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]