VM007

DATA ENCRYPTION PROCESSOR

FEATURES

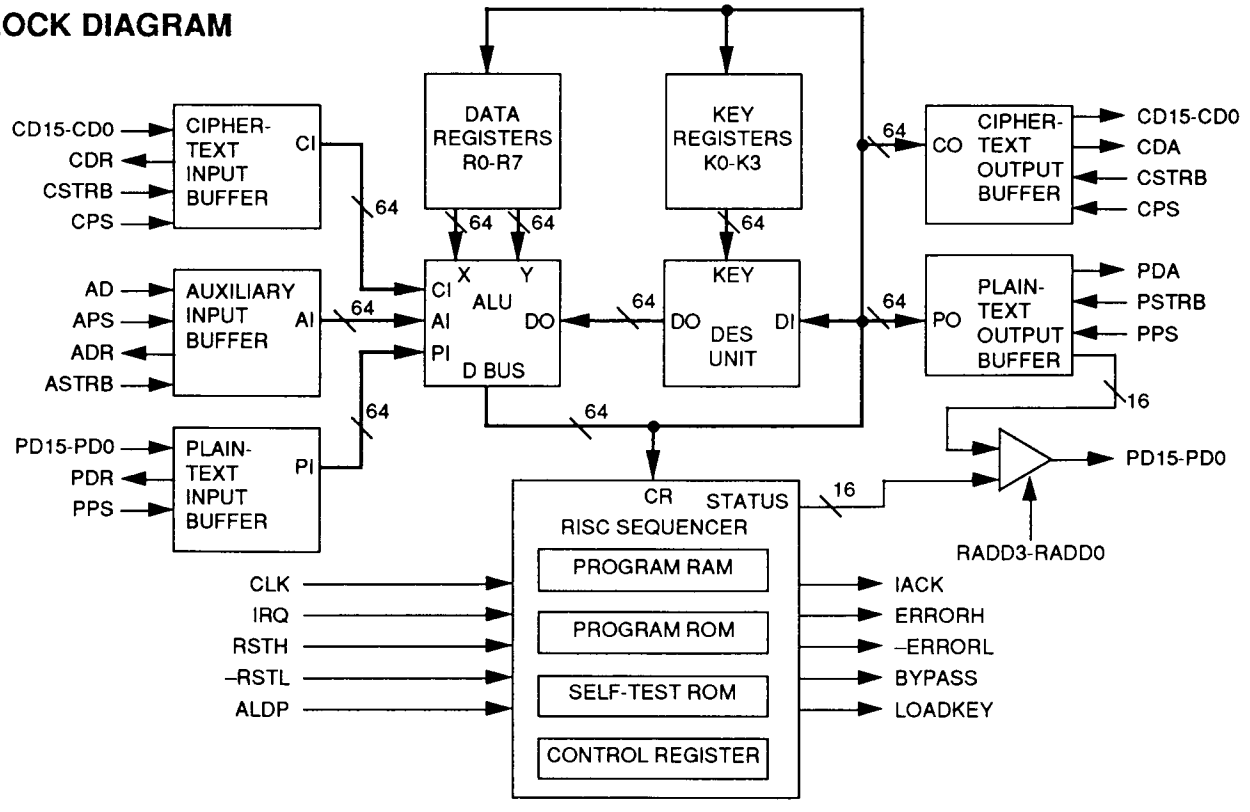
- Complete cryptographic processing system on a single chip
- Supports clock frequencies to 30 MHz
- Capable of encrypting/decrypting 192 Mbits per second using Electronic Codebook (ECB) or Cipher Block Chaining (CBC)
- Supports all DES modes of operation:
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Output Feedback (OFB); 1 to 64-bit
  - Cipher Feedback (CFB); 1 to 64-bit
  - Special A-mode for CFB and OFB
- Four separate and independent interfaces: three data ports and one system interface port
- Class 3 ESD protection (above 4000V)
- Pending validation by National Institute of Standards and Technology (NIST)
- Internal RISC sequencer with on-chip RAM and ROM program memory
- Advanced security features
- Automatic built-in self-test after reset
- 84-lead ceramic or plastic leaded chip carrier (LDCCC, PLCC) packages
- 1.0-micron two layer metal CMOS technology; ensuring highly reliable operation

DESCRIPTION

The VM007 Data Encryption Processor is a programmable integrated circuit that provides a complete cryptographic system on a single chip. It contains a hardware implementation of the Data Encryption Standard (DES), a RISC-based sequencer, data storage registers, and ROM-based microprogram. It is designed to provide very high data and key processing rates, flexible I/O interfacing, and advanced security features.

The VM007 is manufactured using VLSI's 1.0-micron CMOS technology and is available in an 84-lead ceramic or plastic leaded chip carrier. All inputs and outputs are TTL compatible.

