MISTY1 Hardware Macro Specification

Version	Update	Description
0.1	2007/09/16	Initial version is created
0.1.1	2007/09/21	Timing chart (Fig. 6) is fixed
0.2	2007/09/25	Translated

1. Overview

1.1. Hardware macro overview

The features of this MISTY1 hardware macro are summarized in Table 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	MISTY1
Data block size	64 bits
Key size	128 bits
Mode of operation	Electronic Code Book (ECB)
Source file name	MISTY1_1clk.v
Description Language	Verilog-HDL
Top module name	MISTY1
Throughput	128 bit / 9 clock
Round keys	On-the-fly
Round number	8

1.2 Algorithm overview

MISTY1 is a Feistel-type 64-bit block cipher with a 128-bit key. The detailed algorithm is described in the specification [1]. In the following, we describe the 8-round version which is recommended in the specification.

Fig. 1 shows data randomization block. MISTY1 employs FL/FL^{-1} functions in the every 2 rounds of Feistel Network. The internal functions *FO* and *FIij* have nested structures based on Feistel Network.

Before an encryption/decryption process, intermediate keys *K'1~K'8* are generated from secret keys *K1~K8* in key-scheduling block. Fig. 2 shows the intermediate-key generation. Round keys *KOi*, *KIi*, and *KLi* are selected from *K1~K8* and *K'1~K'8* according to Table 2.

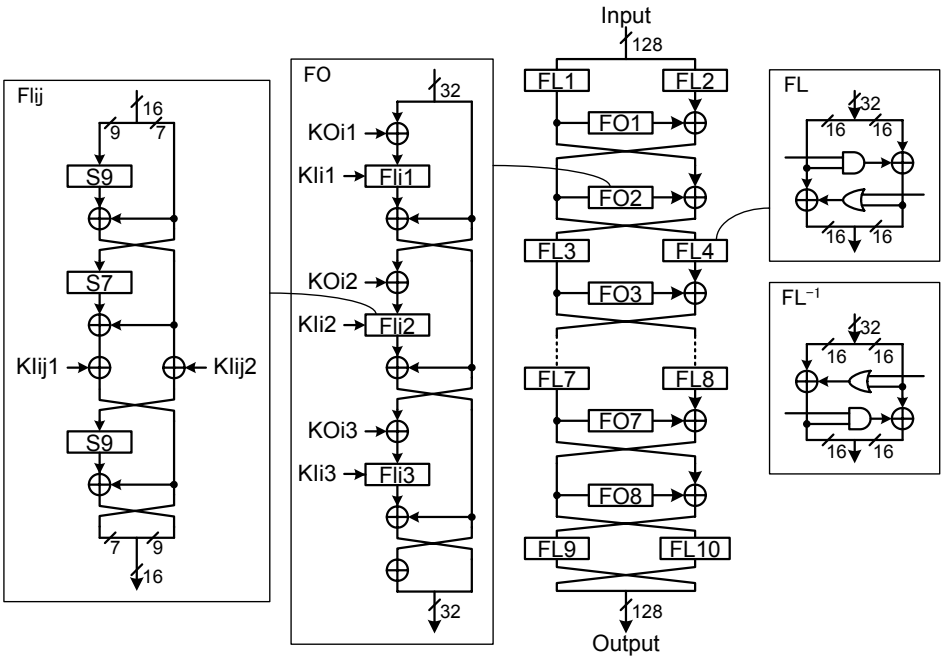

Fig. 1 MISTY1 encryption algorithm

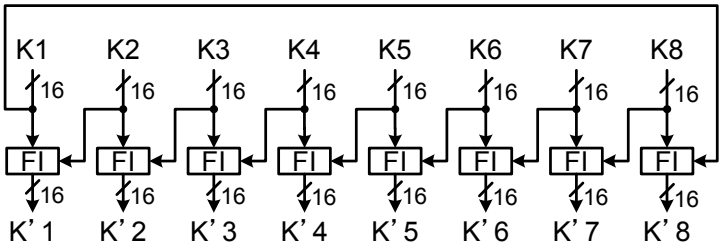

Fig. 2 Intermediate key generation

Table 2 MISTY1 round keys

	KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	KL_{i1}	KL_{i2}
Key	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	$K_{(i+1)/2}$ (odd i) $K'_{i/2+1}$ (even i)	$K'_{(i+13)/2}$ (odd i) $K_{i/2+4}$ (even i)

2. I/O ports

I/O ports of the MISTY1 macro are summarized in Table 3.

