ISO/IEC 18033-3 Standard Cryptographic LSI Specification

- Version 1.0 -

April 1, 200

Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology

Index

1. OVERVIEW

The ISO/IEC Standard Cryptographic LSI for Side-channel Attack Evaluation (Cryptographic LSI) is an LSI in which RSA and block ciphers on “Part3:Block ciphers” in ISO/IEC 18033 (Information technology- Security techniques - Encryption algorithms) are implemented for Side-channel attack evaluation. The cryptographic LSI uses an 0.13 μm CMOS process of TSMC and an 160-pin QFP ceramic package.

There are seven ciphers, AES, DES, MISTY1, Camellia, SEED, CAST and RSA. AES is implemented with seven artitectures. Consequently, there are thirteen cryptographic circuits on the LSI. Two versions of the LSI are built for Japan and countries other than Japan. The key lengths of the cipher circuits are limited on LSIs for countries other than Japan to 56-bit for block ciphers and 512-bit for RSA because of export control. The rest of the bits are fixed.

The details of the ciphers are as follows:

- AES (128-bit key)
  1. Composite field based S-Box, Encryption/Decryption support.
  2. Composite field based S-Box, Encryption support.
  3. Direct mapping S-Box with case syntax, Encryption support.
  4. Positive Polarity Reed-Muller (PPRM, 1-stage) based S-Box, Encryption support.
  5. 3-stage PPRM based S-Box, Encryption support.
  6. Composite field based S-Box, Random Switching Logic (RSL) for Side-channel countermeasure, Encryption/Decryption support.
  7. Composite field based S-Box, Back annotated netlist, Encryption/Decryption support.
- DES, Encryption/Decryption support.
- MISTY1, Encryption/Decryption support.
- Camellia (128-bit key), Encryption/Decryption support.
- SEED, Encryption/Decryption support.
- CAST128, Encryption/Decryption support.
- RSA, 1024-bit power modular multiplier.

The main features of the cryptographic LSI are as follows:

- Supports encryption and decryption.
- Generates trigger signals for measurement through side-channels.
- Outputs intermediate processing data using the AES circuit (1) for fault injection attack evaluation.

2 EXTERNAL SPECIFICATIONS

2.1 I/O Assignments

A functional description of the input and output signals are shown in Table 1. The pin assignments for the LSI are shown in Table 2 and Figure 1. The signals in parentheses "( )" in Table 2 denote signals reserved for future versions and are not used. Power supply pins are divided into I/O cell and core in order to measure power consumption and electromagnetic wave with high precision.

Table 1: Input/output signals

Function (#pin)	Signal Name	#Pin		Direction	Description
System (11)	CLKA	1	--	IN	Clock source.
	CLKB	1	--	IN	(Not connected)
	HRST_N	1	L	IN	Asynchronous reset input.
	LEDO[1:0]	2	L	OUT	(Not connected)
	SWIN[3:0]	4	--	IN	(Not connected)
	PHIN[1:0]	2	--	IN	(Not connected)
Bus Control (4)	WR_N	1	L	IN	Assert write data.
	RD_N	1	L	IN	Assert read data.
	RSV0	1	--	IN	(Not connected)
	RSV1	1	--	IN	(Not connected)
Bus Address (16)	A[15:0]	16	--	IN	Address.
Bus Data (32)	DI[15:0]	16	--	IN	Input data.
	DO[15:0]	16	--	OUT	Output data.
Debug (13)	START_N	1	L	OUT	Indicate start of cipher.
	END_N	1	L	OUT	Indicate end of cipher.
	(TRIG0)	1	--	OUT	(Not connected)
	(TRIG1)	1	--	OUT	(Not connected)
	EXEC	1	H	OUT	Indicate processing cipher.
	STATE[3:0]	4	--	OUT	Indicate selected cryptographic circuit.
	MON[3:0]	4	--	OUT	Debugging information.
Summary		76			

Table 2: Pin assignment (1/4)

Pin NO	Signal Name	I/O	I/F Voltage	output	I/O Buffer	Function
1	PVSS1DGZ					core GND
2	PVSS1DGZ					core GND
3	PVSS2DGZ					I/O GND
4	(SWIN[3])					N.C
5	(SWIN[2])					N.C
6	(SWIN[1])					N.C
7	(SWIN[0])					N.C
8	PVDD2POC					I/O 3.3V
9	(PHIN[1])					N.C
10	(PHIN[0])					N.C
11	N.C					N.C
12	N.C					N.C
13	PVSS2DGZ					I/O GND
14	N.C					N.C
15	N.C					N.C
16	N.C					N.C
17	N.C					N.C
18	N.C					N.C
19	PVDD2DGZ					I/O 3.3V
20	PVDD1DGZ					core 1.2V
21	PVSS1DGZ					core GND
22	PVSS2DGZ					I/O GND
23	N.C					N.C
24	N.C					N.C
25	N.C					N.C
26	(RSV1)					N.C
27	(RSV0)					N.C
28	PVSS2DGZ					I/O GND
29	A[15]	I	3.3V		PDIDGZ	Address
30	A[14]	I	3.3V		PDIDGZ	Address
31	A[13]	I	3.3V		PDIDGZ	Address
32	A[12]	I	3.3V		PDIDGZ	Address
33	PVDD2DGZ					I/O 3.3V
34	A[11]	I	3.3V		PDIDGZ	Address
35	A[10]	I	3.3V		PDIDGZ	Address
36	A[9]	I	3.3V		PDIDGZ	Address
37	A[8]	I	3.3V		PDIDGZ	Address
38	PVSS2DGZ					I/O GND
39	PVSS1DGZ					core GND
40	PVSS1DGZ					core GND

Table 2: Pin assignment (2/4)

Pin NO	Signal Name	I/O	I/F Volatage	output	I/O Buffer	Function
41	PVDD1DGZ					core 1.2V
42	PVDD2DGZ					I/O 3.3V
43	A[7]	I	3.3V		PDIDGZ	Address
44	A[6]	I	3.3V		PDIDGZ	Address
45	A[5]	I	3.3V		PDIDGZ	Address
46	A[4]	I	3.3V		PDIDGZ	Address
47	PVSS2DGZ					I/O GND
48	PVDD1DGZ					core 1.2V
49	A[3]	I	3.3V		PDIDGZ	Address
50	A[2]	I	3.3V		PDIDGZ	Address
51	A[1]	I	3.3V		PDIDGZ	Address
52	A[0]	I	3.3V		PDIDGZ	Address
53	PVDD2DGZ					I/O 3.3V
54	PVSS1DGZ					core GND
55	PVSS2DGZ					I/O GND
56	(CLKB)					N.C
57	PVSS2DGZ					I/O GND
58	CLKA	I	3.3V		PDISDGZ	Clock
59	PVSS2DGZ					I/O GND
60	PVDD1DGZ					core 1.2V
61	PVSS1DGZ					core GND
62	PVSS2DGZ					I/O GND
63	HRST_N	I	3.3V		PDISDGZ	Reset
64	PVSS2DGZ					I/O GND
65	WR_N	I	3.3V		PDIDGZ	Write assert
66	RD_N	I	3.3V		PDIDGZ	Read assert
67	PVDD2DGZ					I/O 3.3V
68	PVSS1DGZ					core GND
69	DO[15]	O	3.3V	8mA	PDO08CDG	Output data
70	DO[14]	O	3.3V	8mA	PDO08CDG	Output data
71	DO[13]	O	3.3V	8mA	PDO08CDG	Output data
72	DO[12]	O	3.3V	8mA	PDO08CDG	Output data
73	PVSS2DGZ					I/O GND
74	PVDD1DGZ					core 1.2V
75	DO[11]	O	3.3V	8mA	PDO08CDG	Output data
76	DO[10]	O	3.3V	8mA	PDO08CDG	Output data
77	DO[9]	O	3.3V	8mA	PDO08CDG	Output data
78	DO[8]	O	3.3V	8mA	PDO08CDG	Output data
79	PVDD2DGZ					I/O 3.3V
80	PVDD1DGZ					core 1.2V