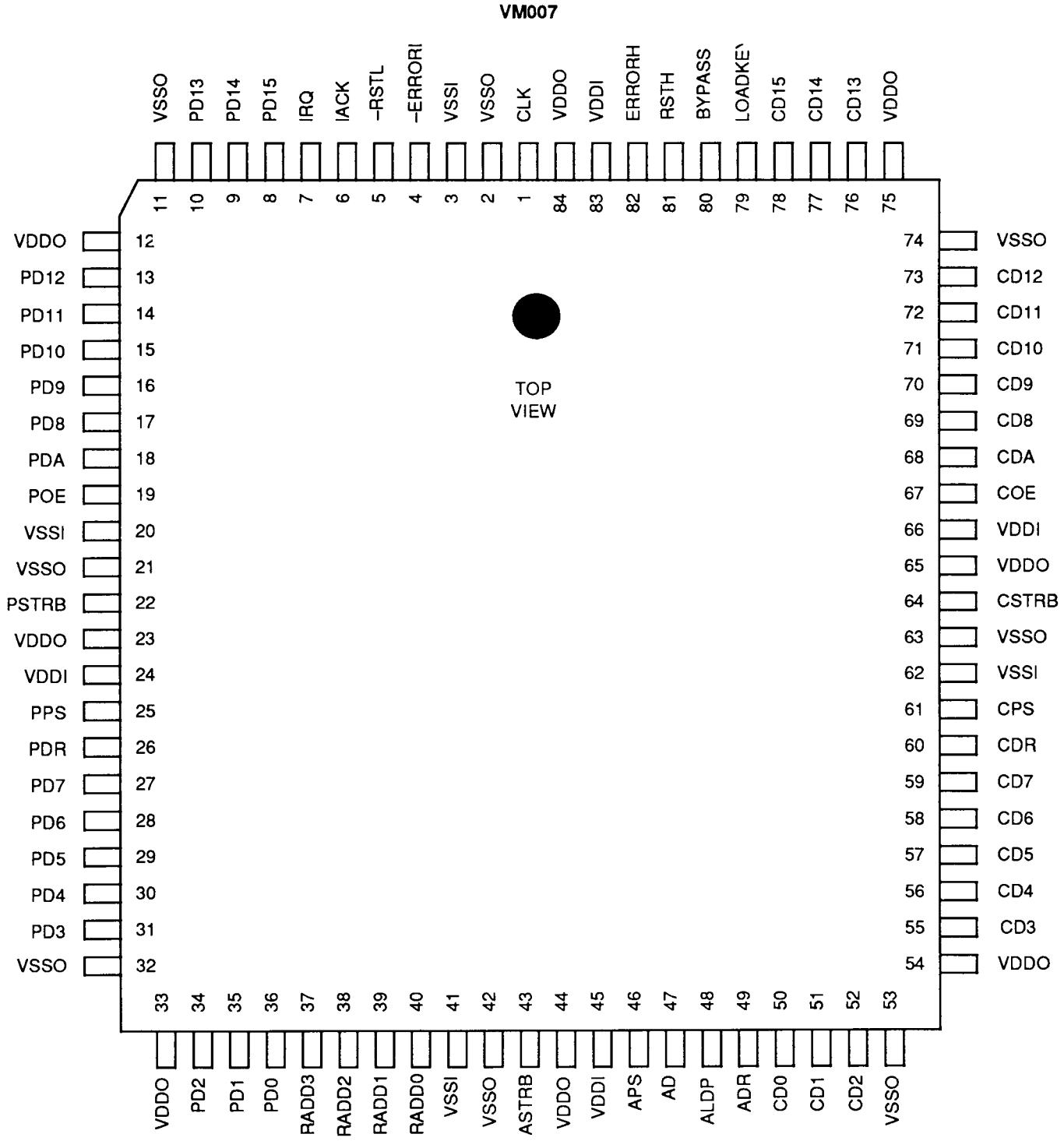
BLOCK DIAGRAM



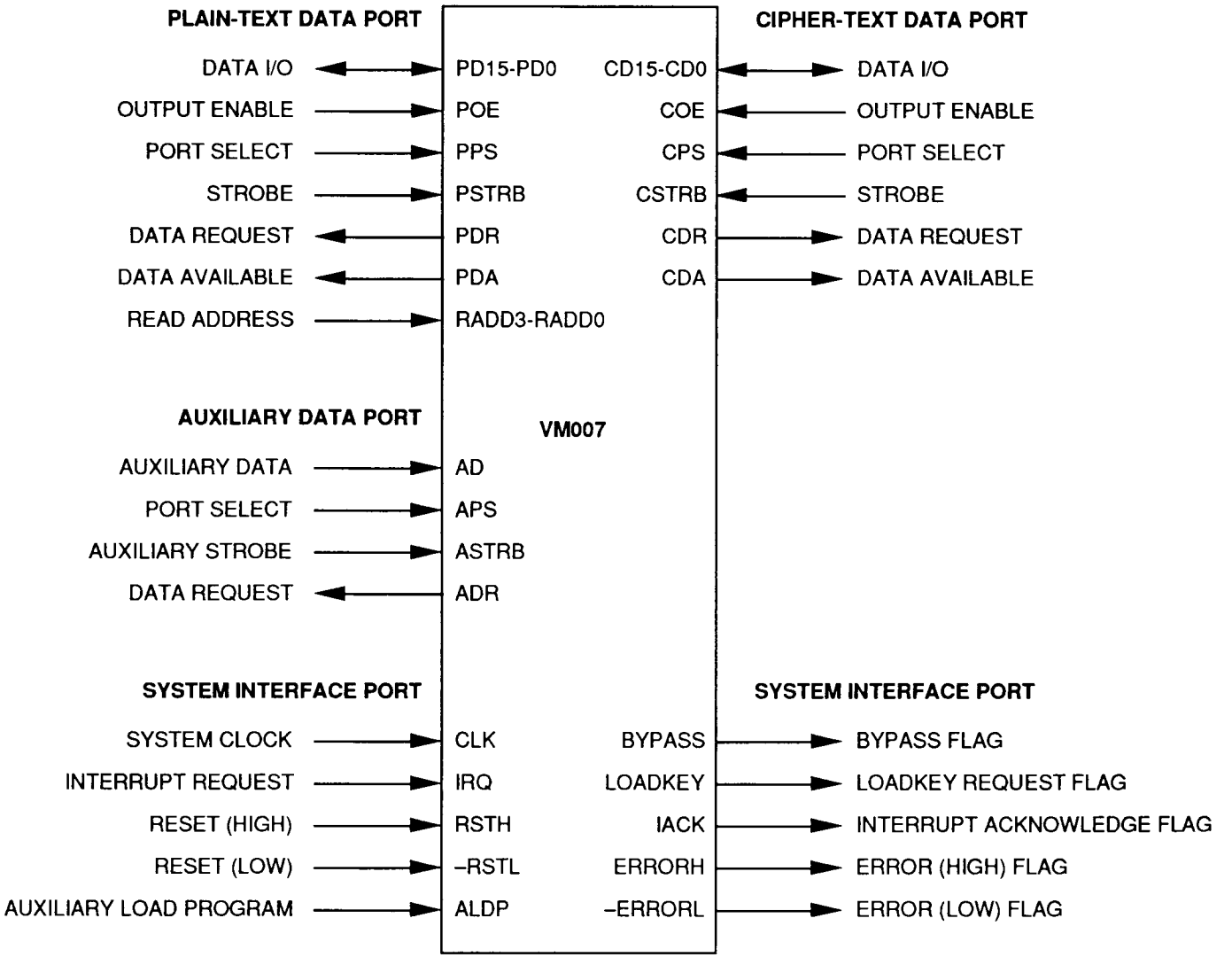
ORDER INFORMATION

Part Number	Operating Temperature Range (TA)	Package
VM007-1-TC	0°C to +85°C	Ceramic Leaded Chip Carrier
VM007-1-QC	0°C to +85°C	Plastic Leaded Chip Carrier
VM007-1-TM	–55°C to +125°C	Ceramic Leaded Chip Carrier

