# SEED Hardware Macro Specification

| Version | Update | Description |
|---|---|---|
| 0.1 | 2007/09/05 | Initial version is created |
| 0.1.1 | 2007/09/21 | Timing chart (Fig. 4) is fixed |
| 0.2 | 2007/09/25 | Translated |
| | | |
| | | |

## 1. Overview

### 1.1 Hardware macro overview

The features of this SEED hardware macro are summarized in Table 1. The detailed algorithm is described in the specification [1]. 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** CAST-128 hardware macro overview

| | |
|---|---|
| **Algorithm** | SEED |
| **Data block size** | 128 bits |
| **Key size** | 128 bits |
| **Mode of operation** | Electronic Code Book (ECB) |
| | SEED_1clk.v |
| **Description Language** | Verilog-HDL |
| **Top module name** | SEED |
| **Throughput** | 128 bit / 16 clock |
| **Round keys** | On-the-fly |

### 1.2 Algorithm overview

The overview of SEED algorithm is shown in Fig. 1. SEED is a Feistel-type block cipher developed by KISA (Korea Information Security Agency) [1], and it only supports a 128-bit key. For the SEED round function, a triplet of a 32-bit G function, a 32-bit XOR, and a 32-bit addition (or subtraction) is executed three times. The G functions consist of 4 S-boxes and a linear permutation. Round keys “K1”-“K16” are generated from the secret key “Key,” which is transformed by addition, subtraction, and G function.

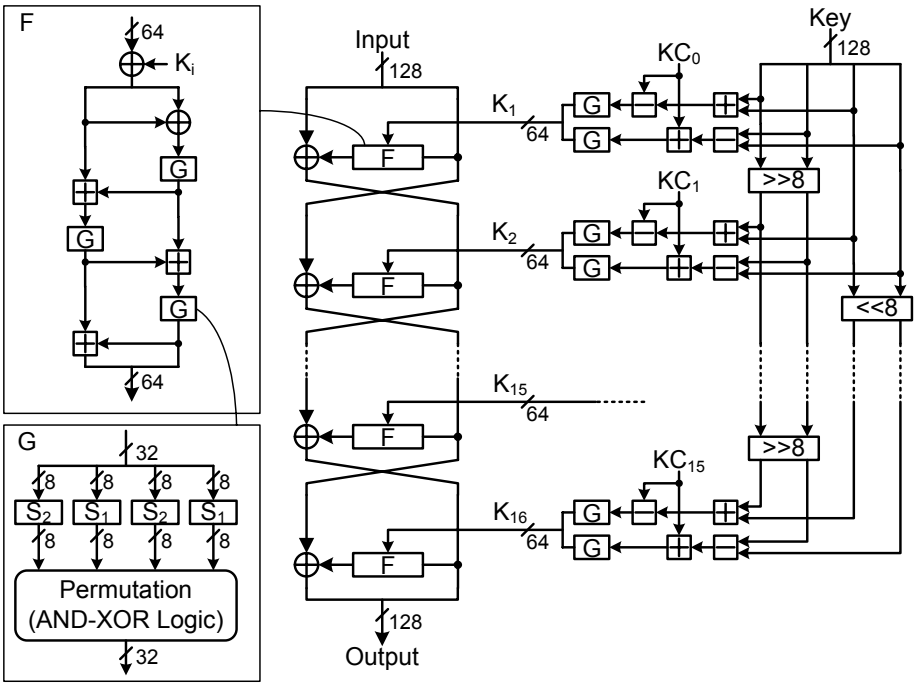


**Fig. 1** SEED algorithm

## 2. I/O ports

I/O ports of the SEED 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 an internal register. If both Drdy and Krdy are assigned to '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 the encryption (or decryption) process is started. |
| EncDec | In | 1 | Encryption and decryption are executed when EncDec=0 and EncDec=1, respectively. An input data should be kept while the encryption/decryption process is running. |
| RSTn | In | 1 | Reset signal. Sequencer logic and internal registers are reset when this signal is assigned to 0. The 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 while an encryption, decryption, or key generation process is executed. When this signal is 1, both 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

## 3.1 Datapath

A datapath of the SEED macro is shown in Fig. 2. This macro executes 1-round operation in 1 clock cycle. A 128-bit block of data is encrypted / decrypted in 16 clocks.