Table 2: Pin assignment (3/4)

Pin NO	Signal Name	I/O	I/F Volatage	output	I/O Buffer	Function
81	PVSS1DGZ					core GND
82	PVSS1DGZ					core GND
83	PVSS2DGZ					I/O GND
84	DO[7]	O	3.3V	8mA	PDO08CDG	Output data
85	DO[6]	O	3.3V	8mA	PDO08CDG	Output data
86	DO[5]	O	3.3V	8mA	PDO08CDG	Output data
87	DO[4]	O	3.3V	8mA	PDO08CDG	Output data
88	PVDD2DGZ					I/O 3.3V
89	DO[3]	O	3.3V	8mA	PDO08CDG	Output data
90	DO[2]	O	3.3V	8mA	PDO08CDG	Output data
91	DO[1]	O	3.3V	8mA	PDO08CDG	Output data
92	DO[0]	O	3.3V	8mA	PDO08CDG	Output data
93	PVSS2DGZ					I/O GND
94	N.C					N.C
95	N.C					N.C
96	N.C					N.C
97	N.C					N.C
98	N.C					N.C
99	PVDD2DGZ					I/O 3.3V
100	PVDD1DGZ					core 1.2V
101	PVSS1DGZ					core GND
102	PVSS2DGZ					I/O GND
103	N.C					N.C
104	N.C					N.C
105	N.C					N.C
106	N.C					N.C
107	N.C					N.C
108	PVSS2DGZ					I/O GND
109	DI[0]	I	3.3V		PDIDGZ	Input data
110	DI[1]	I	3.3V		PDIDGZ	Input data
111	DI[2]	I	3.3V		PDIDGZ	Input data
112	DI[3]	I	3.3V		PDIDGZ	Input data
113	PVDD2DGZ					I/O 3.3V
114	DI[4]	I	3.3V		PDIDGZ	Input data
115	DI[5]	I	3.3V		PDIDGZ	Input data
116	DI[6]	I	3.3V		PDIDGZ	Input data
117	DI[7]	I	3.3V		PDIDGZ	Input data
118	PVSS2DGZ					I/O GND
119	PVSS1DGZ					core GND
120	PVSS1DGZ					core GND

Table 2: Pin assignment (4/4)

Pin NO	Signal Name	I/O	I/F Voltage	output	I/O Buffer	Function
121	PVDD1DGZ					core 1.2V
122	PVDD2DGZ					I/O 3.3V
123	DI[8]	I	3.3V		PDIDGZ	Input data
124	DI[9]	I	3.3V		PDIDGZ	Input data
125	DI[10]	I	3.3V		PDIDGZ	Input data
126	DI[11]	I	3.3V		PDIDGZ	Input data
127	PVSS2DGZ					I/O GND
128	PVDD1DGZ					core 1.2V
129	DI[12]	I	3.3V		PDIDGZ	Input data
130	DI[13]	I	3.3V		PDIDGZ	Input data
131	DI[14]	I	3.3V		PDIDGZ	Input data
132	DI[15]	I	3.3V		PDIDGZ	Input data
133	PVDD2DGZ					I/O 3.3V
134	PVSS1DGZ					core GND
135	(LED[0])					N.C
136	(LED[1])					N.C
137	END_N	O	3.3V	8mA	PDO08CDG	End of cipher
138	START_N	O	3.3V	8mA	PDO08CDG	Start of cipher
139	PVSS2DGZ					I/O GND
140	PVDD1DGZ					core 1.2V
141	PVSS1DGZ					core GND
142	PVSS2DGZ					I/O GND
143	STATE[0]	O	3.3V	8mA	PDO08CDG	Selected cipher
144	STATE[1]	O	3.3V	8mA	PDO08CDG	Selected cipher
145	STATE[2]	O	3.3V	8mA	PDO08CDG	Selected cipher
146	STATE[3]	O	3.3V	8mA	PDO08CDG	Selected cipher
147	PVDD2DGZ					I/O 3.3V
148	PVSS1DGZ					core GND
149	(MON[0])					N.C
150	(MON[1])					N.C
151	(MON[2])					N.C
152	(MON[3])					N.C
153	PVSS2DGZ					I/O GND
154	PVDD1DGZ					core 1.2V
155	EXEC	O	3.3V	8mA	PDO08CDG	Processing cipher
156	N.C					N.C
157	N.C					N.C
158	N.C					N.C
159	PVDD2DGZ					I/O 3.3V
160	PVDD1DGZ					core 1.2V

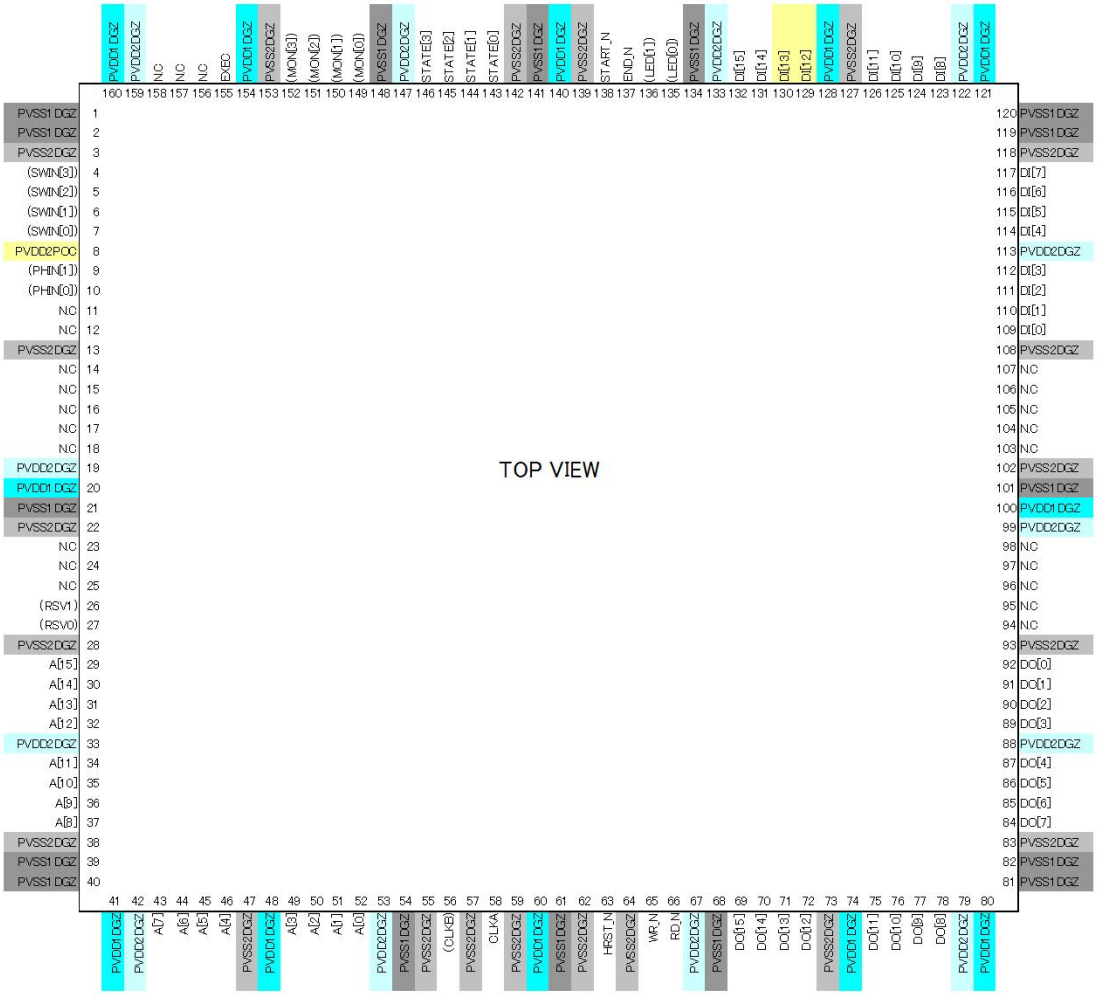


Figure 1: Pin assignment

2.2 Control Interface

Internal register is used to control the cryptographic circuits on the LSI. Table 3 lists the registers. The register is read and written through bus interface. Figure 2, 3, and 4 indicate timing diagram of the bus interface. Details of the register are described in section 3.2.