Table 3 I/O ports

Port name	Direction	Width	Description
Kin	In	128	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 the initial key generation process get started. If both 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 the encryption (or decryption) process is started.
EncDec	In	1	Encryption and decryption are executed when EncDec=0 and EncDec=1, respectively. The input data should be kept while 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

3.4 Datapath

A datapath of the MISTY1 macro is shown in Fig. 3. This macro executes 1-round operation in 1 clock cycle. A 128-bit block of data is encrypted / decrypted in 9 clocks. The datapath consists of key-scheduling block and data randomization block.

A secret key is set to an internal register K through a 128-bit port Kin in key-scheduling block. Soon after that, the intermediate key generation is started in the data randomization block. The obtained intermediate key is contained in an internal register K' after 8 clocks. Round keys are selected from the K and K' in the encryption / decryption process.

An input data (plaintext for encryption, ciphertext for decryption) is set to an internal register data_reg through a 64-bit port Din in the data randomization block. Six operations are shown in Fig. 4. One of them are selected and executed in one clock cycle. An output data (ciphertext for encryption, plaintext for decryption) is obtained from a 64-bit port Dout.

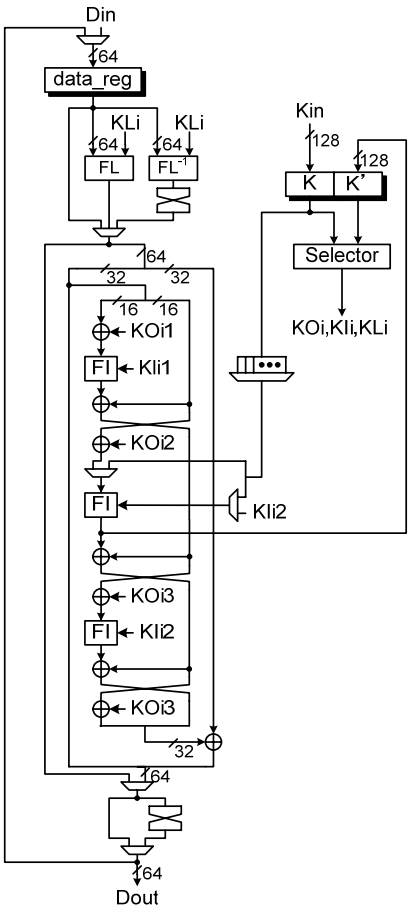

Fig. 3 Datapath

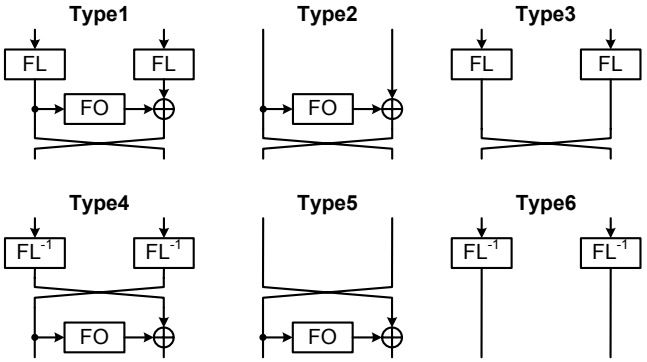

Fig. 4 Operation types in the data randomization process

3.2 State Diagram

The state diagram of the CAST-128 sequencer and its description are shown in Fig. 5 and Table 4, respectively. Note that the sequencer state is set to ”IDLE” when the reset signal is asserted.

