

# GH09.B.3.crypto – Encryption

---

This specifies details about the workloads associated with the GH09.B.3 design.

## Input Workloads

---

The workloads for this benchmark that when combined with this design specification, form a benchmark. The workloads for this design are defined by the following events. Please see the [groundhog\\_09\\_meta\\_document.pdf](#) for a description of workloads.

For this design the key input events are:

- reset – the reset signal [signal event]
  - <value0> tag is the associated Boolean value of the signal. Note that the value can be flipped if the designers wish, and the goal is to indicate the initialization of the system.
- key – this indicates that a 32byte input that will be the cipher key is coming in on the input bus. The 32bytes are stored in value0 and the macro process is for the next 8 input\_data\_valid signals (described below) the key signal will remain active to indicate to the device that the key is being passed in. Once 8 input\_data\_valid signals have occurred then the key signal will be turned off [macro event]
  - <value0> is the hex string value of the cipher key
- input\_block – this is a block of data that will be encrypted. This block should be a string of data that is X\*32bytes long. This block will be read into the device for X\*2 input\_data\_valid signals. The input\_block format is a way of specifying a buffer of data in the external environment that will be streamed into the SUT. [macro event]
  - <value0> is the hex string that is X\*32bytes long
- Input\_data\_valid – this is the signal that indicates the data on the input pins is ready. In the case when this resource is associated with an input resource then it is a simple read. If associated with an input\_block resource it means to read the next 16bytes of the input\_block's string. [signal event]
  - <value0> is the Boolean signal being sent. The default signal will be 1, but note that within the workload there is no associated 0 signal.

## Outputs from the golden functional model tool

---

The associated output resources that will be generated by the golden functional model are:

- output – this is the 32byte output string that represents the encrypted last input. It is also assumed that the `output_data_valid` signal would be sent with the output for every 16 bits of output data. This does not take into account that the *output* signal in the design is only 16 bits wide. [macroevent]
  - <value0> is the 32 character hex string

Note, neither the `output_data_valid` or `input_data_accept` signals are included in the output workload. These signals are part of the handshaking protocol and have been left out for simplicity. These signals, if used, should be verified by the designer.