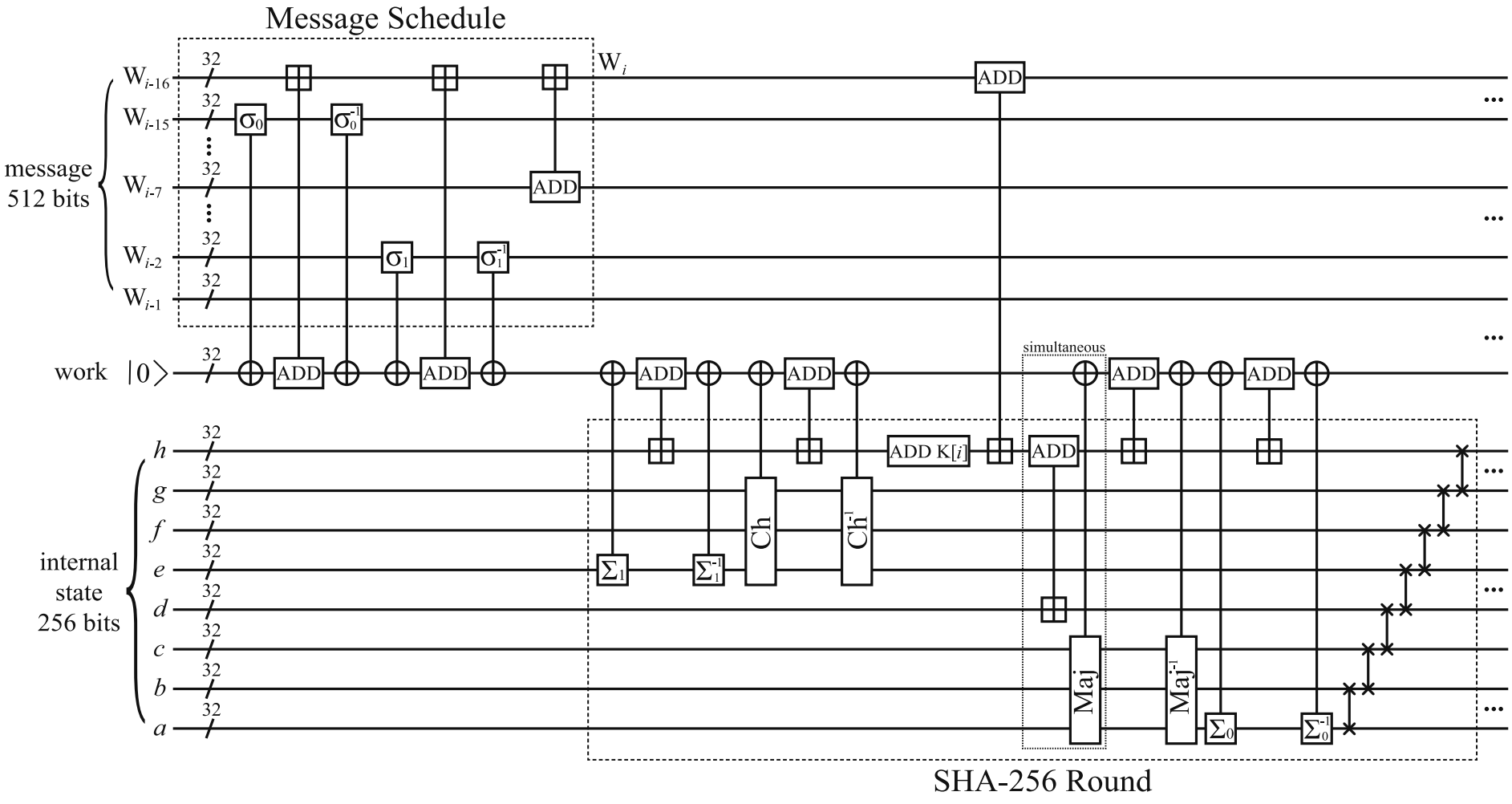

Fig. 10 Reversible circuit for serial implementation of SHA-256 message schedule and round function. The message block consisting of 16 words is recursively updated in place. Note that it is straightforward to make message schedule and round functions work in parallel by expanding the work space. Seven two-qubit gates at the end of round are SWAP gates. The symbol $\boxplus$ is addition modulo 2^{32}