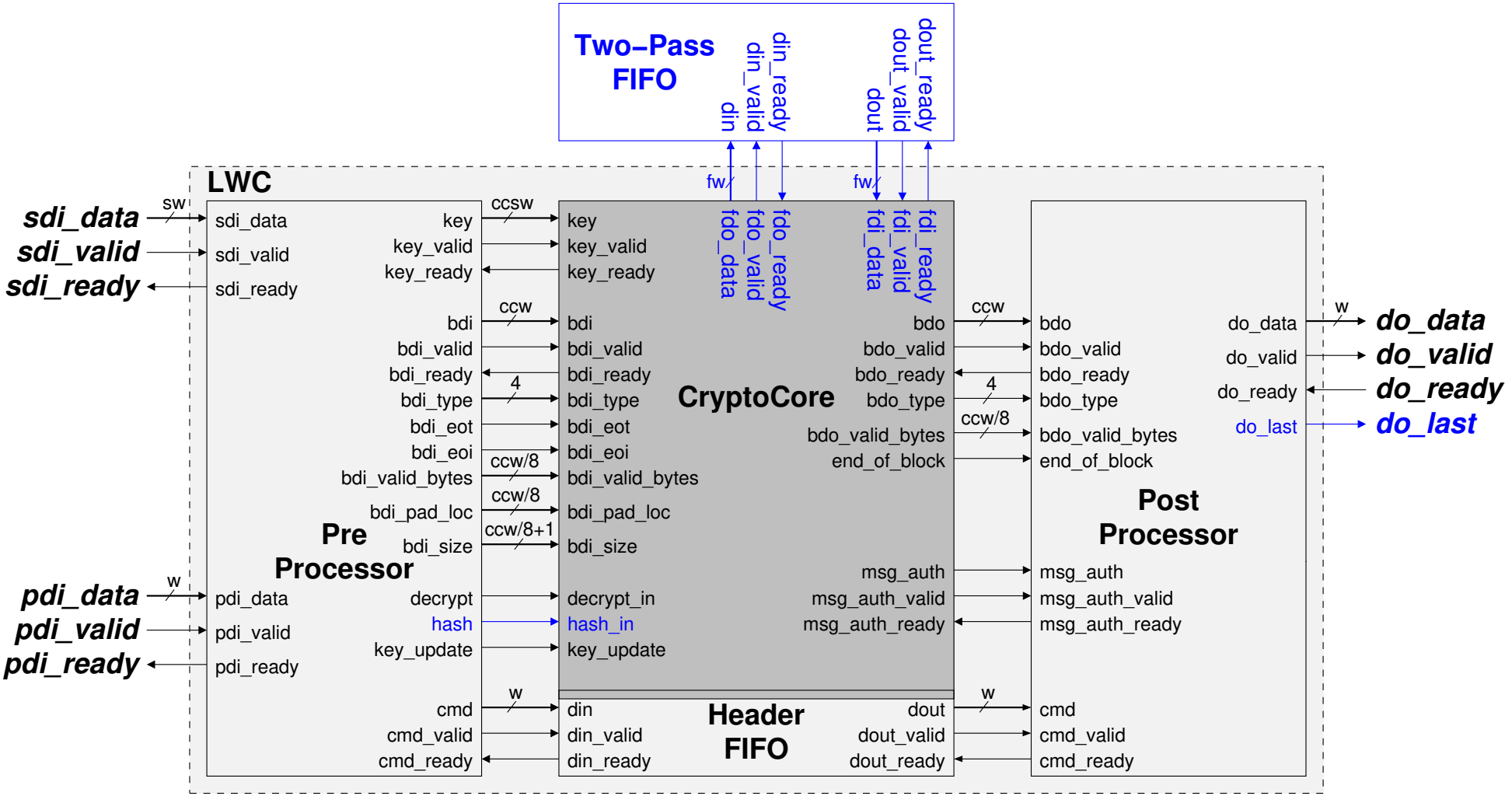
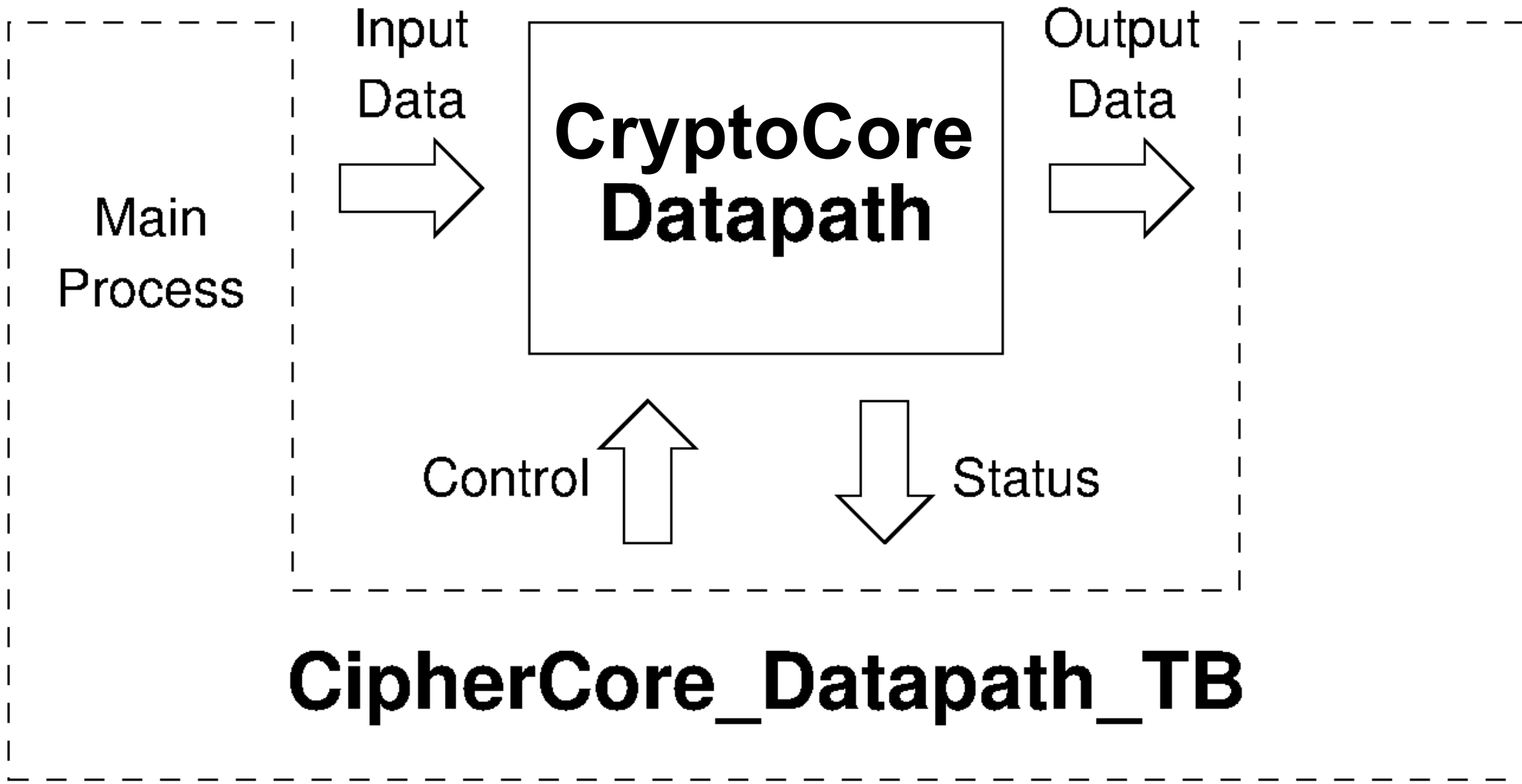
Verification

