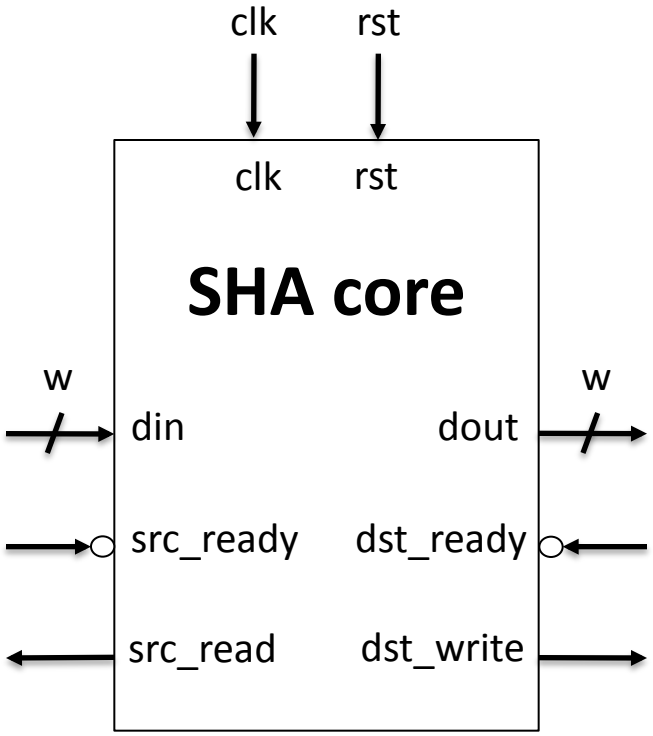
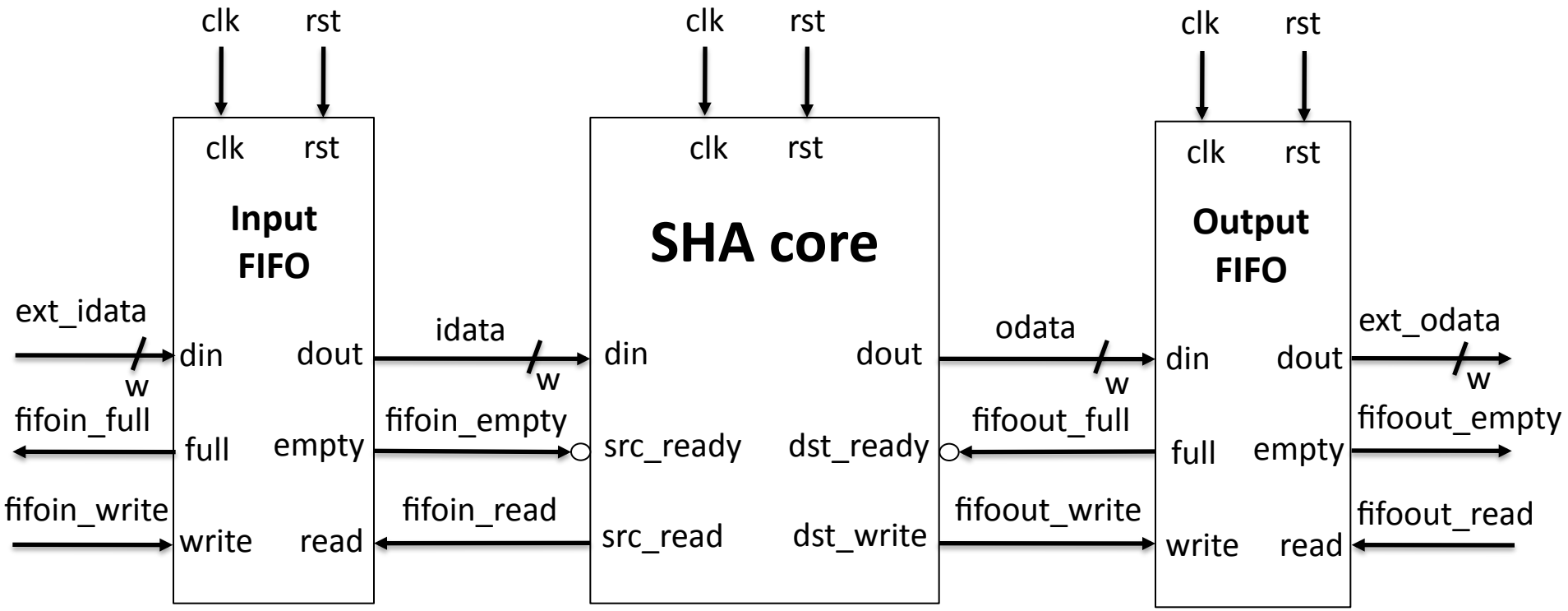
The GMU Interface & Communication Protocol Used in the Implementations of the SHA-3 Round 3 Candidates