The cryptographic circuit is controlled with following procedure:

1 Select cryptographic circuit. Set bits on IPSEL register corresponding to the circuits.
2 Reset the circuit. Set IPRST register to assert reset signal. And then unset register to deassert.
3 Select circuit that outputs cryptographic result. Set bit on OUTSEL register corresponding to the circuit.
4 Select encryption/decryption on MODE resister.
(Optional: Select round on witch intermediate processing data is recoded with AES_COMP circuit through RSEL register.)
5 Set criptographic key.
5.1 Set cryptographic key to KEY0~7 registers in the case of block ciphers. Set index number and divisor to EXP00~3F and MOD00~3F registers in the case of RSA, respectively.
5.2 Start key preparation setting KSET bit of CONT register, and then, wait until the bit is cleared.

6 Start cipher.

6.1 Set input text to ITEXT0~7 registers in the case of 128-bit block ciphers, and to ITEXT0~3 in the case of 64-bit block ciphers. Set the input data to IDATA00~3F resisiters in the case of RSA.

6.2 Start the cipher by setting the RUN bit of the CONT register, and then wait until the bit is cleared.

6.3 Read the output text from the OTEXT0~7 registers in the case of 128-bit block ciphers, and from OTEXT0~3 registers in the case of 64-bit block ciphers. Read output data from the ODATA00~3F registers in the case of RSA.
(Optional: Read the intermediate processing data output of the AES_COMP circuit from the RDATA0~7 registers.)

Table 3: Internal register (1/2)

Function		Addr.	Name	Abbrev.	R/W	Description
System Contol		0000	(Reserved)		--	
		0002	Control register	CONT	R/W	Start cipher (W)/Indicate end of cipher (R). Start key preperation(W)/Indicate end of key preparation(R).Reset cryptographic circuit(W)
		0004	Select cipher register	IPSEL	R/W	Select cryptographic circuit.
		0006	(Reserved)			
		0008	Output select register	OUTSEL	R/W	Select output of cryptographic circuit.
		000A	(Reserved)			
		000C	Mode register	MODE	R/W	Set cipher mode, key length and encryption /decryption.
		000E	Round select register	RSEL	R/W	Select round of intermediate processing data output.
		0010	Test register 1	TEST1	R/W	(Not used)
		0012	Test register 2	TEST2		(Not used)
		: 00FF	(Reserved)			
Block Ciphers	Key	0100	Cryptographic key 0	KEY0	W	MSB 16 bits of key.
		0102	Cryptographic key 1	KEY1	W	16 bits of key nest to KEY0.
		:	:	:	:	:
		010E	Cryptographic key 7	KEY7	W	LSB 16 bits of Key.
		: 013F	(Reserved)			
	Input Text (to LSI)	0140	Input text0	ITEXT0	W	MSB 16 bits of input text.
		0142	Input text1	ITEXT1	W	16 bits input of text next to ITEXT0.
		:	:	:	:	:
		014E	Input text7	ITEXT7	W	LSB 16 bits of input text.
		: 017F	(Reserved)			
	Output Text (from LSI)	0180	Output text0	OTEXT0	R	MSB 16 bits of output text.
		0182	Output text0	OTEXT1	R	16 bits output of text next to OTEXT0.
		:	:	:	:	:
		018E	Output text0	OTEXT7	R	LSB 16 bits of output text.
		: 01BF	(Reserved)			
	Intermediate Data (from LSI)	01C0	Intermediate data0	RDATA0	R	MSB 16 bits of intermediate data.
		01C2	Intermediate data1	RDATA1	R	16 bits of intermediate data next to ITEXT0.
		:	:	:	:	:
		01CE	Intermediate data7	RDATA7	R	LSB 16 bits of intermediate data.
		: 01FF	(Reserved)			

Table 3: Internal register (2/2)

Function		Addr.	Name	Abbrev.	R/W	Description
Public Key Cryptosystem	Index Number	0200	Index number 0	EXP00	W	MSB 16 bits of intermediate data.
		0202	Index number 1	EXP01	W	16 bits of intermediate data next to EXP0.
		:	:	:	:	:
		027E	Index number 63	EXP3F	W	LSB 16 bits of intermediate data.
		: 02FF	(Reserved)			
	Divisor	0300	Divisor 0	MOD00	W	MSB 16 bits of divisor.
		0302	Divisor 1	MOD01	W	16 bits of divisor next to MOD0.
		:	:	:	:	:
		037E	Divisor 63	MOD3F	W	LSB 16 bits of divisor.
		: 03FF	(Reserved)			
	Input Data (To LSI)	0400	Input data 0	IDATA00	W	MSB 16 bits of input data.
		0402	Input data 1	IDATA01	W	16 bits input of data next to IDATA00.
		:	:	:	:	:
		047E	Input data 63	IDATA3F	W	LSB 16 bits of input data.
		: 04FF	(Reserved)			
	Output Data (From LSI)	0500	Output data 0	ODATA00	R	MSB 16 bits of output data.
		0502	Output data 1	ODATA01	R	16 bits output of data next to ODATA0.
		:	:	:	:	:
		057E	Output data 63	ODATA3F	R	LSB 16 bits of output data.
		: 05FF	(Reserved)			
(Reserved)		: FFEF				
LSI Information (0xFFF0 ～0xFFFF)		FFF0 :	(Reserved)			
		FFFC	Version register	VER	R	
		FFFE	(Reserved)		--	