PIN DIAGRAM


VM007
TOP VIEW
1 CLK
2 VSSO
3 VSSI
4 –ERRORI
5 –RSTL
6 IACK
7 IRQ
8 PD15
9 PD14
10 PD13
11 VSSO
12 VDDO
13 PD12
14 PD11
15 PD10
16 PD9
17 PD8
18 PDA
19 POE
20 VSSI
21 VSSO
22 PSTRB
23 VDDO
24 VDDI
25 PPS
26 PDR
27 PD7
28 PD6
29 PD5
30 PD4
31 PD3
32 VSSO
33 VDDO
34 PD2
35 PD1
36 PD0
37 RADD3
38 RADD2
39 RADD1
40 RADD0
41 VSSI
42 VSSO
43 ASTRB
44 VDDO
45 VDDI
46 APS
47 AD
48 ALDP
49 ADR
50 CD0
51 CD1
52 CD2
53 VSSO
54 VDDO
55 CD3
56 CD4
57 CD5
58 CD6
59 CD7
60 CDR
61 CPS
62 VSSI
63 VSSO
64 CSTRB
65 VDDO
66 VDDI
67 COE
68 CDA
69 CD8
70 CD9
71 CD10
72 CD11
73 CD12
74 VSSO
75 VDDO
76 CD13
77 CD14
78 CD15
79 LOADKE\
80 BYPASS
81 RSTH
82 ERRORH
83 VDDI
84 VDDO

VM007 PIN-OUT BY FUNCTIONAL GROUPS



DEFINITION OF TERMS

Below are definitions of terms that are unique to the data encryption process.

DES	Data Encryption Standard (FIPS PUB 46-1).
FIPS PUB	An official publication relating to standards adopted and promulgated under federal regulations. Available from the National Institute of Standards and Technology (NIST), U.S. Department of Commerce.
Plain-text	Data which is not encrypted.
Cipher-text	Data that is in an encrypted form.
Key Variable	64-bit word including eight parity bits.
Active Key	The portion of the key variable without the parity bits (56 bits).
Operating Modes	One of several methods of using DES to encrypt or decrypt data. Reference FIPS PUB 81.
Initialization Vector	64-bit binary constant used at the start of Cipher Block Chaining (CBC), Cipher Feedback (CFB) or Output Feedback (OFB) modes of operation.

SIGNAL DESCRIPTIONS

Signal Name	Pin Number	Signal Type	Signal Description
PLAIN-TEXT DATA PORT			
PD15-PD0	8-10, 13-17, 27-31, 34-36	I/O	Plain-text Data Bus Bits 15-0 - A 16-bit data port for plain-text data and other control information. PD15 is the most significant bit (MSB).
POE	19	I	Plain-text Out Enable - This signal enables the Plain-text Output Buffer to be driven on PD15-PD0
PPS	25	I	Plain-text Port Select - An active high signal that enables the port buffer to send or receive data.
PSTRB	22	I	Plain-text Strobe - This strobe completes a read or write of plain-text data to the Plain-text Output Data Buffers. Maximun frequency = 50 MHz.
PDR	26	O	Plain-text Data Request - This status flag is active until the Plain-text Input Buffer is full.
PDA	18	O	Plain-text Data Available - This status flag is active until the Plain-text Output Buffer is empty.
RADD3-RADD0	37-40	I	Read Address Bus Bits 3-0 - Used to select a section of the memory map to display on the Plain-text Data Port.
AUXILIARY DATA PORT			
AD	47	I	Auxiliary Data - Serial data input port used for program, key, or other data used by the chip.
APS	46	I	Auxiliary Port Select - An active high signal that enables the port buffer to receive data.
ASTRB	43	I	Auxiliary Strobe - Rising edge completes loading of SD bit.
ALDP	48	I	Auxiliary Load Program - This signal is used during an interrupt to determine which port is to receive program and control data.
ADR	49	O	Auxiliary Data Request - A status flag which remains high until the auxiliary buffer is full.
CIPHER-TEXT DATA PORT			
CD15-CD0	50-52, 55-59 69-73, 76-78	I/O	Cipher-text Data Bus Bits 15-0 - A 16-bit data port that is used for encrypted data. CD15 is the most significant bit (MSB).
COE	67	I	Cipher-text Output Enable - This active high input enables the Cipher-text Output Buffer to drive the CD15-CD0 pins.
CPS	61	I	Cipher-text Port Select - An active high signal that enables the input or output buffers to receive data or send data.
CSTRB	64	I	Cipher-text Strobe - Rising edge completes the read or write operation on the port. Maximun frequency = 50 MHz.
CDR	60	O	Cipher-text Data Request - High until the Cipher-text Input Buffer is full.
CDA	68	O	Cipher-text Data Available - High until Cipher-text Output Buffer is empty.
SYSTEM CONTROL SIGNALS			
CLK	1	I	Clock - The system clock input. Its frequency operation is from 1 to 30 MHz and is active on its rising edge.
IRQ	7	I	Interrupt Request - An active high interrupt request used to halt cipher operations in order to change programs, keys, or initialization vectors.
RSTH	81	I-IPU	Reset High - Active high asynchronous reset input.
–RSTL	5	I-IPD	Reset Low - Active low asynchronous reset input.

SIGNAL DESCRIPTIONS (Cont.)