Table 4 Sequencer States

State	Description
KEY_SCHED	Key scheduling for round key generation is executed.
ENCRYPT	Encryption is performed
DECRYPT	Decryption is performed
IDLE	Idle state

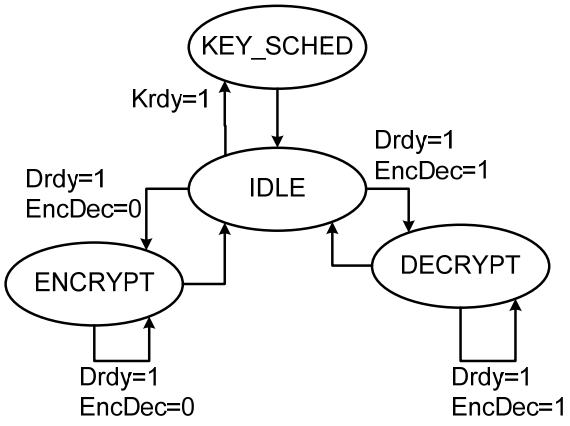

Fig. 5 State diagram of sequencer logic

4. Timing Chart

Fig. 6 shows the timing chart of the key scheduling, encryption, and decryption process for the MISTY1 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 goes to "IDLE"

CLK2: By asserting Krdy=1, the 128-bit secret key on Kin is stored to an internal register. Soon after that, the key scheduling process is started, and BSY is set to 1. The sequencer state is set to "KEY_SCHED."

CLK3~10: The key scheduling takes 8 clocks, and thus Kvld and BSY are set to 1 and 0 in CLK10, respectively. The sequencer state goes to "IDLE".

CLK10: Drdy is set to 1, and the 64-bit input data (plaintext) is stored into an internal register at the rising edge in CLK11.

CLK11: The encryption process is started in accordance with EncDec=0, and BSY is set to 1. The sequencer state is set to "ENCRYPT."

CLK12~20: The encryption takes 9 clocks, and thus it is completed in CLK20. The output data (ciphertext) is output from Dout and Dvld is set to 1 only in the 9th clock of the process (i.e., CLK19). The sequencer is set to "IDLE," and BSY goes 0 in CLK20.

CLK21: By asserting Drdy=1, the next operation is started. The 64-bit input data (ciphertext) is stored into an internal register. The decryption process is started in accordance with EncDec=1, and BSY is set to 1. The sequencer state is set to "DECRYPT."

CLK22~30: The decryption also takes 9 clocks. and thus it is completed in CLK30. The output data (plaintext) is output from Dout and Dvld is set to 1 only in the final clock of the process (CLK29). The sequencer is set to "IDLE," and BSY goes 0 in CLK30.

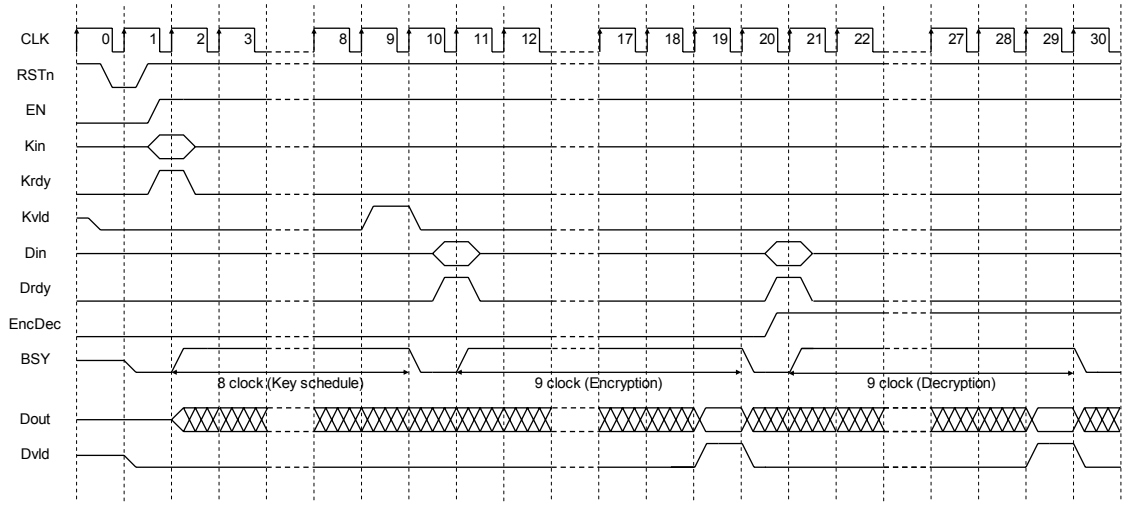

Fig. 6 Timing Chart

5. Reference

[1] M. Matsui, "Specification of MISTY1 – a 64-bit Block Cipher," NESSIE Project.
https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions.html