Overview


Two–Pass FIFO
din
din_valid
din_ready
dout
dout_valid
dout_ready
fw
fdo_data
fdo_valid
fdo_ready
fdi_data
fdi_valid
fdi_ready
LWC
sdi_data
sdi_valid
sdi_ready
sw
sdi_data
sdi_valid
sdi_ready
Pre Processor
key
key_valid
key_ready
ccsw
bdi
bdi_valid
bdi_ready
bdi_type
bdi_eot
bdi_eoi
bdi_valid_bytes
bdi_pad_loc
bdi_size
ccw
4
ccw/8
ccw/8
ccw/8+1
pdi_data
pdi_valid
pdi_ready
w
decrypt
hash
key_update
cmd
cmd_valid
cmd_ready
CryptoCore
key
key_valid
key_ready
bdi
bdi_valid
bdi_ready
bdi_type
bdi_eot
bdi_eoi
bdi_valid_bytes
bdi_pad_loc
bdi_size
decrypt_in
hash_in
key_update
Header FIFO
din
din_valid
din_ready
dout
dout_valid
dout_ready
bdo
bdo_valid
bdo_ready
bdo_type
bdo_valid_bytes
end_of_block
msg_auth
msg_auth_valid
msg_auth_ready
Post Processor
bdo
bdo_valid
bdo_ready
bdo_type
bdo_valid_bytes
end_of_block
msg_auth
msg_auth_valid
msg_auth_ready
cmd
cmd_valid
cmd_ready
do_data
do_valid
do_ready
do_last
w
do_data
do_valid
do_ready
do_last