Signal Name	Pin Number	Signal Type	Signal Description
SYSTEM CONTROL FLAGS			
BYPASS	80	O	Bypass Mode - Programmable output flag used to indicate that the Bypass Mode is in operation.
LOADKEY	79	O	Load Key Request - Programmable output flag used to display system request for Key Variables.
IACK	6	O	Interrupt Acknowledge - This output is the acknowledge signal for an interrupt request.
ERRORH	82	O-IPU	Error High - An active high signal from the VM007 provided to alert the external system to an error condition. ERRORH is active following a system reset on the RSTH input until the built-in self-test is completed successfully. It can also be activated by an error condition during cipher processing.
–ERRORL	4	O-IPD	Error Low - An active low output signal from the VM007 provided to alert the external system to an error condition. –ERRORL is active following a system reset on the RSTL input until the built-in self-test is completed successfully. It can also be activated by an error condition during cipher processing.
POWER & GROUND PINS			
VSSI	3, 20, 41, 62	GND	Ground Core Connection - 0 volts.
VDDI	24, 45, 66, 83	PWR	Power Core Connection - Nominally +5 volts. Recommended to be bypassed separately from power pad connections to increase noise immunity.
VSSO	2, 11, 21, 32, 42, 53, 63, 74	GND	Ground Pad Connection - 0 volts.
VDDO	12, 23, 33, 44, 54, 65, 75, 84	PWR	Power Pad Connection - Nominally +5 volts. Recommended to be bypassed separately from the power core connection to increase noise immunity.

SIGNAL LEGEND

Signal Code	Signal Type
I	Input
I-IPD	Input with internal pull-down resistor; min = 22k ohms, max = 150k ohms.
O	Output
O-IPU	Output with internal pull-up resistor; min = 22k ohms, max = 150k ohms.
I/O	Input/Output (bidirectional)
GND	Ground
PWR	Power

FUNCTIONAL DESCRIPTION

The VM007 is a complete cryptographic processing system on a single chip. The device is designed to achieve high data through-put while providing advanced security features and superior reliability. In addition, the chip offers an optional programming interface to give the user flexibility to process complex cryptographic functions. These features make the VM007 uniquely able to solve demanding applications in high performance computing systems.

The VM007 is equipped with four separate and independent interfaces (refer to the diagram "VM007 Pin-Out by Functional Groups"). Three of these are data ports and the fourth is a set of system control pins. Each interface has a separate clock input which is used to synchronize control and data activity. The first data interface, called the Plain-text Port, is used to send or receive data which is in a decrypted (plain-text) form. The Plain-text Port can also be used to send and receive control data and Key Variables. The second interface is called the Cipher-text Port and is used to send or receive data in an encrypted form. A serial-input Auxiliary Port is provided to give an optional path for control and key information. The last port is the system interface, which is used to control the clock, reset, and interrupt functions.

Internally, the VM007 is composed of independent units coordinated by a 16-bit RISC sequencer (refer to the "Block Diagram" on page one). Internal data buses and storage registers operate on 64-bit data words. A 64-bit ALU is provided for logical, arithmetic, and shifting operations. A high-speed hardware implementation of the Data Encryption Standard (DES) is provided to perform Electronic Codebook computation. Data and Key Registers allow multiple cryptographic computations to run concurrently. All internal data processing is synchronized to the system clock (CLK).

SYSTEM INTERFACE

The system interface consists of a group of pins which are all synchronized by the system clock (CLK). The system interface pins control the reset, error detection and interrupt functions of the chip. In addition, several pins (ALDP, BYPASS, and LOADKEY) are used by the RISC Sequencer to control and display status of the device.

Resets

A pair of reset input pins (RSTH, –RSTL) provide redundant system initialization. An active input signal on either of these pins will cause an immediate chip reset and initiate the built-in self-test (BIST) procedure. The reset circuits are activated asynchronously to the system clock (CLK) to drive every register and control circuit to a predetermined value. The internal error detection circuits are triggered to an active state by the reset pins. This results in an active state on the error output pins (ERRORH, and –ERRORL). The reset circuits are designed so that once they are triggered to the reset state, even by a very short reset pulse, they hold for at least one full clock cycle before becoming inactive. Consequently, the clock is required in order to exit the reset state, but not to enter it.

Built-In Self-Test

Once the reset circuits become inactive, the RISC Sequencer will execute a sequence of instructions from a BIST ROM. This procedure must execute successfully before the VM007 will respond to any external signals. The BIST cannot be bypassed and will require approximately 1024 clock cycles to complete. Once BIST is complete, the RISC will be cleared to the System Library ROM and execute the system interrupt routine. During the internal interrupt routine, the IACK pin will become active. If the error output pins are still active after the IACK, then the BIST has detected a failure in the device, and further diagnostics should be run.

Interrupts

The Interrupt Request (IRQ) pin is provided to alert the VM007 to halt cipher processing and execute the system interrupt routine. The purpose of this routine is allow the Control Register (CR) and user program RAM to be updated with new information. Once the interrupt routine has started, the interrupt acknowledge (IACK) pin will be active. The first instruction executed by the system interrupt routine checks the value of the ALDP input pin. A high value on ALDP indicates to the sequencer that CR and program data will come from the serial-input Auxiliary Port. Otherwise, it will come from the Plain-text Port. CR values are 32 bits long, and RISC instructions are loaded in pairs (two 16-bit words). The CR data is always loaded first, followed by as many as 128 RISC instructions.

Once the IRQ pin becomes inactive, the interrupt routine will terminate immediately, and the RISC will branch to the initial address stored in the Control Register. It is not necessary to reload the CR before the interrupt routine terminates.

DATA INTERFACES

The input and output buffers (see the block diagram on page one) are composed of a 64-bit FIFO storage register and a flexible state-machine controller. Most operations of the I/O buffers are synchronized to the strobe used for that port. However, transfer of data to or from the central processing area is synchronized to the system clock (CLK). All data buffers are enabled to send or receive data by the I/O parameter of the Control Register. Status of any I/O buffer can be queried using the memory map on the Plain-text Port.

The input buffers connected to the Plain-text and Cipher-text Ports are all constructed the same way. They can receive up to 64 bits of data before they are full. The size of the input word is specified by a parameter in the Control Register called word-size. The word-size for the Auxiliary Port is always 1 bit. The number of bits stored in the input FIFO is controlled by a parameter called block-size. The block-size number is generally set to correspond to the size of the data block used for the specific cryptographic mode of operation being processed. For example, when using Electronic Codebook (ECB) mode, the block-size is set to 64 bits.

Output buffers for the Plain-text and Cipher-text Ports are similar to the input buffers. They respond to the word-size and block-size parameters in the same way, and they can hold up to 64 bits of data.