The datapath consist of key-scheduling part and data randomization part. A 128-bit secret key contained in an internal register key_reg through a port Kin. Round keys are generated from the value in key_reg on the fly. A 128-bit input data (plaintext for encryption, ciphertext for decryption) is set to an internal register data_reg through a port Din. A 128-bit output data (ciphertext for encryption, plaintext for decryption) is obtained from a port Dout.

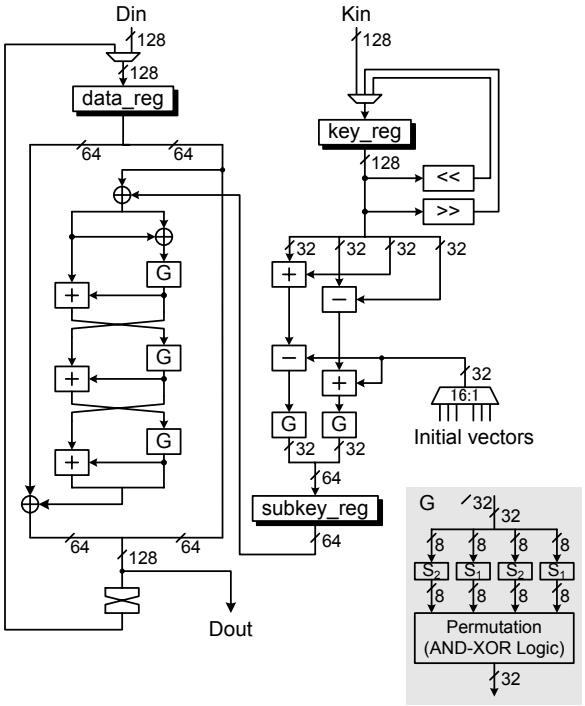


**Fig. 2** Datapath

## 3.2 State Diagram

The state diagram of the SEED sequencer and its description are shown in Fig. 3 and Table 4, respectively.

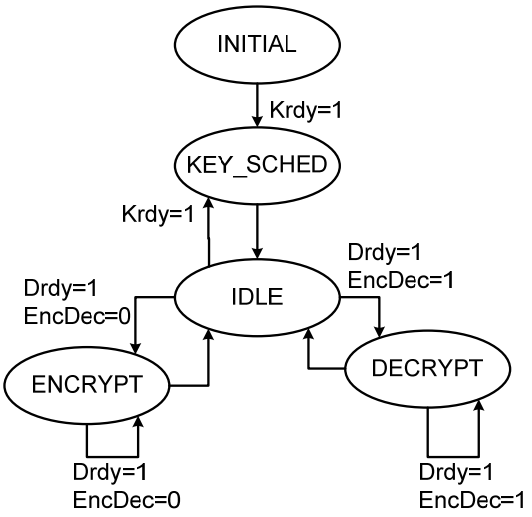


**Fig. 3** State diagram of sequencer

**Table 4** Sequencer States

| State | Description |
|---|---|
| INITIAL | Initial state |
| KEY_SCHED | Key scheduling for round key generation is executed. |
| ENCRYPT | Encryption is performed |
| DECRYPT | Decryption is performed |
| IDLE | Idle state with invalid data on the port Dout. |

# 4. Timing Chart

Fig. 4 shows the timing chart of the key scheduling, encryption, and decryption process for the SEED macro in the minimum cycles for the control signals. The operations are performed as follows.

**CLK1:** The sequencer logic is initialized by resetting RSTn to 0. The sequencer state is set to "INITIAL."

**CLK2:** By asserting Krdy=1, a 128-bit secret key on Kin is stored to an internal register for encryption in accordance with EncDec=0. Note that the key scheduling process should be executed whenever the value of EncDec is changed. BSY is set to 1 for one clock. The sequencer state is set to "KEY_SCHED".