Phase I
Datapath

Phase I: Verification



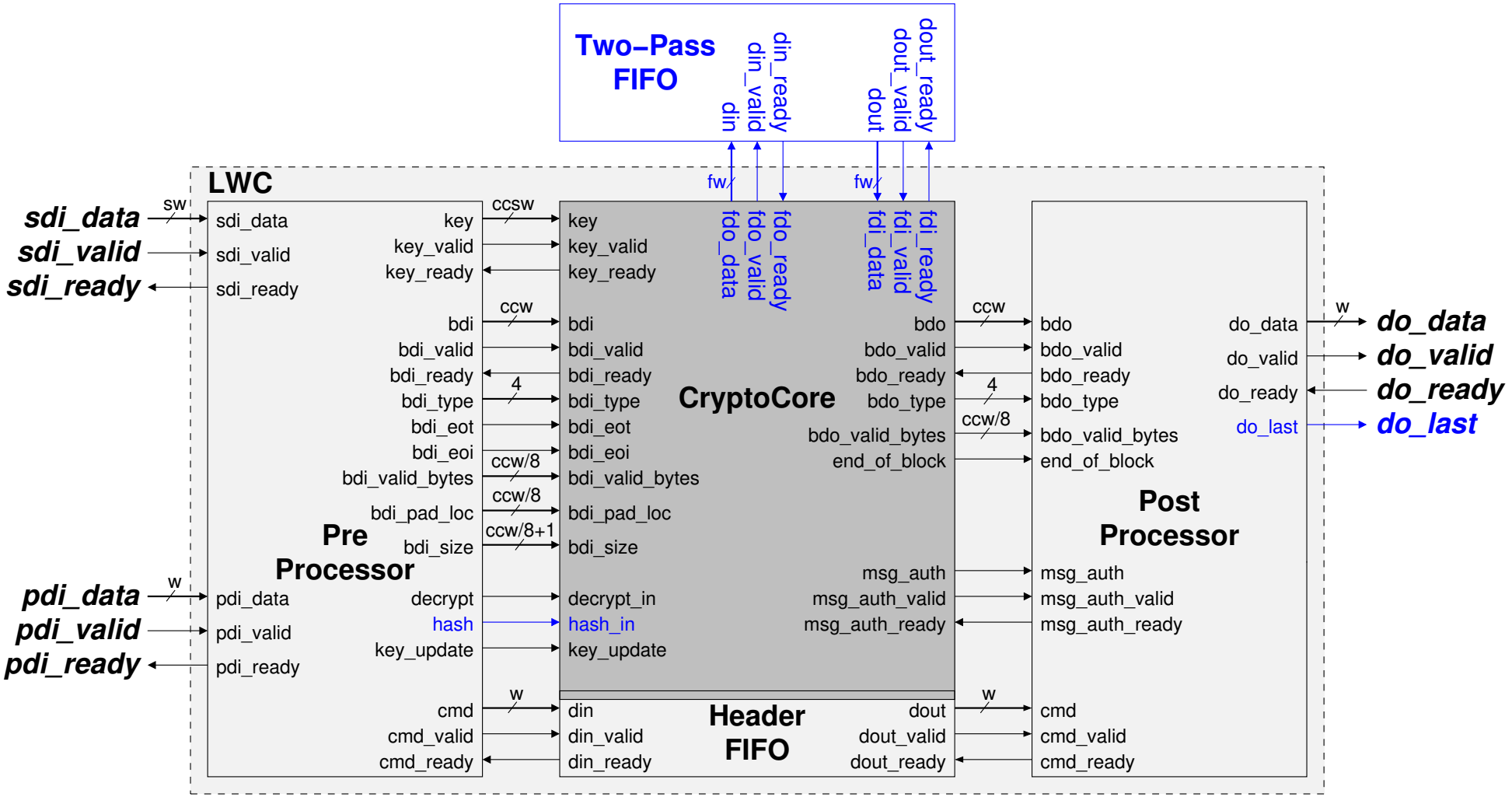
Phase I: Verification

Consists of one primary process handling input, control and verification against expected output

Testbench should focus on the verification of basic functionality of the circuit. At a minimum, it should verify a complete operation for encryption and decryption with two blocks of data.

