Changelog to ACE (Round 2 Candidate)

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

September 27, 2019

The following changes are done in Round 2 ACE submission.

1. **In Chapter 6:** Major editorial changes, including:
   - 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 ACE datapath (previously Section 6.3.1)
   - Changes between old and new ACE datapath section
     - updated Figure 6.2 (now Figure 6.12):
       - added two missing round/step multiplexers
       - more details on input/output multiplexers
       - changed SB-64 to highlight its implementation details
     - some changes in text to match the new Figure 6.2
     - added detailed description of use of the multiplexers in Figure 6.2
   - Expanded Table 6.3 to include more detailed theoretical estimates (now Table 6.7), corresponding text is changed to match new table
   - Removed old Section 6.3.2 "ACE FSM and lfsr_c" Rationale: Section 6.3.1 is entirely dedicated to ACE FSM while lfsr_c is discussed in detail in Section 5.6.2
   - In Section 6.4:
     - Removed Table 6.4:
       - the synthesis results for the ACE permutation are subsumed in Table 6.3
       - the "pre-PAR, no optimizations" synthesis results are replaced by "post-PAR, with optimizations" synthesis results in Table 6.9 (column ST Micro 65 nm)
     - Table 6.9 - new ASIC implementation results
       - "post-PAR, with optimizations" synthesis results
       - 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. There are minor changes in the testbench of ACE hardware implementation. The corresponding changelog file is added in add_vhdl folder.

2. Added comments in software codes to make them more comprehensible. Moreover, we have included microcontroller codes with the submission package in add_mCPU folder.

3. Fixed some minor typos.

4. Changes in coversheet:

   - updated the website link
   - current affiliation of Riham AlTawy is added as a footnote.