**CAMELLIA SPECIFICATION**

**INTERFACE *(portName\_(direction))***

**KIN\_I:** The data input array [KIN\_I()] is used to pass a new key to the cipher.

**KRDY\_I:** The key ready input [KRDY\_I], when asserted, indicates that a new key is provided in KIN\_I.

**DIN\_I:** The data input array [DIN\_I()] is used to pass a word to the cipher.

**ENCDEC\_I:** The encdec input [ENCDEC\_I] indicates whether the current data in DIN\_I is to decrypt or to encrypt. The signal is negated to ENCRYPT, and is asserted to DECRYPT the input data.

**DRDY\_I:** The data ready input [DRDY\_I], when asserted, indicates the beginning of either a new encryption phase, or a new decryption phase.

**BSY\_O:** The busy output [BSY\_O()], when asserted, indicates that the cipher is either reading a new key, or it is (de)encoding a word.

**KVDL\_O:** The key read output [KVDL\_O}, when asserted, indicates that the cipher read a key.

**DVLD\_O:** The data ready output [DVDL\_O], when asserted, indicates that new data is provided on [DOUT\_O]

**DOUT\_O:** The data output array [DOUT\_O] provides the output result generated by the cipher.

**Load a key**

* CLOCK EDGE 0
  + A key is provided on [KIN\_I]
  + [KRDY\_I] is asserted
* CLOCK EDGE 1
  + cipher asserts BSY\_O in response to asserted [KRDY\_I]
* CLOCK EDGE 7
  + cipher negates BSY\_O
  + cipher asserts [KVDL\_O]

**encode a word**

* CLOCK EDGE 0
  + A word is provided on [DIN\_I]
  + [ENCDEC\_I] is negated
  + [DRDY\_I] is asserted
* CLOCK EDGE 1
  + cipher asserts BSY\_O in response to asserted [DRDY\_I]
* CLOCK EDGE 24
  + cipher negates BSY\_O
  + cipher asserts [DVDL\_O]
  + cipher provides new data on [DOUT\_O]

**decode a word**

* CLOCK EDGE 0
  + A word is provided on [DIN\_I]
  + [ENCDEC\_I] is asserted
  + [DRDY\_I] is asserted
* CLOCK EDGE 1
  + cipher asserts BSY\_O in response to asserted [DRDY\_I]
* CLOCK EDGE 24
  + cipher negates BSY\_O
  + cipher asserts [DVDL\_O]
  + cipher provides new data on [DOUT\_O]