Changelog to WAGE (Round 2 Candidate)

Mark Aagaard, Riham AlTawy, Guang Gong, Kalikinkar Mandal, Raghvendra Rohit, and Nusa Zidaric

September 27, 2019

The following changes are done in WAGE Round 2 submission.

- 1. In Chapter 6: Major editorial changes, including:
 - Fix in Figure 6.1: i_mode signal remove 2-bit(mistake in old fig)
 - Expanded Section 6.2 with details on
 - 6.2.1 Interface protocol
 - 6.2.2 Protocol timing
 - 6.2.3 Control phases
 - Expanded Section 6.3 (changed section title accordingly)
 - 6.3.1 State machine
 - 6.3.2 WAGE datapath (previously Section 6.3.1)
 - Changes between old and new WAGE datapath section
 - * added more detailed explanation
 - * new Figure 6.11, showing details on input/output multiplexers and control multiplexers, figure reflected in text
 - Expanded table 6.2 to include more detailed theoretical estimates (now table 6.5), corresponding text is changed to match the new table
 - Removed old Section 6.3.2 "The WAGE_module and the control" Rationale: Section 6.3.1 is entirely dedicated to WAGE FSM
 - In Section 6.4:
 - * Removed table 6.3:
 - · the synthesis results for the WAGE permutation are subsumed in Table 6.2
 - · the "pre-PAR, no optimizations" synthesis results are replaced by "post-PAR, with optimizations" synthesis results in Table 6.7 (column ST Micro 65 nm)
 - * Table 6.7 new ASIC implementation results
 - · "post-PAR, with optimizations" synthesis results
 - \cdot added technologies: TSMC 65 nm, ST Micro 90 nm, IBM 130 nm
 - · results for unrolled (parallel) implementations

Note that the area and performance data have changed slightly due to improvements in the synthesis scripts.

- 2. Fixed the bug related to tag generation in the reference implementation. More specifically, the last 2 bits of tag were always zero. The bug was in wage_gentag function and details are as follows.
 - Incorrect one: $tmp_tag[18] = ((state[18] \gg 2) \& (0x03));$
 - Correct one: $tmp_{tag}[18] = ((state[18] \ll 2) \& (0x60));$

Note that the bug does not affect the specification of WAGE. The fixed code has been already posted on LWC forum (OFFICIAL COMMENT: WAGE, dated April 30, 2019). We have included the updated code with round 2 package for the sake of completeness.

- 3. Added microcontroller code with the submission package.
- 4. Fixed some minor typos in the document.
- 5. Updated the current affiliation of Riham AlTawy and link of WAGE website in coversheet.