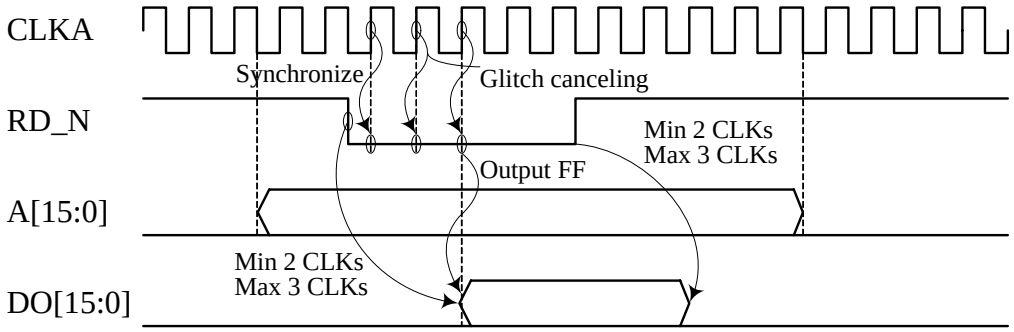


Figure 2: Timing diagram of reading register

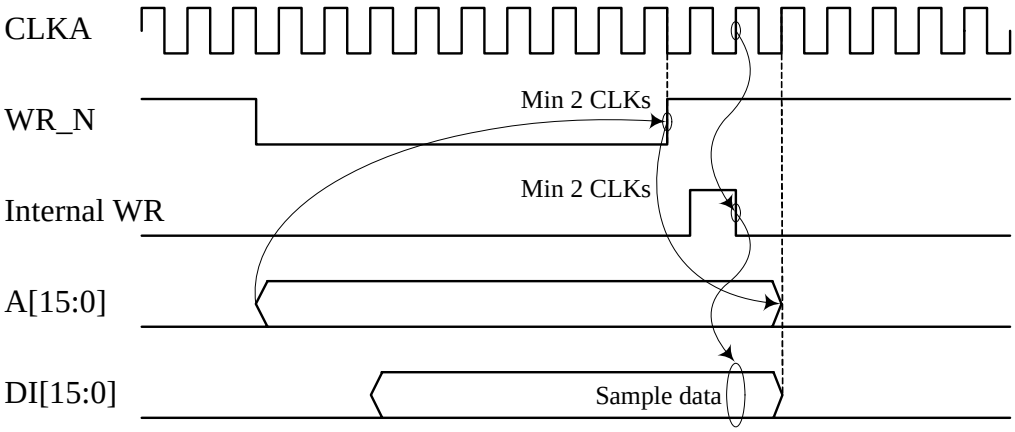


Figure 3: Timing diagram of writing register

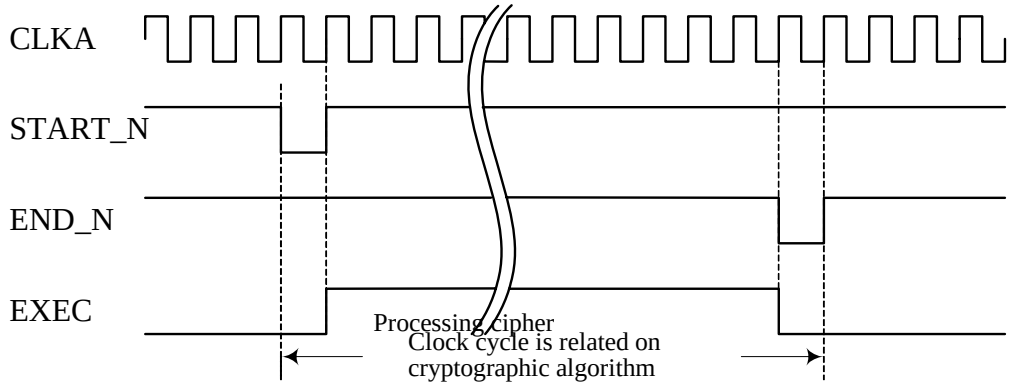


Figure 4: Timing diagram of debug pins

3. INTERNAL SPECIFICATIONS

3.1 LSI Circuitry

The block diagram of the LSI is illustrated in Figure 5. The LSI consists of thirteen cryptographic circuits and interface circuits. Details of the circuits on the LSI are provided on the website of the Computer Structures Laboratory, Graduate School of Information Sciences, Tohoku University (http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.html). The hierarchy of codes used in the circuits is shown in Figure 6.

Table 4: Cryptographic circuits on the LSI

Number	Name	Description
0	AES_Comp	Composite field based S-Box, Encryption/Decryption support with 128-bit key.
1	AES_Comp_ENC_top	Encryption part of AES_Comp.
2	AES_TBL	Direct mapping S-Box with case syntax, Encryption support with 128-bit key.
3	AES_PPRM1	Positive Polarity Reed-Muller (PPRM, 1-stage) based S-Box, Encryption support with 128-bit key.
4	AES_PPRM3	3-stage PPRM based S-Box, Encryption support with 128-bit key.
5	DES	DES, 64-bit key (8-bit parity)
6	MISTY1	MISTY, 64-bit block, 128-bit key. S7 and S9 S-box is designed with case syntax.
7	Camellia	Camellia, 128-bit block. S-box is designed with case syntax.
8	SEED	SEED, 64-bit block, 128-bit key.
9	CAST128	CAST128, 64-bit block, 128-bit key.
10	RSA	RSA, 1024-bit Montgomery power modular multiplier using 32-bit multiplier.
11	AES_SSS1	Composite field based S-Box. Random Switching Logic (RSL) is applied for Side-channel countermeasure. Encryption/Decryption support.
12	AES_S	Composite field based S-Box. Back annotated netlist is used in order to comfirm delay to FPGA implementation. Encryption /Decryption support.

