NTT Accelerator with AXI Stream Wrapper

Hardware Module Specification

1. Overview

The **NTT (Number Theoretic Transform) Accelerator** is a hardware module designed to perform fast number theoretic and inverse number theoretic transformations, primarily used in post-quantum cryptographic algorithms such as *Kyber*. The accelerator supports both NTT and INTT modes, selectable through a dedicated control signal. It uses a standard **AXI4-Stream** interface for input and output data, ensuring full compatibility with DMA controllers, memory interfaces, or other AXI-compliant components.

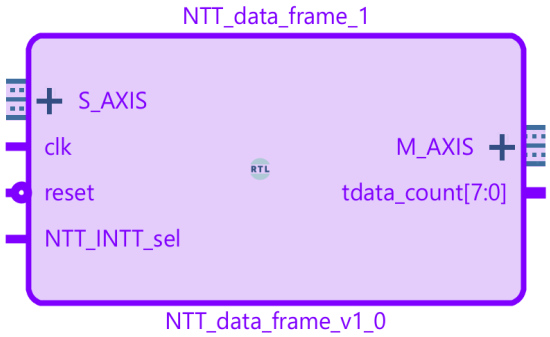

Figure 1: AXI Stream Based Wrapper for NTT/INTT accelerator

2. Interface Description

2.1. Clock and Reset

Signal	Direction	Description
`clk`	Input	System clock input. The accelerator supports operating frequencies up to **100 MHz**.
`aresetn`	Input	Active-low asynchronous reset. When deasserted (logic 0), the accelerator resets all internal registers and counters.

2.2. Control Signal

Signal	Direction	Description
`NTT_INTT_sel`	Input	Mode select signal: • Logic '1' → Perform **NTT Transform** • Logic '0' → Perform **Inverse NTT (INTT)**

2.3. AXI Stream Input Interface (S_AXIS)

Signal	Direction	Width	Description
S_AXIS_tdata	Input	32 bits	Input data stream to the accelerator. Each transaction represents a 32-bit coefficient or word.
S_AXIS_tvalid	Input	1 bit	Indicates that valid data is available on S_AXIS_tdata.
S_AXIS_tready	Output	1 bit	Indicates that the accelerator is ready to accept data.
S_AXIS_tlast	Input	1 bit	Marks the last data word of a packet or frame. Used for end-of-stream indication.

Data Transfer Rule: A data word is transferred on the rising edge of the clock when both S_AXIS_tvalid and S_AXIS_tready are high.

2.4. AXI Stream Output Interface (M_AXIS)

Signal	Direction	Width	Description
M_AXIS_tdata	Output	32 bits	Output data stream containing transformed coefficients.
M_AXIS_tvalid	Output	1 bit	Indicates valid output data on M_AXIS_tdata.
M_AXIS_tready	Input	1 bit	Indicates that the downstream component is ready to receive data.
M_AXIS_tlast	Output	1 bit	Indicates the last output data corresponding to the input frame. Mirrors S_AXIS_tlast.

2.5. Indicator Signal

Signal	Direction	Width	Description
tdata_counter	Output	32 bits	A register that tracks the number of valid data words successfully streamed into the accelerator via the AXI Stream interface. It increments when both S_AXIS_tvalid and S_AXIS_tready are asserted.

3. Functional Description

When data streaming begins, the accelerator continuously receives data through the AXI Stream input interface and performs the selected NTT or INTT transformation internally.

3.1. Data Flow Rules

1. **Start of Data:** When S_AXIS_tvalid is asserted, the accelerator assumes that a new data frame has started. From this point, 128 data words are expected continuously. Internal counters increment only when both S_AXIS_tvalid and S_AXIS_tready are high.

2. **Continuous Stream:** Data must be transmitted without interruption until all 128 data words are sent. Since AXI4-Stream does not carry address information, the accelerator uses this 128-count sequence to detect frame boundaries.

3. **Incomplete Stream Handling:** If data streaming is interrupted:

   - Send remaining dummy data until the count reaches 128, allowing the internal counter to reset properly, or
   - Deassert `aresetn` momentarily to force the accelerator into idle, then restart streaming.

4. `S_AXIS_tlast` **Behavior:** The `S_AXIS_tlast` signal does not affect internal computation; however, after `S_AXIS_tready` is deasserted, up to 30 data cycles may remain unread due to slower read speed compared to write speed. It is simply propagated to the output as `M_AXIS_tlast` to mark the final data word.

4. Performance Constraint

The accelerator requires that the data fetch rate (**read speed**) be greater than or equal to the input data rate (**write speed**).

- **Read speed:** Rate at which the next stage (e.g., DMA or memory) fetches data from `M_AXIS`.
- **Write speed:** Rate at which data is streamed into `S_AXIS`.

If the read speed is lower, data congestion may occur. To mitigate this, use a FIFO buffer at the output side of the accelerator to absorb timing mismatches and ensure continuous operation.

5. Summary of Key Points

Category	**Condition / Rule**
Data width	32 bits
Frame length	128 / 256 samples per transform
Supported frequency	Up to 100 MHz
Operating modes	NTT / INTT
AXI Protocol	Standard AXI4-Stream
Required condition	Read speed Write speed
Error handling	Send garbage data to complete 128 count or assert reset
`tlast` usage	Indicates end of data frame only