SECURITY FEATURES

The VM007 has many advanced security features to enhance the security and system reliability of the device, and protect data and key variables. These features are divided into the following categories:

- Pin interface
- System architecture
- Built-in self-test procedure
- DES Unit implementation
- Error detection

PIN INTERFACE

Separate Plain-text/Cipher-text Ports
The partitioning of the pin interface provides security to the system by separating the Plain-text and Cipher-text Ports. If the chip is used in this fashion on a circuit board, plain-text will not mix with cipher-text except in the Bypass mode.

Redundant Reset Pins
This feature provides redundant reset pins (RSTH, –RSTL). Either pin alone is sufficient to initiate a full system reset, including the clearing of all program, data, and key registers. The reset is initiated and accomplished asynchronously and does not require the system clock. Once initiated, a reset can not be aborted. In addition, a reset always triggers the error detection circuit, which forces both ERRORH and –ERRORL active. A reset always initiates the built-in self-test procedure.

Redundant Error Pins
This feature provides redundant error pins (ERRORH, –ERRORL) to protect against a failure on one of the signals.

No Partial Resets
The reset circuit will trap very short pulses on the reset pins and respond to them with a full system reset. This feature is provided to avoid partial system reset by glitches on either reset pin.

Critical Pins Forced Active
Several pins (see Signal Legend) incorporate internal pull-up and/or pull-down resistors on the silicon chip. This provides a default value on the pin when the pin is not driven from the outside. The defaults for the reset and error pins force them to be active, providing feedback to the system that there is a problem on these signals, or alerting the chip to a failure in the system.

SYSTEM ARCHITECTURE

Key Registers are Write-only
After a Key Variable is loaded into a Key Register, it can not be viewed or modified. Key Variables which need to be viewed or modified can be stored in the Data Registers first, then moved to the Key Register later. Only keys in the Key Register can be used by the DES Unit.

Limited Access to Control Register
The Control Register (CR) can only be modified during the interrupt routine or under software control. This prevents accidental changes to the CR which might compromise the security of the device.

Sequencer Instruction Internal Only
All instructions executed by the sequencer must come from dedicated internal instruction memory. This prevents tampering or monitoring of the instructions during execution. User programs must be downloaded to the VM007 under system interrupt procedures.

User Control over Encryption Processing
The programming interface in the VM007 allows user programs to control the device operation. This allows the user to develop elaborate routines for checking data and cipher integrity, as well as flexibility to incorporate more advanced modes of operation as they are developed.

Output Data Buffers Disabled Until Data Available
Both the Plain-text and Cipher-text Output Buffers are gated low until data is ready. This prevents old data, or erroneous data from leaving the chip.

BUILT-IN SELF-TEST

Automatic Built-In Self-Test after Reset
Following the completion of the reset, an internal self-test procedure is initiated. The self-test cannot be stopped or bypassed. If the device fails this procedure, the error pins will stay active.

DES UNIT

Hardware Implementation of DES ECB Mode
The Data Encryption Standard (DES) algorithm is built in hardware on the chip and can not be changed. In addition, the DES hardware unit contains an autonomous Electronic Codebook mode sequencer.

Always Completes Cipher
Once the DES Unit receives data and starts the cipher task, the Unit will not respond to any signal except clock and reset until the entire sequence is complete.

Continuous Parity Checking
The Key Variable is loaded with full DES parity into the DES Unit. The parity of the Key Variable is checked upon every clock cycle as the algorithm is performed. All parity errors trigger the error detection circuit into an active state, alerting the system to the error condition.

Key Warning Flags
The DES Unit has circuits which become active when an active Key Variable is all zero or all one, even if such a key has valid parity. These warning flags are provided in the programming interface to allow user programs to detect and act upon key variables which are weak.

Output Bus Disabled Until Cipher Complete
The output bus of the DES Unit is gated to an all zero value until the DES algorithm is completed. This feature protects accidental release of intermediate results of the cipher process.

ERROR DETECTION

Illegal Instruction Check
Instructions in the user programming interface are checked for validity.

Illegal Sequence Check
An illegal sequence of instructions which results in a system lock-up are detected. All such situations result in an active error on the error pins.

Key Parity Error Detection
All parity errors in Key Variables which enter the DES Unit cause an error condition.

MODES OF OPERATION

The VM007 supports all DES modes of operation:

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- A-mode for CFB and OFB

Refer to FIPS PUB 81 for a complete description of DES modes of operation.

ELECTRONIC CODEBOOK (ECB) MODE

The ECB mode is the fundamental cryptographic function of the DES algorithm. Plain-text data is divided into blocks of 64 bits to be encrypted. If the length of the plain-text data is not a multiple of 64 bits, then it must be extended (padded) to a length that is a multiple of 64 bits. Each block of plain-text is encrypted by computing a 64-bit block of cipher-text using the DES encryption algorithm and a 64-bit Key Variable. A description of this procedure can be found in the document titled Federal Information Processing Standards Publication 46-1. Each block of cipher-text resulting from the ECB encryption can use a different Key Variable. All other cryptographic modes of operation use the ECB procedure as part of the cipher process.

Cipher-text data is decrypted using the DES decryption algorithm and the 64-bit Key Variable used during encryption. Each 64-bit block of cipher-text used in the ECB decryption process must be that which was created by the ECB encryption process. A miss-alignment in dividing the cipher-text into 64-bit blocks will prevent the DES algorithm from computing the plain-text even if the correct Key Variable is used. Each block of cipher-text is independent in the sense that the decryption process does not rely upon other blocks of cipher-text in order to compute the plain-text.

CIPHER BLOCK CHAINING (CBC) MODE

The CBC mode differs from the ECB mode in that an additional 64-bit data block, called an Initial Vector (IV), is needed in addition to the 64-bit Key Variable. To perform CBC encryption, the first 64 bits of plain-text data are combined with the IV using a bit-wise exclusive OR function. The result of the exclusive OR function is encrypted using the ECB mode. The cipher-text from the ECB procedure is the first 64-bit block of CBC cipher-text. In addition, the cipher-text also becomes the IV to be used with the next block of plain-text data. This process is repeated until all the plain-text is encrypted.