**CLK3:** The key scheduling takes 1 clock, and thus BSY and Kvld are set to 0 and 1, respectively. The sequencer state goes to "IDLE." At the same time, by the signal Drdy is set to 1 and the 64-bit input data (plaintext) is stored into an internal register on the rising edge.

**CLK4:** The encryption process is started in accordance with EncDec=0, and BSY is set to 1. The

sequencer state is set to “ENCRYPT.”

**CLK5-20**: The encryption takes 16 clocks, and thus it is completed in CLK20. The output data (cipherext) is output from the 128-bit port Dout and the flag Dvld is set to 1 only in the 16th clock of the encryption process (i.e., CLK19). The sequencer is set to “IDLE,” and the flag BSY goes to 0 in CLK20.

**CLK21:** By asserting Krdy=1, the 128-bit secret key on the port Kin is stored to an internal register for decryption in accordance with EncDec=1. BSY is set to 1 for one clock. The sequencer state is set to “KEY_SCHED”.

**CLK22:** The key scheduling finishes. The flags BSY and Kvld are set to 0 and 1, respectively. The sequencer state goes “IDLE.” At the same time, by The signal Drdy is set to 1, and the 64-bit input data (plaintext) is stored into an internal register.

**CLK23:** By asserting Drdy=1, the next operation is started. The 64-bit input data (ciphertext) is stored into an internal registers. The decryption process is started in accordance with EncDec=1, and BSY is set to 1. The sequencer state is set to “DECRYPT.”

**CLK24~39:** The decryption also takes 16 clocks. and thus it is completed in CLK39. The output data (plaintext) is output from Dout and Dvld is set to 1 only in the 16th clock of the decryption process (i.e., CLK38). The sequencer is set to “IDLE,” and BSY goes to 0 in CLK39.

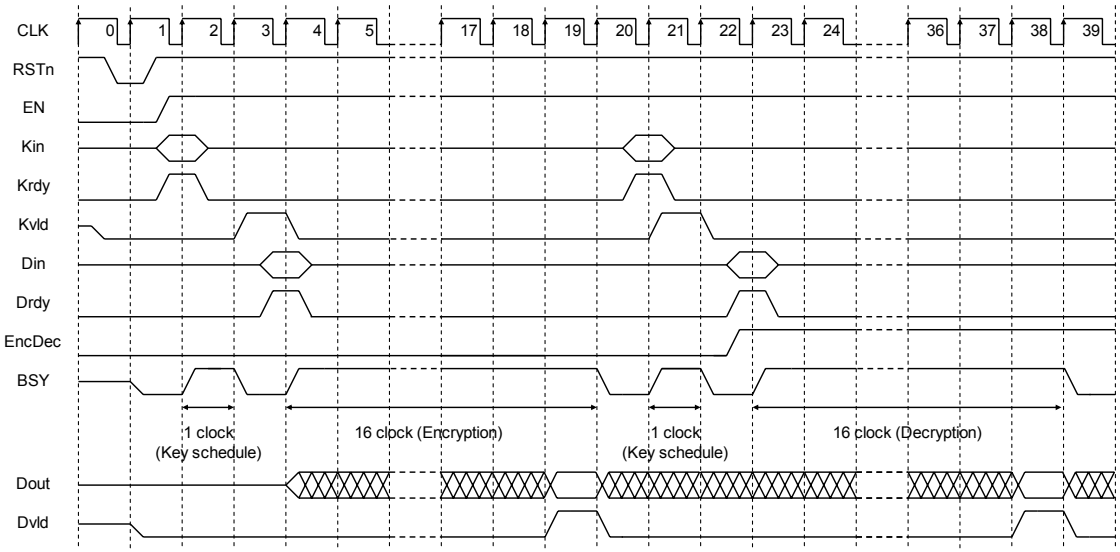


**Fig. 4** Timing Chart

# 5. Reference

[1] SEED Algorithm Specification,
http://www.kisa.or.kr/seed/data/Document_pdf/SEED_Specification_english.pdf