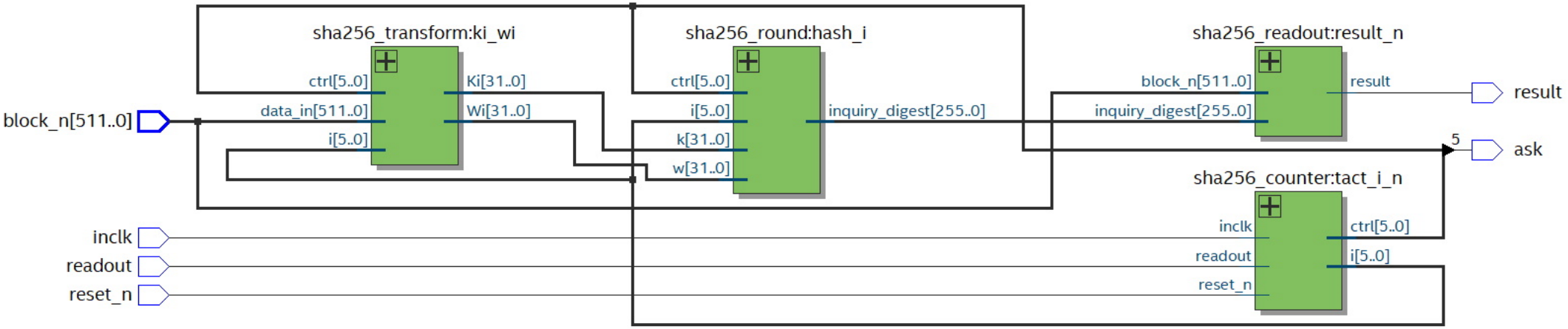
SHA256 hash chesker IP
(intellectual property virtual component)

(EN)
The block calculates the message hash from the sequence of prepared 512-bit data blocks and compares it with the given template.
Processing each data block requires 64 clock cycles.
The process of interaction with the block is carried out in the following sequence.
At the beginning of each calculation cycle, set the reset input to high and read to low.
Submit the clock frequency to the "inclk" input.
Form a low level "reset_n" with the beginning and end on the trailing edges of such a signal.
When high levels of the request signal "ask" appears and no later than 1/2 of the period, put first and next 512-bit message data blocks at the "block_n" input.
Simultaneously with setting the last data block, set the "readout" input to a high level.
At the next request "ask", set a control hash data at the "block_n" input.
With a corresponding message hash after 1 period, the output of the "result" will go to a low value for 1 clock period.

(РУС)
Блок вычисляет хеш сообщения из последовательности подготовленных 512-битных блоков данных и сравнивает его с заданным шаблоном.
Обработка каждого блока данных требует 64 такта.
Процесс взаимодействия с блоком осуществляется в следующей последовательности.
В начале каждого цикла расчета установить на входах ресет высокий, а чтения низкий уровни.
Подать синхро-частоту на вход такт.
Сформировать ресет с началом и окончанием по задним фронтам такового сигнала.
На появление высоких уровней сигнала запроса и не позже 1/2 периода выставлять на вход данных очередные 512-битные блоки данных сообщения.
Одновременно с выставлением последнего блока данных выставить на вход чтения высокий уровень.
На следующий запрос выставить на вход данных контрольный хеш.
При хеше соответствующем сообщению через 1 период выход результата перейдет в низкое значение на 1 тактовый период.

Circuit pucker 6 - synchronous duct with the shift register and counter separately and ask



Circuit pucker 6 - two-blocks message hashing epures