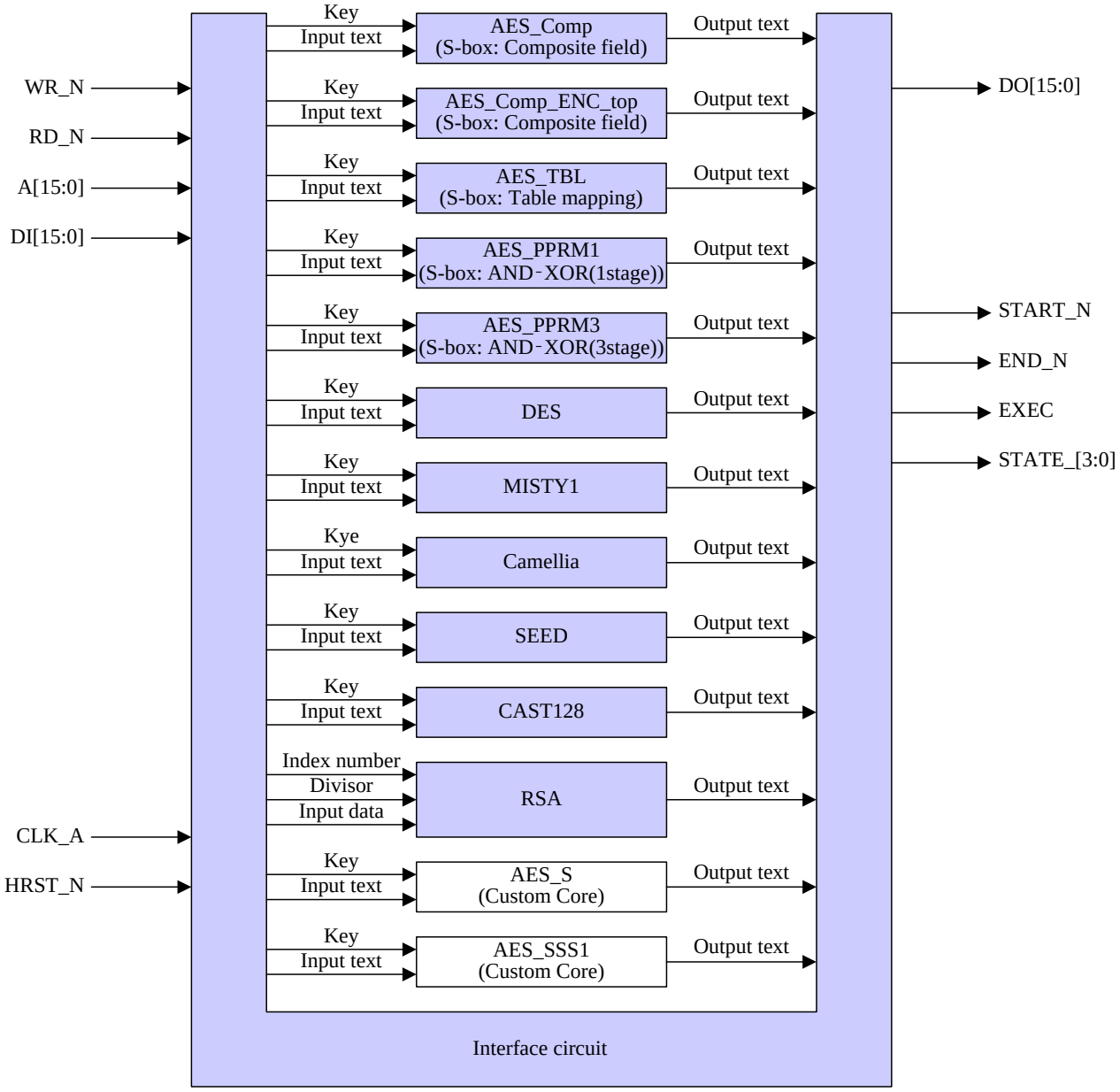


Figure 5: Block diagram of the LSI

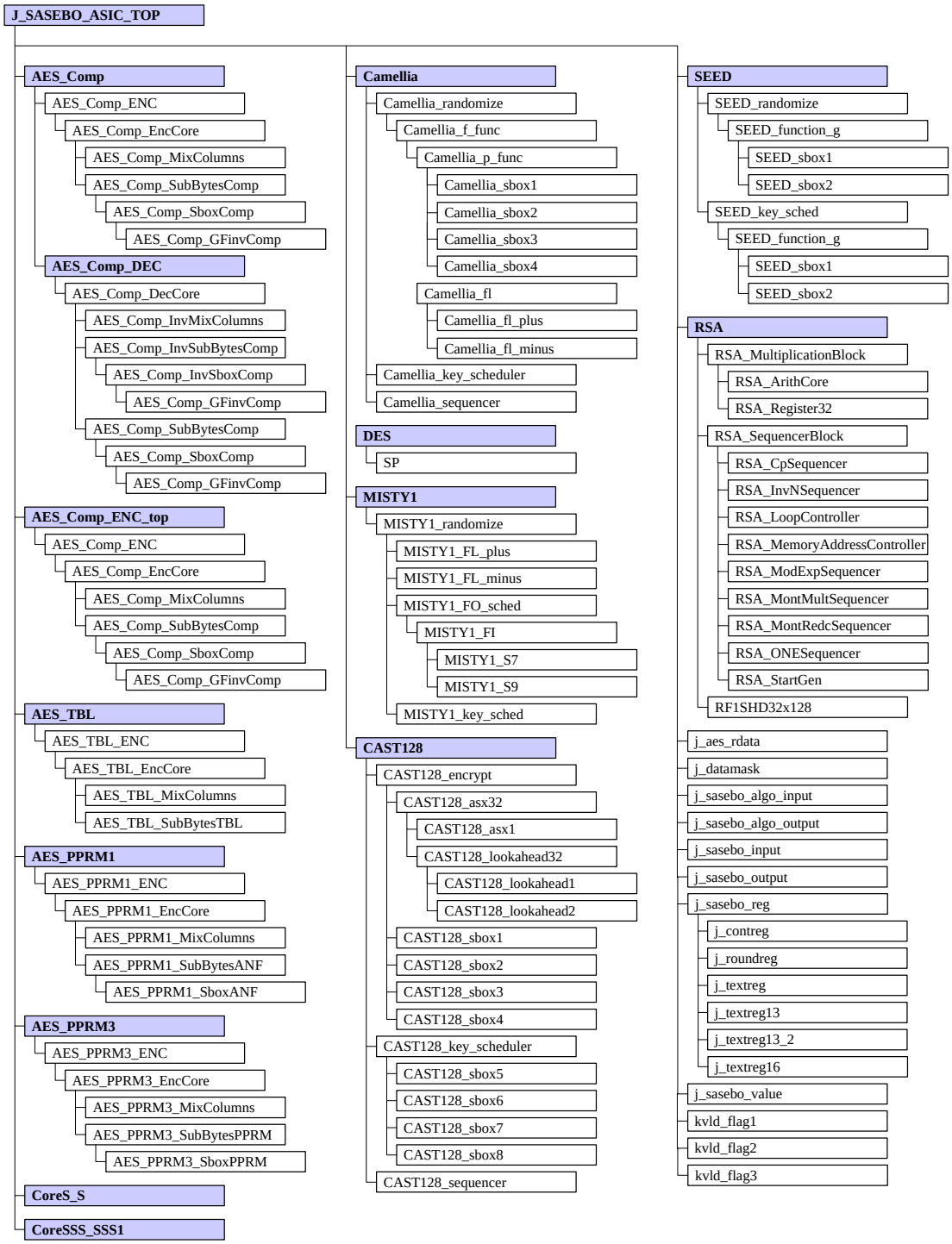


Figure 6: Hierarchy of codes of the ciphers

3.2 Cryptographic Circuit Interface

Block diagrams of the block ciphers interface are illustrated in Figures 7 and 8. Figures 9 and 10 show the RSA interface.

