DESIGN AND IMPLEMENTATION OF SUBNORMAL FLOATING-POINT SoC FOR SECURED SIGNAL PROCESSING USING PIPELINE INTERCONNECT

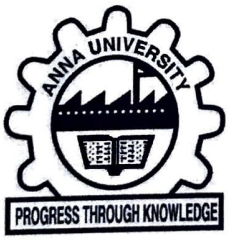
A THESIS

Submitted by

SENTHIL P

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY



FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

ANNA UNIVERSITY

CHENNAI 600 025

AUGUST 2020

ABSTRACT

Software level implementation, execution time variations of the equal-sized inputs in a floating-point (FP) instruction are quantifiable that bring out the information of the executed data from a secured environment. These quantifiable timing variations are called as data timing channels (DTC). The exposed data state is captured and analysed by an adversary for retrieving the image pixels on a deep neural network (DNN) through multiplication timing channels (MTC). MTC is happened when normalized and subnormal FP numbers are taken for FP multiplication. Procedures used in normalization and denormalization have differed for normalized and subnormal numbers used in FP arithmetic. Both procedures produce different amounts of delay in FP multiplication that results in MTC. In conventional CPU and GPU implementations, the combination of subnormal number and normalized number are not used in the FP addition and multiplication.

Processing of subnormal numbers shows the performance degradation in the form of delay, area, and power consumption in conventional hardware. In hardware and software implementation, normalized and subnormal numbers may produce the zero, subnormal and normalized output with different delays. Subnormal processing does not make any complexity in FP addition but it affects severely in FP multiplication as well as fused multiply-add. The negative exponent normalized (NEN) inputs are having the level of complications that equals to the subnormal numbers. It requires the denormalization before the mantissa computations and again it requires the normalization after mantissa computations. Denormalization and normalization for the NEN number increase the delay, area, and power consumption in its denormalization hardware. In this work, it is being proposed as a single step after mantissa multiplication in FP multiplication.

The main objective of the proposed work is to provide an effective hardware design for subnormal number processing. Subnormal processing experiences the inconsistent delays on behalf of additional hardware. This delay is a source for creating the DTC. Another objective is to resolve the inconsistent delays in the FP multiplier rather than FP addition.

At first phase, initially a conventional normalized FP adder is designed with the delay of 65.18 ns. Later, additional circuits for subnormal /NEN processing are introduced in this conventional FP adder with a delay of 70 ns Subnormal processing slightly increases the delay in FP adder and DTC is not generated. Multiplier is proposed for subnormal/NEN processing at second phase, it produces the subnormal, normalized, infinity, and zero outputs with the delays of 45.50 ns, 42.23 ns, 11.62 ns, and 10.12 ns respectively in Startix III FPGA. One important observation is noted that subnormal processing provides delay inconsistency in FP multiplier. Unintentional or unbalanced delays are caused in subnormal processing for stand-alone FP multiplication.

The consequence of an unbalanced delay is opening the DTC on four paths for the attacker to capture the timing variations. In the four-path proposed multiplier, it is resolved through the delay balancing for mitigating the DTC at third phase, the delay of the multiplexer and flip flop based mitigations are balancing at the level of 48.68 ns and 42.56 ns respectively. Both mitigations are using the control circuit based delay balancing in the FP multiplier to avoid the DTCs. Further pipelined implementation reduces the delay in 4-path multiplier with the latency of 11 clock cycles.

Finally, the integration of the FP adder and FP multiplier is formed as a pipelined FMA microarchitecture. The proposed microarchitecture performs the FP addition, FP multiplication, and FMA operations. Proposed subnormal number processing modifies the single-cycle FMA operation into two cycles where one cycle is for multiplication another one cycle is taken for

accumulation. Proposed subnormal number processing, FP data paths are designed as per the IEEE 754 single precision standard. Gate level circuits are designed in Verilog HDL and converted into block symbols. All block symbols are connected in IEEE 754 standard to get the FP adder, multiplier and FMA unit design. In this design, Intel Quartus II 16.1 EDA tool is used for interconnecting all the sub-blocks. The tool simulates the FP data path for functional verification and synthesizes to implement the designed circuit in Stratix III FPGA. Consequently, power and timing are checked using power play power analyser and time quest timing analyser in Intel Quartus II 16.1 EDA.

Due to the DTC threats, subnormals and NEN inputs are avoided in conventional FP data paths. When normalized input is combined with NEN/subnormal inputs for FMA operations used in CNN, quantifiable delay variations bring the state of the image pixel/weight. It is captured by the adversary to recover the image pixel and weight. Proposed FP hardware hides the quantifiable delay into a balanced delay in subnormal processing. Future research of FP SoC will be carried in ASIC implementation. Accurate STA in ASIC tools will calculate the gate delay as well as wire delay. The purpose of the accurate STA will be used to find the chances of insertion of hardware trojan (HT) in longest as well as shortest paths. Measurable path delay can help to identify the HT and HT can alter the functionality of FP circuit easily. It should be avoided through the hardware obfuscation that hides the physical structure of the circuits without affecting its functionalities.