DES Hardware Macro Specification

Version	Update	Description
0.1	2007/09/04	Initial version is created
0.2	2007/09/25	Timing chart is modified

1. Overview

The features of this DES hardware macro are summarized in Table 1. Detailed algorithm is designed in the FIPS 46-3 [1] specification. Only the ECB (Electronic Code Book) mode is supported, but the other modes such as CBC (Cipher Block Chaining) can be easily supported by using additional data buffers and a control circuit.

Table 1 DES hardware macro overview

Algorithm	DES
Data block size	64 bits
Key size	64 bits
Mode of operation	Electronic Code Book (ECB)
Source file name	DES.v
Description Language	Verilog-HDL
Top module name	DES
Throughput	64 bit / 16 clock
Round keys	On-the-fly

2. I/O ports

I/O ports of the DES macro are summarized in Table 2.

Table 2 I/O ports

Port name	Direction	Width	Description
Kin	In	64	Key input
Din	In	64	Data input
Dout	Out	64	Data output
Krdy	In	1	When Krdy=1, a secret key is latched in an internal register, and initial key scheduling process is executed. If Drdy and Krdy assigned to be '1' at the same time, Krdy=1 has priority.
Drdy	In	1	When Drdy=1, a plaintext (or ciphertext) data is latched in an internal register, and encryption (or decryption) process is

			started.
EncDec	In	1	Encryption and decryption are executed when EncDec=0 and EncDec=1, respectively. Bit data on the port EncDec is stored in an internal register when encryption or decryption starts in response to Drdy=1.
RSTn	In	1	Reset signal. Sequencer logic and internal registers are reset when this signal is assigned to 0. Reset can be executed any time when the clock signal CLK is input, even if the enable signal EN=0.
EN	In	1	Enable signal. When EN=1, this macro is activated.
CLK	In	1	System clock. All registers are synchronized with the rising edge of this signal.
BSY	Out	1	Busy status flag. This signal is assigned to 1 during encryption, decryption, or key generation process is executed. When this signal is 1, signals Drdy and Krdy are ignored.
Kvld	Out	1	When round-key generation process is completed, this signal becomes 1 during the next one clock cycle, and then it goes 0. Soon after that, encryption and decryption processes are ready to start.
Dvld	Out	1	When encryption or decryption process is completed and cipher text or plain text are ready on the data output port Dout, this signal becomes 1 during the next one clock cycle, and then it goes 0.

3. Hardware Architecture

The hardware architecture of the DES macro is shown in Fig. 1.

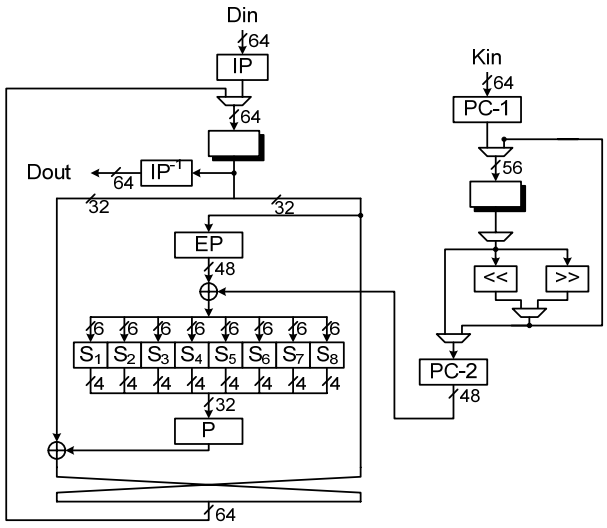

Fig.1 Hardware architecture of the DES macro

4. Timing Chart

Fig. 2 shows the timing chart of the encryption process of the DES macro in the minimum cycles for the control signals. The operations are performed as follows.

CLK1: The sequencer logic is initialized by resetting the signal RSTn to 0.
CLK2: By asserting Krdy=1, the 64-bit secret key on the port Kin is stored to an internal register. The flag Kvld is set to 1.
CLK3: The signal Drdy is set to 1, and the 64-bit plaintext is stored into an internal register.
CLK4: The encryption process is started in accordance with EncDec=0, and BSY is set to 1.
CLK5~18: The encryption takes 16 clocks, and thus it is completed in CLK19. The ciphertext is output from the 64-bit port Dout. The flag BSY goes 0, and Dvld goes to 1.

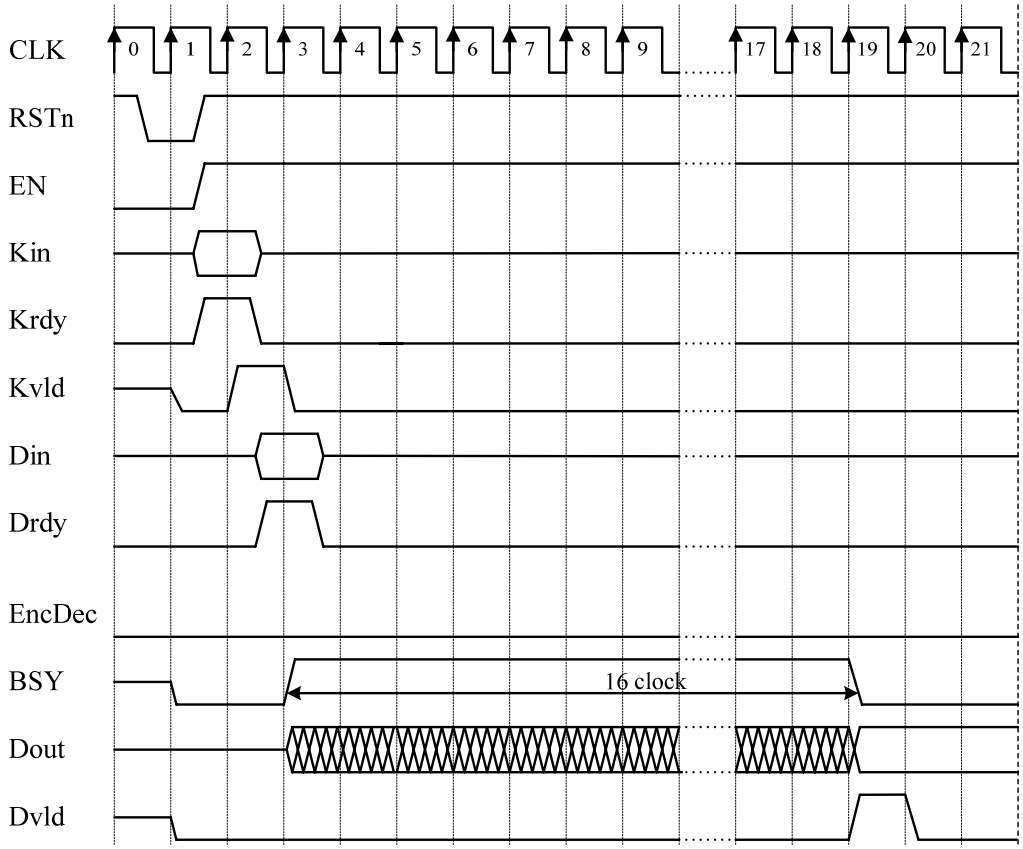

Fig. 2 Timing Chart

5. Reference

[1] “FIPS PUB 46-3 DATA ENCRYPTION STANDARD (DES),” NIST, Oct 1999.