Control signals should emulate the behavior of the future controller

Phase II
LWC


Two–Pass FIFO
din
din_valid
din_ready
dout
dout_valid
dout_ready
LWC
fw
fdo_data
fdo_valid
fdo_ready
fdi_data
fdi_valid
fdi_ready
sdi_data
sdi_valid
sdi_ready
sw
sdi_data
sdi_valid
sdi_ready
key
key_valid
key_ready
ccsw
bdi
bdi_valid
bdi_ready
bdi_type
bdi_eot
bdi_eoi
bdi_valid_bytes
bdi_pad_loc
bdi_size
ccw
4
ccw/8
ccw/8
ccw/8+1
Pre Processor
pdi_data
pdi_valid
pdi_ready
w
decrypt
hash
key_update
cmd
cmd_valid
cmd_ready
w
key
key_valid
key_ready
bdi
bdi_valid
bdi_ready
bdi_type
bdi_eot
bdi_eoi
bdi_valid_bytes
bdi_pad_loc
bdi_size
decrypt_in
hash_in
key_update
CryptoCore
din
din_valid
din_ready
Header FIFO
bdo
bdo_valid
bdo_ready
bdo_type
bdo_valid_bytes
end_of_block
msg_auth
msg_auth_valid
msg_auth_ready
dout
dout_valid
dout_ready
ccw
4
ccw/8
w
bdo
bdo_valid
bdo_ready
bdo_type
bdo_valid_bytes
end_of_block
msg_auth
msg_auth_valid
msg_auth_ready
cmd
cmd_valid
cmd_ready
Post Processor
do_data
do_valid
do_ready
do_last
w
do_data
do_valid
do_ready
do_last

