AES Hardware Macro Specification

Version	Update	Description
0.1	2007/09/04	Initial version is created
0.2	2007/09/25	Decryption part is added

1. Overview

The features of this AES hardware macro were summarized in Table 1. Detailed algorithm designed based on the FIPS 197 [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 AES hardware macro overview

Algorithm	AES
Data block size	128 bits
Key size	128 bits
Mode of operation	Electronic Code Book (ECB)
Source file name	AES2.v
Description language	Verilog-HDL
Top module name	AES
Throughput	128 bit / 10 clock
Round keys	Pre-calculation and On-the-fly

2. I/O ports

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

Table 2 I/O ports

Port name	Direction	Width	Description
Kin	In	128	Key input
Din	In	128	Data input
Dout	Out	128	Data output
Krdy	In	1	When Krdy=1, a secret key is latched in 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

			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

This hardware macro consists of two data processing modules, which are encryption and decryption modules. The hardware architectures of the modules are shown in Fig.1 and Fig.2, respectively. In this hardware macro, an S-box is defined as an 8-bit input/output look-up table. The Verilog-HDL code AES.v also contains other type of S-box implementations where a composite field inverter [2] and the three-stage Reed-Muler logic [3] are used. A user can simply replace the S-box block in the source code.

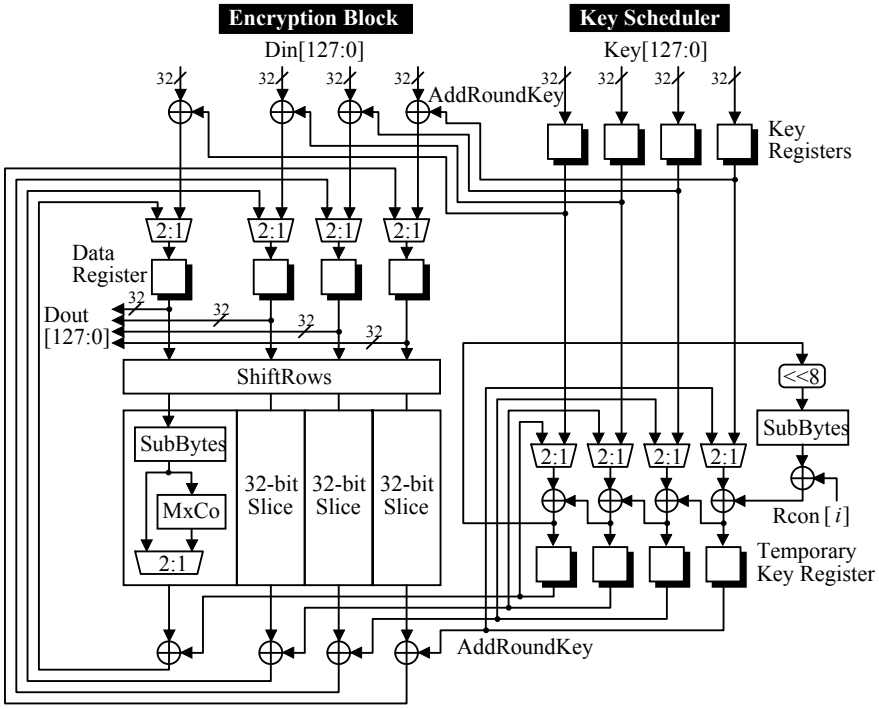

Fig.1 Hardware architecture of the AES encryption module.