CBC decryption takes the first 64 bits of cipher-text and decrypts it using ECB decryption. The resulting plain-text is exclusive ORed with the IV to form the first block of CBC plain-text data. The first cipher-text block also becomes the IV for the CBC decryption of the next cipher-text block. This process is repeated until all the cipher-text is decrypted. CBC mode is similar to ECB in that both require the plain-text (and cipher-text) to be integral multiples of 64 bits in length. However, CBC mode differs from ECB in that each block of cipher-text cannot be decrypted until the correct IV is generated. These IVs are generated during the decryption process of the preceding block of cipher-text. Consequently, the CBC cipher-text blocks are "chained" together, and must be decrypted in the same order that they were originally encrypted.

CIPHER FEEDBACK (CFB) MODE

The CFB mode also uses an Initial Vector (IV), but unlike the CBC mode, it is defined to operate on data blocks which can be as small as one bit, as large as 64 bits, or any size in-between. First, the IV is encrypted using a standard ECB step. The ECB cipher-text is combined with the first block of plain-text using a bit-wise exclusive OR function to form the first block of CFB cipher-text. The first IV and the CFB cipher-text are then barrel shifted to produce the next IV. The process is repeated until all the plain-text is encrypted.

CFB decryption starts with an ECB encryption of the IV. The ECB result is exclusive ORed bit-wise with the first word of the cipher-text to form the first word of plain-text. The next IV is formed by taking the first IV and barrel shifting it with the first cipher-text word.

OUTPUT FEEDBACK (OFB) MODE

The OFB mode also uses an Initial Vector (IV). First the IV is encrypted using the standard ECB step. The ECB result is exclusive ORed bit-wise with the plain-text to form the cipher-text. The new IV is created by taking the first IV and output of the first ECB step and barrel shifting them to produce the next IV. The process is repeated until all the plain-text in encrypted.

A-Mode

The A-mode is used when the cipher-text stream uses a parity bit in each byte of data.

REGISTER MEMORY MAP

The VM007 chip has a set of address pins labeled RADD3-RADD0. These pins are used to select the contents of internal status registers to display them an the Plain-text Output Port (refer to Table One: Register Memory map). The ability to view the contents of specific registers is provided so that the external system can monitor the internal state of the VM007. However, access to internal data registers (R0-R7) or key registers (K0-K3) is not provided in order to maintain security. Additional security is provided by the fact that the Register Memory Map is read-only.

Four RADD pins are provided in order to support a memory map of sixteen separate bytes. If the Plain-text Port is configured to use 16-bit words, then data in the memory map is viewed as a pair of bytes, and the least significant address bit, RADD0, is ignored. If an 8-bit interface is selected, then RADD0 is used. If a 1-bit interface is selected, then the Register Memory map should not be used at all, and all the RADD pins should be driven low.

Please note that the register values displayed in the Register Memory Map are not necessarily synchronized to the Plain-text Port timing. In fact, many of these signals are synchronized to the system clock (CLK), and some are direct input pins of the VM007 device. Therefore, care must be taken when reading the memory map registers so that data set-up and hold is maintained long enough for the external system to latch the data.

ID REGISTER

The ID register is provided in order to give the external system a means to identify the version of the VM007 device. The value in this register is embedded permanently in the layout of the silicon. When viewed as a 16-bit quantity, the ID register is always a hex value "0071" (for version VM007-1), and hex value "0072" hex (for version VM007-2).

TABLE 1. REGISTER MEMORY MAP (READ-ONLY)

RADD3-RADD0 Read Address (RADD)	Registers (Bits 15-0)	
	x = 0	x = 1
000x	PD15-PD8	PD7-PD0
001x	ID Register A	ID Register B
010x	Auxiliary Status	DES Status
011x	RISC Status	PC Address
100x	CR0	CR1
101x	CR2	CR3
110x	PI Status	PO Status
111x	CI Status	CO Status

RISC STATUS REGISTER

The RISC Status Register is a concatenation of important control signals in the RISC sequencer. The OP1 field (bits 3-0) displays the instruction op-code currently executed in the sequencer. The bit called PASS (active-high), displays the conditional execution status of the current op-code. If PASS is not active, the sequencer will stop execution until the conditions specified by the instruction are satisfied. The ALDP and IRQ status bits display the value on the input pins after they are synchronized to CLK. The EQZ signal from the ALU displays the status of the last comparison from a XOR or AND logical operation.

RISC PC ADDRESS REGISTER

The Program Counter (PC) of the RISC sequencer is available in order to monitor the execution of the internal programs. The program counter increments upon every clock cycle of CLK except when the RISC executes a branch instruction or conditional execution holds the PC.

TABLE 2. MEMORY MAP - DES UNIT STATUS

Bit	Name	Default	Function
7	RDIA	0	RISC Data Input Available
6	DDIR	1	DES Data Input Request
5	DDOA	0	DES Data Output Available
4	RDOR	0	RISC Data Output Request
3	COP	0	Cipher Operation in Progress
2	ZERO	0	Active Key is all Zeros
1	ONE	0	Active Key is all Ones
0	PER	0	Active Key has Parity Error

TABLE 3. MEMORY MAP - RISC STATUS

Bit	Name	Default	Function
7	EQZ	0	ALU Equal Zero (flag)
6	ALDP	0	Auxiliary Load Program (input pin)
5	IRQ	1	Interrupt Request (input pin)
4	PASS	1	RISC Execution Enabled
3	OPA	0	OP-code
2	OPB	0	OP-code
1	OPC	0	OP-code
0	OPD	0	OP-code

Where: (OPA, OPB, OPC, OPD) is: OP-code field from currently executed instruction.

