTED at Addr=4 | ABit=0 BBit=0 | AB=1 BB=1
SIFTED at Addr=5 | ABit=1 BBit=1 | AB=0 BB=0
SIFTED at Addr=6 | ABit=1 BBit=0 | AB=1 BB=1
SIFTED at Addr=7 | ABit=1 BBit=1 | AB=0 BB=0
SIFTED at Addr=8 | ABit=0 BBit=0 | AB=1 BB=1
SIFTED at Addr=9 | ABit=1 BBit=0 | AB=1 BB=1
SIFTED at Addr=10 | ABit=1 BBit=1 | AB=0 BB=0
FSM reached DONE at time = 695000

==== QKD Sifting Result ====
Total sifted bits : 11
Error bits        : 6
QBER (%)          : 54.55%
```

Refrences

1. An FPGA-Based 4 Mbps Secret Key Distillation Engine for Quantum Key Distribution Systems
2. An Overview of Postprocessing in Quantum Key Distribution
3. A Real-Time QKD System Based on FPGA
4. A Complete Beginner Guide to the Number Theoretic Transform (NTT) – Ardianto Satriawan, Rella Mareta, Hanho Lee
5. Open-Source FPGA Implementation of Number-Theoretic Transform for CRYSTALS-Dilithium

Student Profile

Name: Sourabh Tyagi
Institute Name: VIT-AP University
RISE-UP Batch: 05/2025, 22BEC7191
Project Guide: Rohit Chaurasiya, IIT Jammu