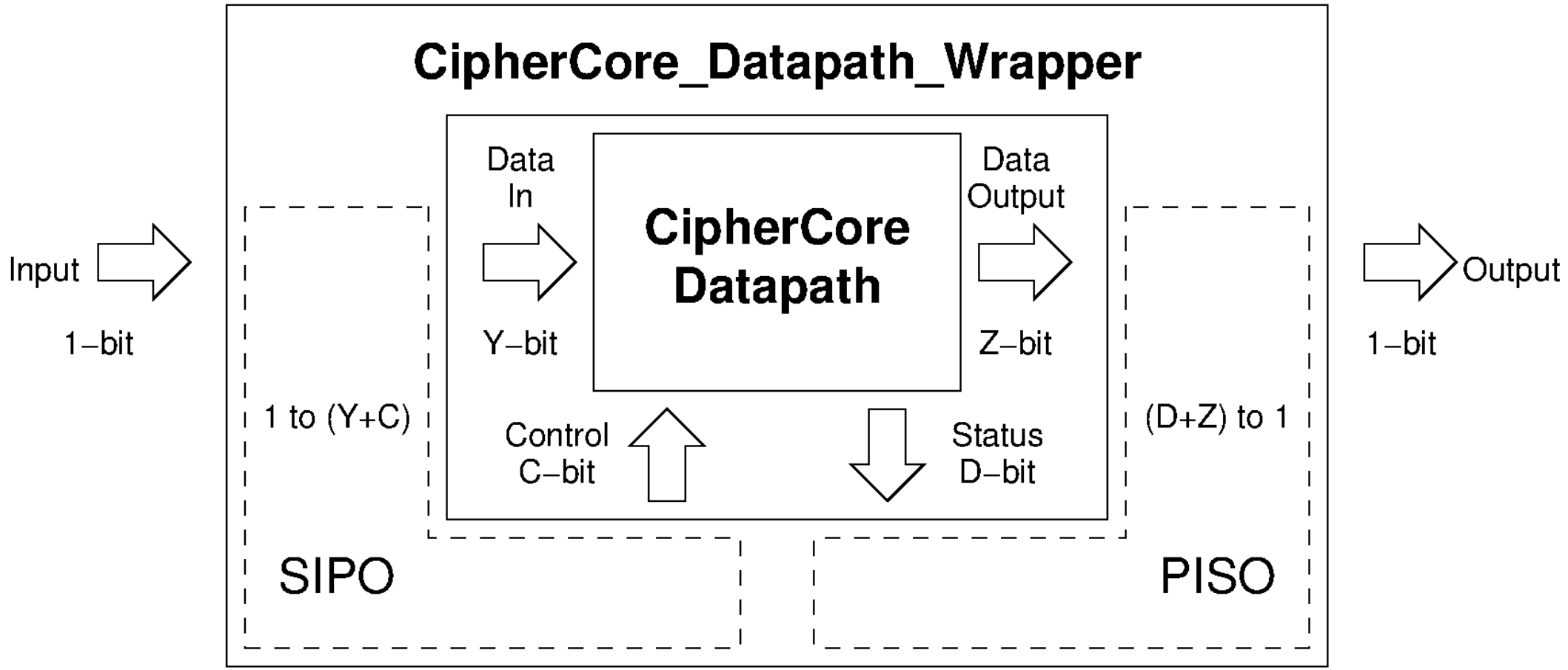
Result Generation

Phase I: Result Generation

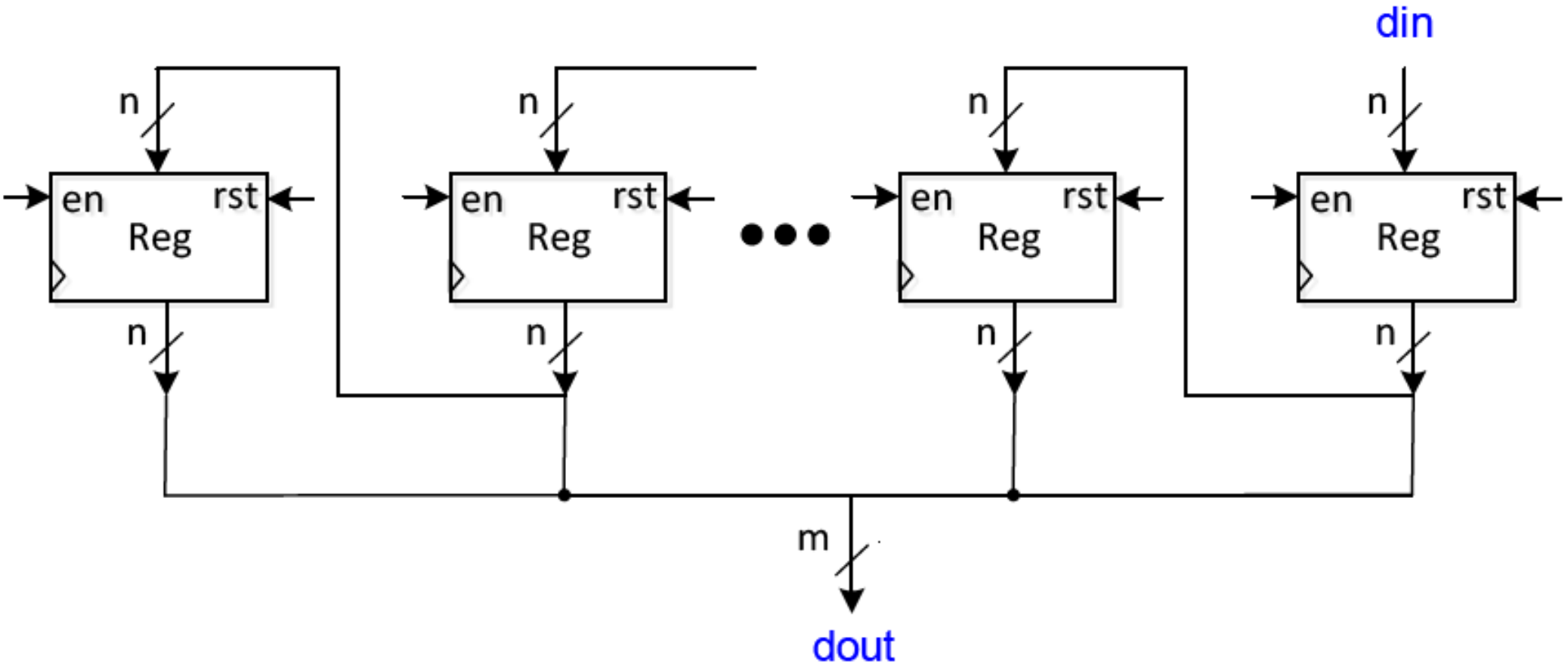
Generation of results often cannot be done directly due to the limit on the number of pins in the targeted chips.

As a result, one must wrap a unit using components such as SIPO (Serial-In-Parallel-Out) and PISO (Parallel-In-Serial-Out) units.

Result Generation



SIPO: Serial In Parallel Out



PISO: Parallel In Serial Out