TABLE 4. MEMORY MAP - INPUT FIFOs (Input Data FIFOs: PISTAT, CISTAT, and AISTAT)

Bit	Name	Default	Function
7	DR	0	Data Request (output pin)
6	DA	0	Data Available (input pin)
5	RDR	0	RISC Data Request
4	FDA	0	FIFO Data Available
3	FULL	0	FIFO Full Flag
2	BS1	0	Byte Counter (MSB)
1	BS2	0	Byte Counter
0	BS3	0	Byte Counter (LSB)

Where: BS1, BS2, BS3 count data is loaded

000 = 0 bytes (or 8 bytes if FULL is true)	100 = 4 bytes loaded
001 = 1 bytes loaded	101 = 5 bytes loaded
010 = 2 bytes loaded	110 = 6 bytes loaded
011 = 3 bytes loaded	111 = 7 bytes loaded

TABLE 5. MEMORY MAP - OUTPUT FIFOs (Output Data FIFOs: POSTAT and COSTAT)

Bit	Name	Default	Function
7	DR	0	Data Request (input pins)
6	DA	0	Data Available (output pins)
5	FDR	1	FIFO Data Request
4	RDA	0	RISC Data Available
3	EMPTY	1	FIFO Empty (flag)
2	BS1	0	Byte Counter (MSB)
1	BS2	0	Byte Counter
0	BS3	0	Byte Counter (LSB)

Where: BS1, BS2, BS3 count data is unloaded

000 = 0 bytes (or 8 bytes if EMPTY is true)	100 = 4 bytes unloaded
001 = 1 bytes unloaded	101 = 5 bytes unloaded
010 = 2 bytes unloaded	110 = 6 bytes unloaded
011 = 3 bytes unloaded	111 = 7 bytes unloaded

CONTROL REGISTER

The Control Register (CR) in the VM007 holds several parameters that are needed during device operation. The CR is divided into four groups of eight bits, each of which controls a different aspect of device operation. Table 1 shows each group, labelled CR0-CR3. The CR can be modified in one of two ways. First, the system interrupt routine expects to receive a new CR value during an interrupt acknowledge. If one is given, it replaces the current CR when the system interrupt routine jumps to its initial address. This is the most common way to change the CR. The second way to modify the CR is for a program routine to execute the SCR command, which can modify any of the four CR groups. If a Library Program Routine is executed, consult the reference page for that routine to determine if it changes a CR value during execution. Otherwise, the effects of the SCR command are limited to those which the programmer intends.

TABLE 6. CONTROL REGISTER (CR), BITS 31-0

Name	Bit	Function
CR0	31-24	I/O Control Parameters
CR1	23-16	Data Size Parameters
CR2	15-8	Default Parameters
CR3	7-0	Initial Program Address

CR0 - I/O Control Parameters

The input/output control parameters are used to set a value on an output pin, or to enable an input or output data buffer. Three of the output pins on the VM007 are controlled directly by this word in the CR; IACK, BYPASS, and LOADKEY.

TABLE 7. I/O CONTROL PARAMETERS (BITS 31-27)

Bit	Name	Default	Function
31	IACK	0	Interrupt Acknowledge (pin)
30	BYPASS	0	Bypass mode (pin)
29	LOADKEY	0	Load Key mode (pin)
28	AIBE	0	Auxiliary Input Buffer Enable
27	PIBE	0	Plain-text Input Buffer Enable
26	POBE	0	Plain-text Output Buffer Enable
25	CIBE	0	Cipher-text Input Buffer Enable
24	COBE	0	Cipher-text Output Buffer Enable

CR1 - Data Size Parameters
This group of bits holds the size of the I/O words used on the Plain-text and Cipher-text Ports, as well as the size of the internal data blocks. Selecting a word-size less than 16 bits on either Plain-text or Cipher-text Ports will disable the unused pins of the bus interface.

TABLE 8. DATA SIZE PARAMETERS (BITS 23-16):

Bit	Name	Default	Function
23	PW1	1	Plain-text Port Word-size
22	PW2	0	Plain-text Port Word-size
21	CW1	1	Cipher-text Port Word-size
20	CW2	0	Cipher-text Port Word-size
19	A-MODE	0	A-Mode enable
18	BLK1	1	Block-size
17	BLK2	0	Block-size
16	BLK3	0	Block-size

Where:

PW1	PW2	Size
0	0	1-bit words (serial)
0	1	8-bit words
1	0	16-bit words
1	1	32-bit words (not used at this time)

BLK1 (Blocks)	BLK2	BLK3	Size
0	0	0	1-bit data
0	0	1	8-bit data
0	1	0	16-bit data
0	1	1	32-bit data
1	x	x	64-bit data

CR2 - Default Parameters
The error override bits have an unusual characteristic, they display the current value of the error detection circuit. If the error bits are enabled, they will stay enabled until disabled by writing to the CR2 again. However, if they are disabled, but an error condition still exists, they will immediately become active again upon the next clock cycle. All the other bits in the CR stay where you set them, until they are modified by a new CR value, or modified by the SCR command.

TABLE 9. DEFAULT PARAMETERS (BITS 15-8)

Bit	Name	Default	Function
15	ERRORH	1	Error High Override
14	–ERRORL	0	Error Low Override
13	RESETH	1	Reset High Override
12	–RESETL	0	Reset Low Override
11	IOSYNC	0	I/O Sync Mode
10	ENCRYPT	1	Encrypt Default Mode
9	KEY1	0	Key Default
8	KEY2	0	Key Default

Where:

KEY1	KEY2	Key Register:
0	0	K0
0	1	K1
1	0	K2
1	1	K3

CR3 - Initial Program Address
The initial program address is used to determine the location to jump to once the interrupt routine is complete. (See Library Program documentation.)

TABLE 10. INITIAL PROGRAM ADDRESS (BITS 7-0)

Bit	Name	Default	Function
7-0	ADDRESS	'h70	Initial Address

USER PROGRAMMING INTERFACE

The VM007 is composed of a set of autonomous hardware resources whose activity is coordinated by a central programmable sequencer. The instructions executed by the sequencer are specifically tailored to the data flow architecture of the chip in order to balance high data processing rates with flexible functionality. The program memory for the sequencer resides entirely on the VM007 to enhance the security and reliability of the instruction execution. Consequently, there is no dedicated external address or data bus for the sequencer.

A library of sequencer programs is stored in a read-only memory (ROM) structure on the chip. A description of these library programs is given in the section called "System Library Routines". All of the standard cryptographic modes of operation are supplied in the System Library and it is possible to operate the device utilizing only these routines. However, the user may also write programs that can be used alone or in combination with the system library routines to optimize the VM007 for a particular application.