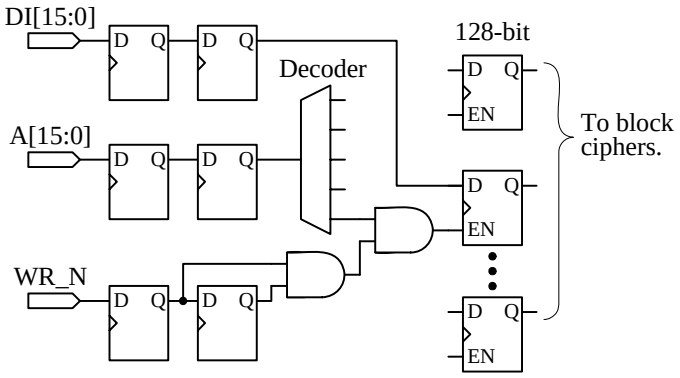


Figure 7: Data input interface of the block ciphers

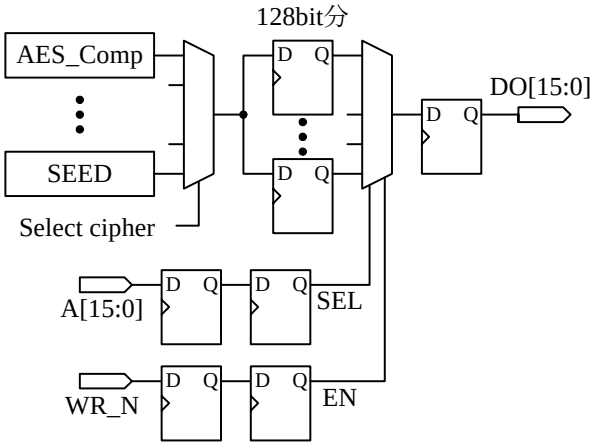


Figure 8: Data output interface of the block ciphers

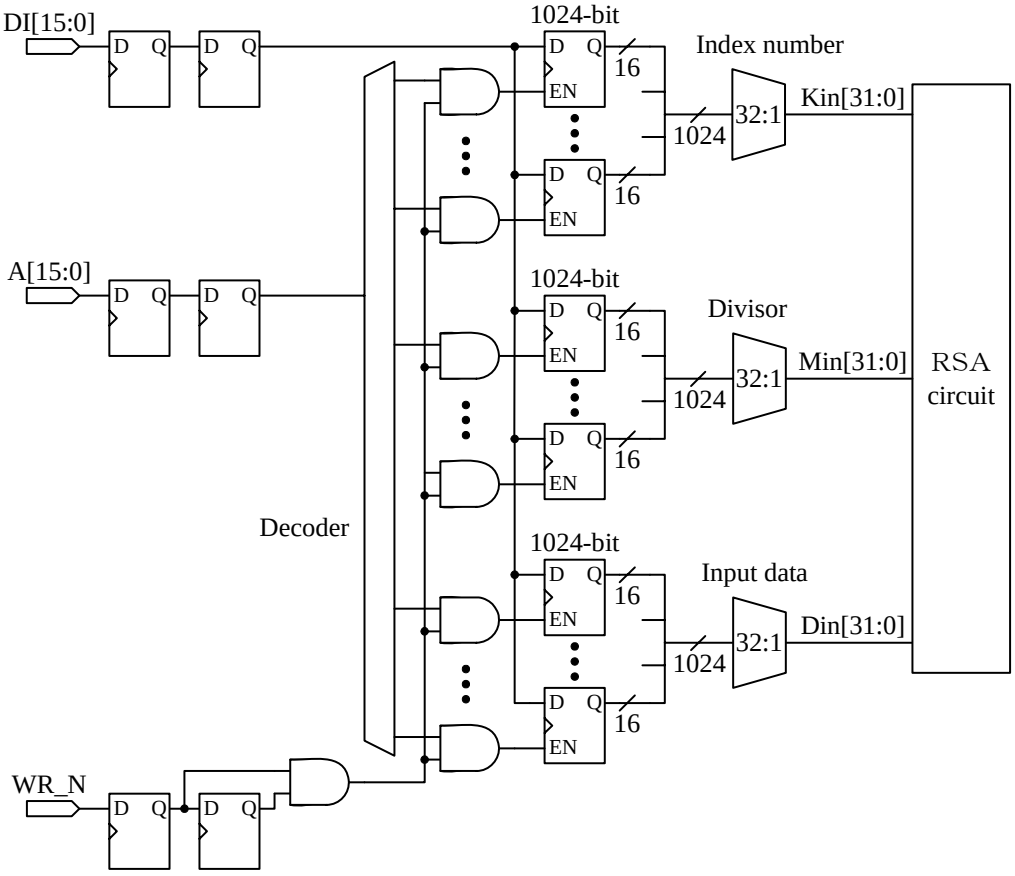


Figure 9: Data input interface of RSA

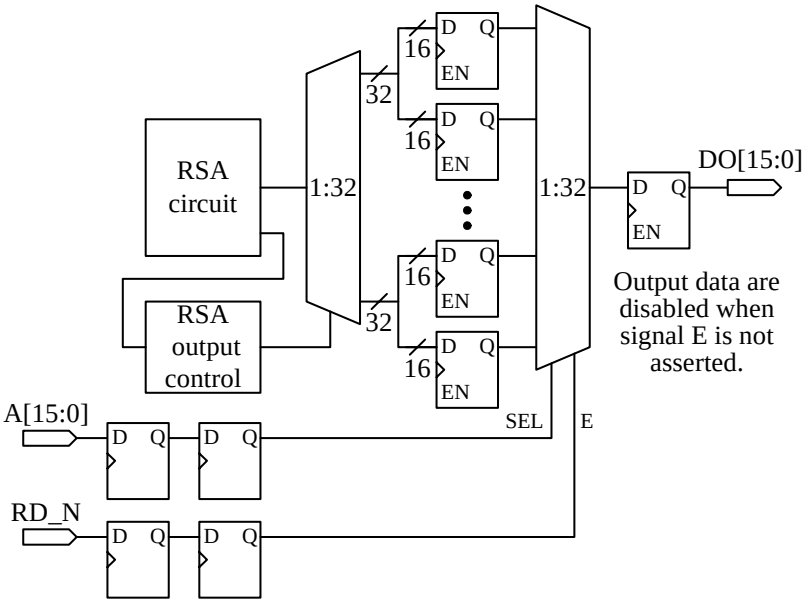
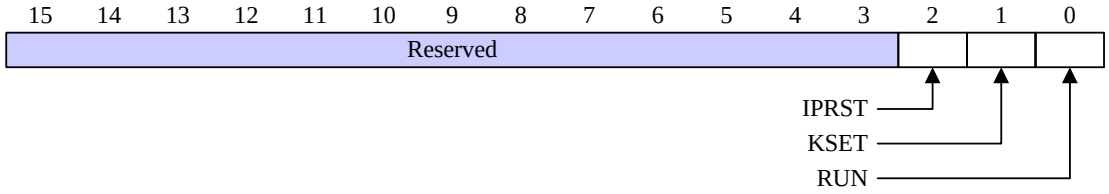


Figure 10: Data output interface of RSA

3.3 Internal register

- **CONT, Control register: 0x0002, R/W**

The CONT register provides control to cryptographic circuits.



Bit 0: RUN

When this bit is set, selected ciphers are started with interval 16-cycle. This bit is cleared automatically when output text or data is ready. All operations to registers are ignored when this bit is set 1.

Bit 1: KSET

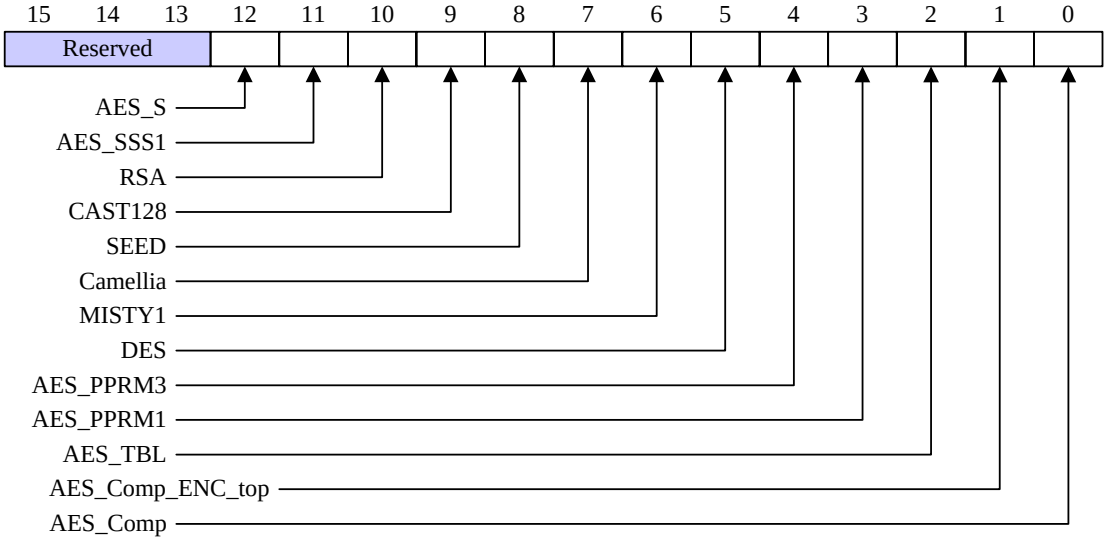
When this bit is set, preparation of the cryptographic key starts. This bit is cleared automatically when the cryptographic key is ready. All operations on registers are ignored when this bit is set. CAUTION: The LSI will become unstable if the RUN bit is set while this bit is set to 1.

Bit 2: IPRST

Assert reset signal to cryptographic circuit selected on the IPSEL register when this bit is set. The reset signal is deasserted when this bit is cleared. The default value of this bit is 1.

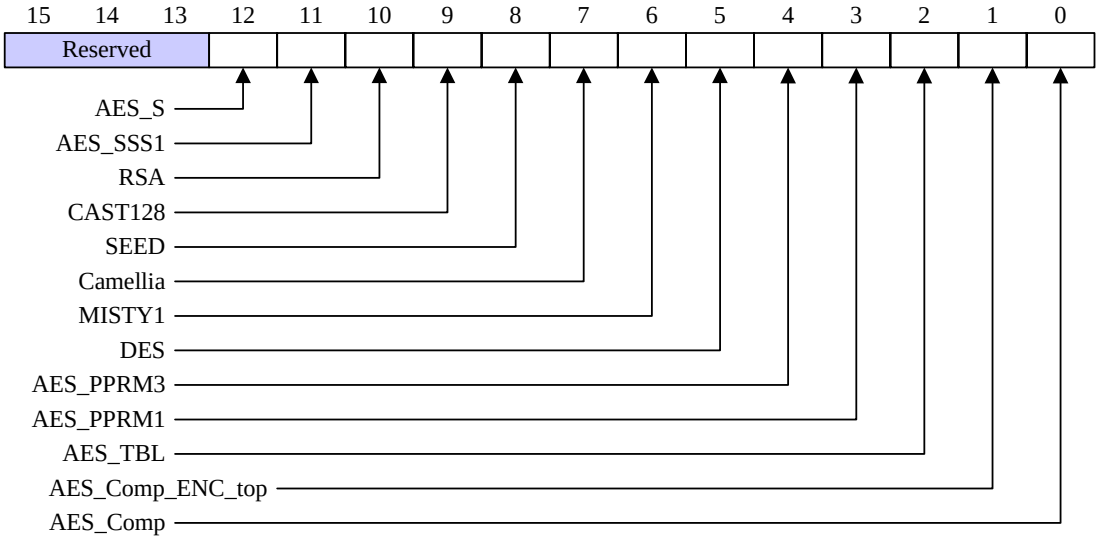
- **IPSEL, Select cipher register: 0x0004, R/W**

The IPSEL register is used to enable cryptographic circuits with operational clock control. The clock is activated according to set bits. In normal use, one bit is set at a time.