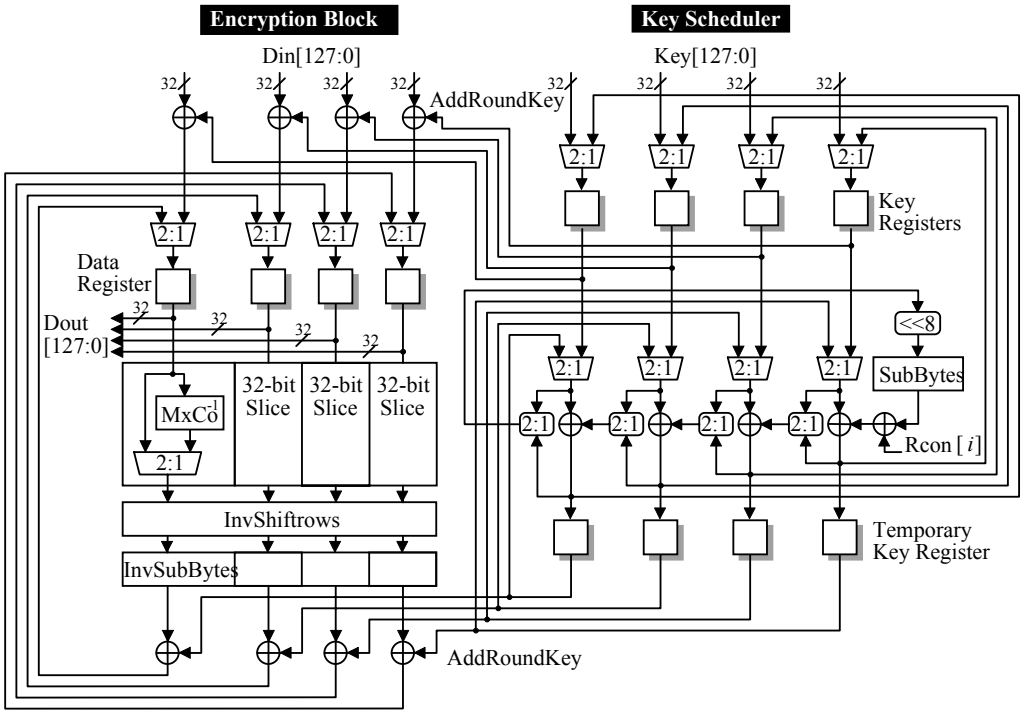

Fig.2 Hardware architecture of the AES decryption module.

4. Timing Chart

Fig. 3 shows the timing chart of the encryption process of the AES 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 128-bit secret key on the port Kin is stored to an internal register.
CLK3: The signal Drdy is set to 1, and the 128-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.
CLK5~12: The encryption takes 10 clocks, and thus it is completed in CLK13. The ciphertext is output from the 128-bit port Dout. The flag BSY goes to 0, and Dvld goes to 1.

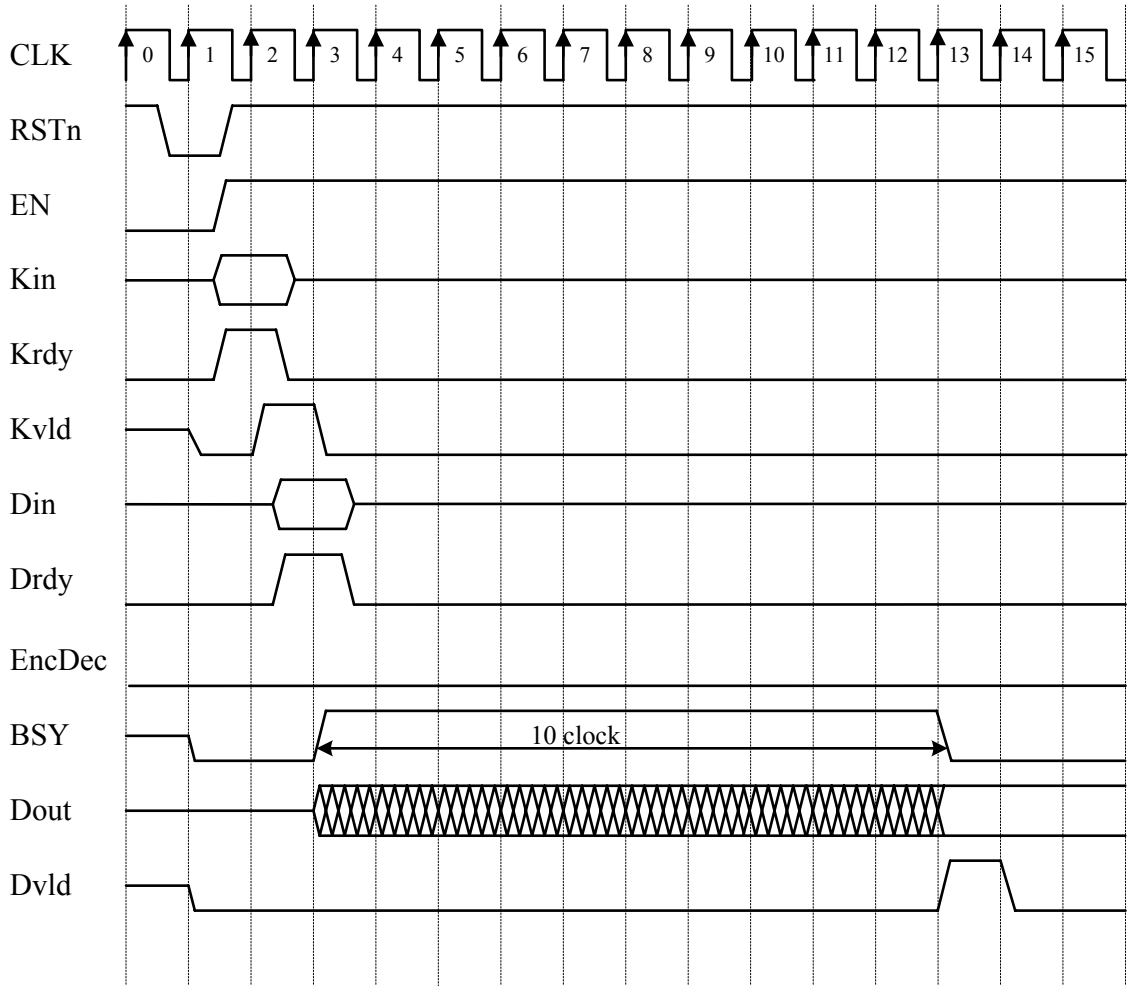

Fig. 3 Timing Chart of the encryption process.