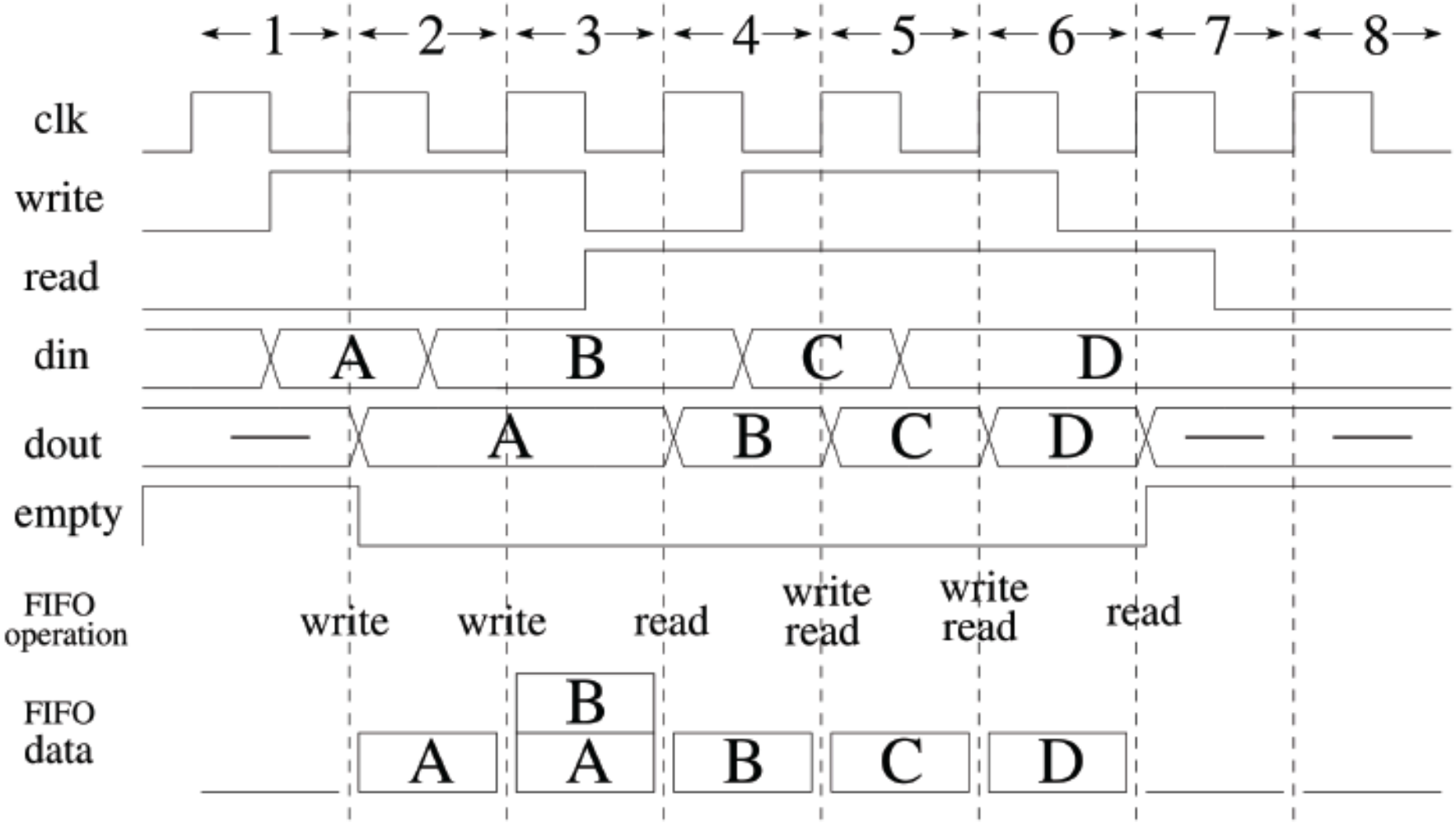
SHA Core Interface



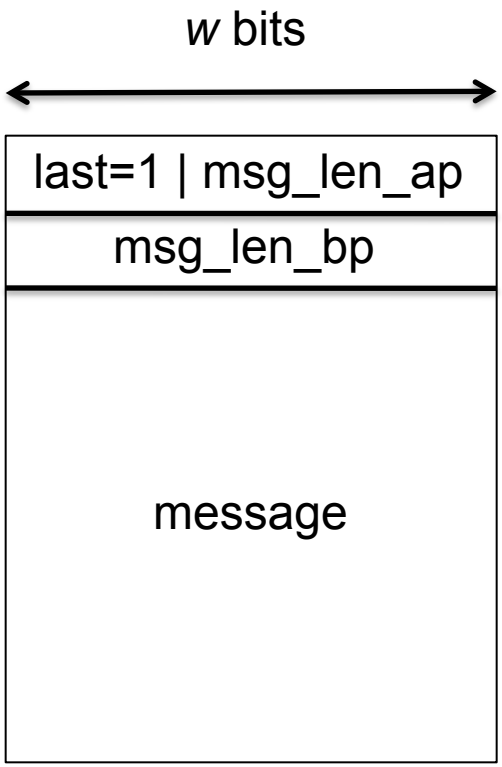
SHA Core Interface + Surrounding FIFOs



Operation of FIFO

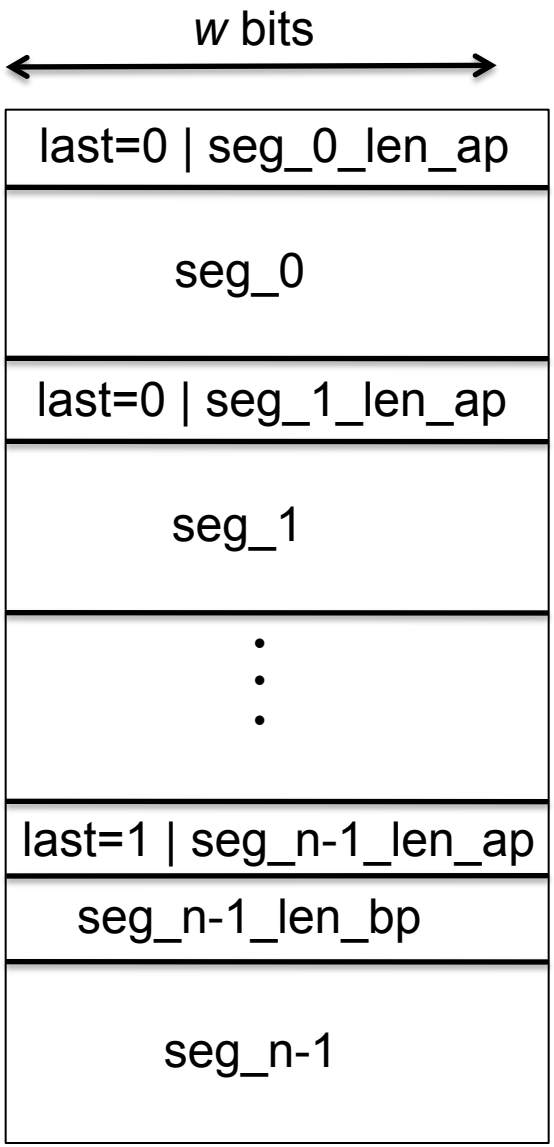


Communication Protocol for Padded Messages Without Message Splitting



msg_len_ap – message length after padding [bits]
msg_len_bp – message length before padding [bits]

Communication Protocol for Padded Messages With Message Splitting



seg_i_len_ap – segment i length after padding* [bits]

seg_i_len_bp – segment i length before padding [bits]

* For all i < n-1 segment i length after padding is assumed to be a multiple of the message block size, *b* [characteristic to each function], and thus also the word size, *w*. The last segment cannot consist of only padding bits. It must include at least one message bit.