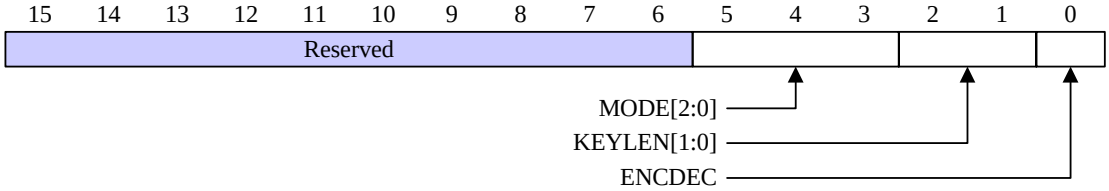
- **OUTSEL, Output select register: 0x0008, R/W**

The OUTSEL register is used to select the cryptographic circuit that will output the results. In normal use, these bits are set in the same way as an IPSEL register. CAUTION: Do NOT set more than one bit of this register.



➢ **MODE, Mode register: 0x000C, R/W**

The MODE register is used to set the operational modes of cryptographic circuits, including cipher modes, key lengths and encryption/decryption.



Bit 5-3: MODE[2:0]

Not used. These bits are fixed at 000. Cipher mode is fixed at ECB (Electoric Code Book).

Bit 2-1: KEYLEN[1:0]

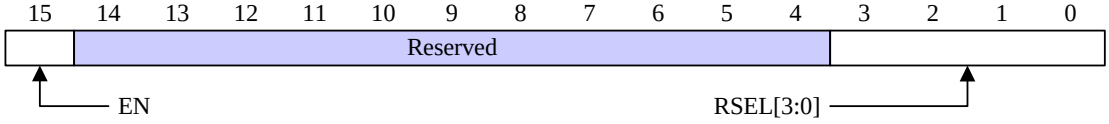
Not used. These bits are fixed at 00. Key length is fixed.

Bit 0: ENCDEC

When this bit is set, cryptographic circuits perform decryption. NOTE: The setting is flipped on DES circuits. The setting is ignored on circuits that do not support decryption.

➢ **RSEL, Round select register: 0x000E, R/W**

The RSEL register is used to set the cryptographic round of AES_Comp in which intermediate processing data is recoded. This register is ignored in the case of other circuits.



Bit 15: EN

When this bit is set, intermediate processing data recording is enabled.

Bit 3-0: RSEL[3:0]

This field specifies the cryptographic round of AES_Comp in which intermediate processing data is recoded into RDATA0~RDATA7.

➢ **TEST1, Test register 1: 0x0010**

➢ **TEST2, Test register 2: 0x0012**

Not used. TEST1 and TEST2 registers are used to debug the LSI.

➢ **KEY0~7, Cryptographic key register: 0x0100~010E, R/W**

The KEY0~7 registers are used to set the 128-bit cryptographic keys of block ciphers. The bit assignment of 128-bit cryptographic keys is illustrated in the following figure.

127 (MSB)							(LSB) 0
KEY0	KEY1	KEY2	KEY3	KEY4	KEY5	KEY6	KEY7

Use KEY4~7 registers to set the 56-bit key for DES. Figure 11 shows the bit assignment of the key.

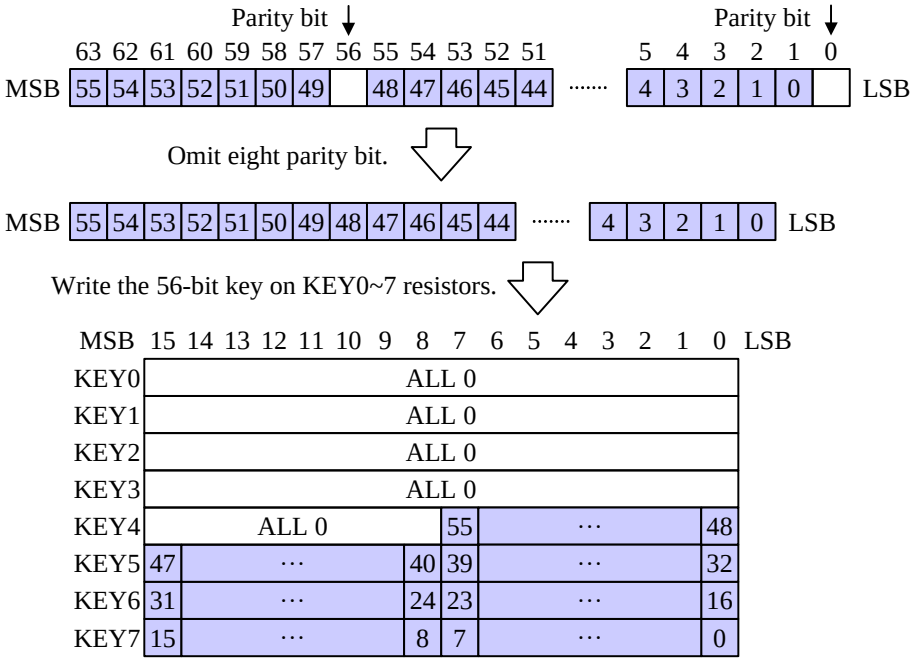


Figure 11: Bit assignment of the DES 56-bit cryptographic key.

➢ **ITEXT0~7, Input text register: 0x0140~014E, R/W**

ITEXT0~7 registers are used to set the input text of block ciphers. The bit assignment of 128-bit text is illustrated in the following figure. Use ITEXT0~ITEXT4 to set 64-bit text.

127 (MSB)							(LSB) 0
ITEXT0	ITEXT1	ITEXT2	ITEXT3	ITEXT4	ITEXT5	ITEXT6	ITEX7

➢ **OTEXT0~7, Output text register: 0x0180~018E, RO**

OTEXT0~7 provide the cryptographic results of block cipers. The bit assignment of 128-bit text is illustrated in the following figure. Read 64-bit text from OTEXT0 to OTEXT4.

➢ **RDATA0~7, Intermediate data register, 0x01C0~01CE, RO**

RDATA0~7 provides the intermediate processing data of AES_Comp. Bit assignment of 128-bit data is illustrated in the following figure.

127 (MSB)							(LSB) 0
RDATA0	RDATA1	RDATA2	RDATA3	RDATA4	RDATA5	RDATA6	RDATA7

- **EXP00~3F, Index number register:, 0x0200~027E, R/W**
- **MOD00~3F, Divisor register: 0x300~037E, R/W**
- **IDATA00~3F, Input data register : 0x0400~047E, R/W**

These registers are used to set index number, divisor and input data of RSA. MSB 16 bits of data are mapped into the registers that have “00” proposition, EXP00, MOD00, and IDATA00.

- **ODATA00~3F, Output data register: 0x0500~057E, RO**

ODATA00~3F provides the cryptographic result of RSA. MSB 16 bits of output data are mapped into ODATA00.