Fig. 4 shows the timing chart of the decryption process of the AES 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 128-bit secret key on the port Kin is stored to an internal register.
CLK3: Key scheduling is started in accordance with EncDec=1, and the flag BSY goes to 1.

CLK14: Key scheduling is finished. The flag Krdy is set to 0, Kvld goes to 1, and BSY goes to 0. The signal Drdy is set to 1, and the 128-bit ciphertext on the port Din is stored into an internal register.

CLK15: The decryption process is started in accordance with EncDec=1, and BSY is set to 1.

CLK16~23: The encryption takes 10 clocks, and thus it is completed in CLK24. The plaintext is output from the 128-bit port Dout. The flag BSY goes to 0, and Dvld goes to 1.

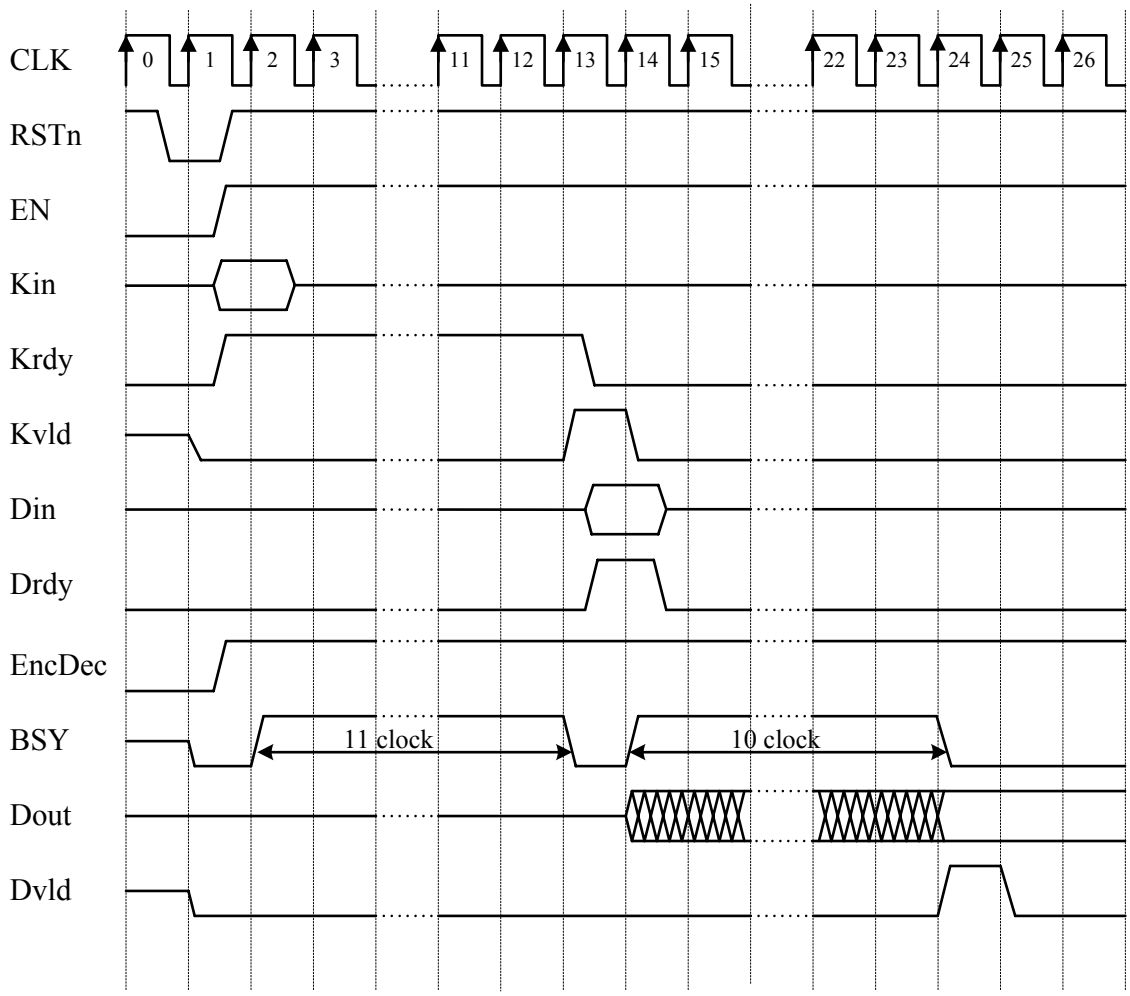

Fig. 4 Timing Chart of the decryption process.

5. Reference

[1] National Institute of Standards and Technology, "FIPS PUB 197: ADVANCED ENCRYPTION STANDARD (AES)," Nov. 2001.

[2] Satoh, A., Morioka, S. Takano, K. and Munetoh, S., "A Compact Rijndael Hardware Architecture with S-Box Optimization," *Advances in Cryptography - ASIACRYPT 2001*, LNCS 2248, pp.239-254, Dec. 2001.

[3] Morioka, S. and Satoh, A., "An Optimized S-Box Circuit Architecture for Low Power AES Design," *in Proc. CHES 2002*, LNCS 2523, pp.271-295, 2003.