- **VER, Version register: 0xFFFC, RO**

The version register indicates the LSI version.
0x0F5A: Japan
0xC381: Countries other than Japan

3.4 Clock

Figure 12 illustrates the block diagram of the clock control circuitry. Geted clock is supplied to the cryptographic circuits using the clock control circuit. The clock control circuit asserts a clock gating signal according to the IPSEL register. The clock phase is adjusted to the peripheral circuits.

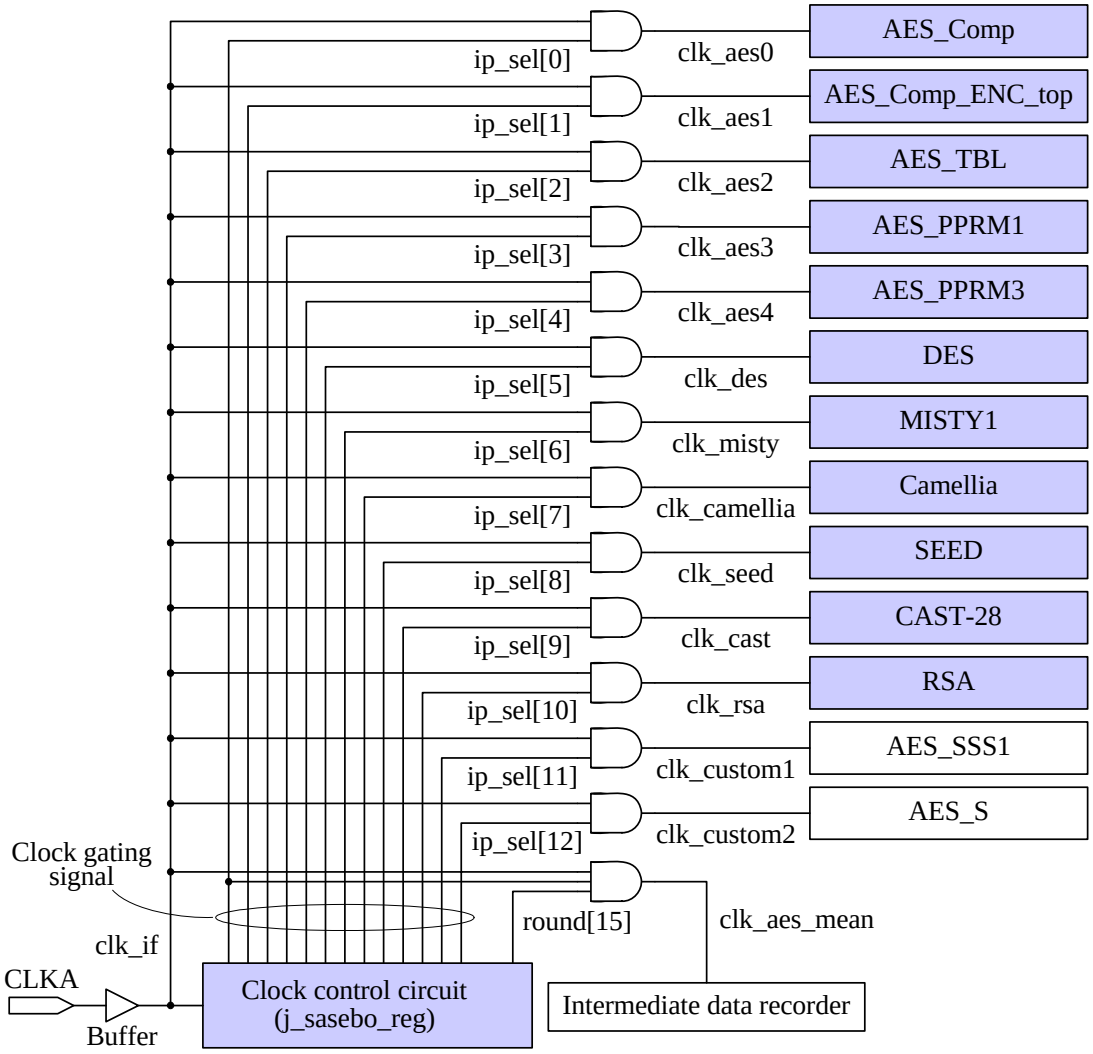


Figure 12: Block diagram of the clock control circuitry

3.5 Reset

The LSI is initialized using the HRST_N signal. Internal reset is deasserted synchronously using the CLK_A clock. After initialization, the LSI interface circuit is activetd. The reset signals of the cryptographic circuits are asserted, and the clock is disabled and enters a quiescent state.

Enable the cryptographic circuit using the following procedure:

1. Select the cryptographic circuits using the IPSEL register.
   The clock is supplied to the selected cryptographic circuits.
2. Deassert the reset signal of the cryptographic circuits.
   The reset signal is deasserted synchronously through the CONT register.

Figure 13 illustrates the block diagram of the reset distribution circuitry.

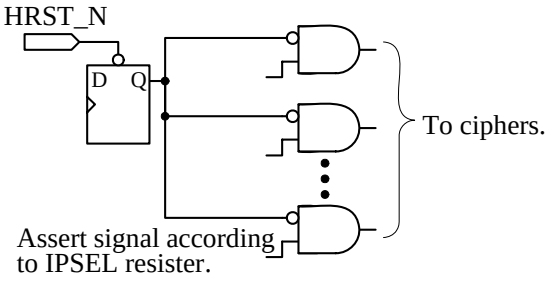


Figure 13: Block diagram of the reset distribution circuitry

3.6 Additional information

- **Key length limitations**

The key length of the non-Japanese LSI version is limited due to export restrictions. The limitations are decribed in Table 5. The lower 56 bits of the key are available for block ciphers with non-Japanese LSI versions. The upper 72 bits are fixed to 0x000102030405060708. AES_SSS1 and AES_S keys are limited in both LSI versions. The lower 512 bits of inputs are available for RSA with the non-Japanese version. The upper 512 bits are fixed at zero.

Table 5: Key length limitations

Cryptographic circuit	Japanese version	Foreign version
DES	56 bits of key are available.	Same as on the left.
AES_Comp/ AES_Comp_ENC_top/ AES_TBL/AES_PPRM1/ AES_PPRM3/MISTY1/ Camellia/SEED/CAST128	128 bits of key are available.	Upper 72 bits of key are fixed (See figure 14). Lower 56 bits are available.
AES_SSS1 AES_S	Upper 72 bits of key are fixed (See figure 14). Lower 56 bits are available.	Same as on the left.
RSA	1024 bits of index number, divisor, and input data are available.	Upper 512 bits of index number, divisor, and input data are fixed to zero. Lower 512 bits are available.

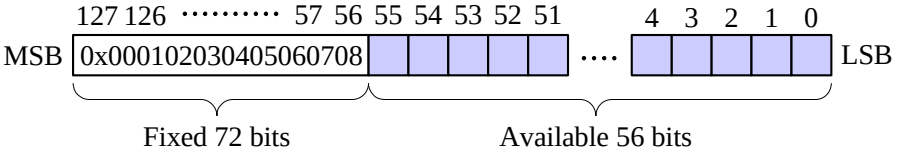


Figure 14: Bit assignment of a limited key

- **Cryptographic circuit processing interval**

The cryptographic circuits start processing after 16 cycles from when the RUN bit of the CONT register is set.

- **Simultaneous processing of cryptographic circuits**

Cryptographic circuits process simultanesously according to IPSEL register: however, one of the circuits output result data according to the OUTSEL register. This operation is used to inject noise into the power consumption.

Technical inquiries:

National Institute of Advanced Industrial Science and Technology (AIST)

Research Center for Information Security (RCIS)

Room 1102 Akihabara-Daibiru, 11F

1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan

TEL: +81-3-5298-4722

FAX: +81-3-5298-4522