The VM007 contains a random access memory (RAM) area for storage of user programs. User programs allow much greater flexibility in the function of the device, as well as gaining access to hardware features not used by the Program Library. Instructions such as Set Key Parity (SKP) and the associated hardware in the ALU are provided for users who wish to create their own DES Key Variables. Other instructions, such as Decrement (DEC) are provided to allow programs to keep track of data processing using count variables.

INSTRUCTION SET REFERENCE GUIDE

The instruction set for the VM007 RISC Sequencer is composed of 16 basic instructions. The instructions are 16 bits long and are broken down into four operand fields of four bits each. The first field (listed as OP1) in Table 11, is the opcode for the instruction. xsrc, ysrc, and dest values are defined by the table called Operand Fields (Table 12). These fields define where data is coming from and where it will be placed.

The flag codes for the two jump instructions are defined in the Jump Condition Flags Table (Table 13). The user can monitor the various flags by addressing the appropriate register with the RADD pins as defined in the Register Memory Map.

Some instructions, such as ECE, have fields that are either all or partially zero. These fields are reserved for future use. In order to ensure upward compatibility, the user should be sure that zeros are used in these locations.

The instruction set is defined in more detail on the following pages.

All instructions except MVL require one clock cycle to execute. All branching instructions which are successful are followed by a NOP cycle in order to allow time to fetch the next instruction. Instructions which can fail due to resource delay will create NOP cycles until the resource is ready. For this reason, the user should check to make sure that the appropriate resources are available before continuing execution to avoid placing the processor in an endless loop.

TABLE 11. INSTRUCTION SET OP-CODES

OP1	OP2	OP3	OP4	Mnemonic	Description
0000	xsrc	00kk	0000	ECE	ECB encrypt X with K
0001	xsrc	00kk	0000	ECD	ECB decrypt X with K
0010	xsrc	ysrc	dest	BSH	Barrel Shift X, Y, put in d
0011	xsrc	00vv	dest	LRT	Left Rotate X by V, put in d
0100	xsrc	dest	dest	MOV	Move X to e, d
0101	xsrc	dest	dest	MVN	Move invert X to e, d
0110	xsrc	ysrc	dest	XOR	XOR X, Y, put in d
0111	xsrc	ysrc	dest	AND	AND X, Y, put in d
1000	xsrc	0000	dest	SKP	Set key parity bits
1001	xsrc	0nnn	dest	MVL	Move VALUE to d
1010	00rr	valu	valu	SCR	Set Control Register
1011	xsrc	0000	0000	LPD	Load Program from X
1100	xsrc	addr	addr	DEC	Decrement X, if 0, jump J
1101	cri0	addr	addr	CRI	Call/Return/INIT
1110	flag	addr	addr	JPN	Jump to address J if F is false
1111	flag	addr	addr	JMP	Jump to address J if F is true

TABLE 12. OPERAND FIELDS

OP1	X Source	Y Source	Destination
0000	R0	R0	R0
0001	R1	R1	R1
0010	R2	R2	R2
0011	R3	R3	R3
0100	R4	R4	R4
0101	R5	R5	R5
0110	R6	R6	R6
0111	R7	R7	R7
1000	Zero	Zero	K0
1001	Zero	Zero	K1
1010	Zero	Zero	K2
1011	Zero	Zero	K3
1100	PI	*DO	PO
1101	CI	*DO	CO
1110	AI	*DO	CR
1111	DO	DO	DI

Note: Sources with * are for aliased source. Zero means sources are all 0.

TABLE 13. JUMP CONDITION FLAGS

Code	Flag	Description
0000	PIA	Source: Plain-text internal data Input Available
0001	CIA	Source: Cipher-text internal data Input Available
0010	AIA	Source: Auxiliary internal data Input Available
0011	DOA	Source: Data Output Available (DES Unit)
0100	DOR	Destination: Plain-text internal data Output Request
0101	COR	Destination: Cipher-text internal data Output Request
0110	AOR	Destination: Auxiliary internal data Output Request
0111	DIR	Destination: Data Input Request (DES Unit)
1000	COP	DES Unit: Cipher-text Operation in Progress
1001	ZERO	DES Unit: Active Key is all 0s
1010	ONE	DES Unit: Active Key is all 1s
1011	PER	DES Unit: Active Key has Parity Error
1100	EQZ	ALU: Output is all 0s
1101	ALDP	Load Program from Auxiliary Port (input pin)
1110	IRQ	System Interrupt Requested (input pin)
1111	UNC	Unconditional; always true (always false)

AND

Logical AND

The AND instruction takes two 64-bit data words, performs a bit-wise AND function, and moves the result to the selected destination. AND can be used to initiate an encrypt or decrypt task if the destination operand is the input to the DES Unit (DI). This is called an implicit cipher request and uses the default settings in the Control Register to select the Key Register and the cipher mode. The AND executes in one clock cycle if the source and destination registers are available. If the AND instruction fails to execute due to an unavailable resource, the RISC will execute NOP instructions until the resource becomes available.

Fields	Bit Value	Description
OP1	0111	AND Instruction Code
OP2	xsrc	X Source Data
OP3	ysrc	Y Source Data
OP4	dest	Destination Operand

Control Register

The default key parameter in the Control Register is used to select the Key Variable during an implicit cipher request. The default mode parameter (encrypt or decrypt) is selected by the value in the encrypt parameter (bit 6)

Conditional Execution

The AND instruction uses the following flags to evaluate.

Source Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
POR, COR, AOR, DIR

BSH

Barrel Shift

The BSH instruction takes two 64-bit data words, X and Y, performs a barrel shift, and moves the 64-bit result to the selected destination. The barrel shift logic can perform a left-shift of the concatenated operand {X,Y} by 1, 8, 16, 32, or 64 bits. The size of the shift is determined by the value in the block-size parameter in the Control Register. The barrel shift function is essential for the Cipher Feedback (CFB) and Output Feedback (OFB) modes of operation.

Control Register

The block-size parameter in the Control Register selects the size of the barrel shift operation.

Fields	Bit Value	Description
OP1	0010	BSH Instruction Code
OP2	xsrc	X Source Data
OP3	ysrc	Y Source Data
OP4	dest	Destination Operand

Conditional Execution

The BSH instruction uses the condition flags associated with the source and destination address to allow completion of the instruction. If the condition flags associated with the sources or destination are not active, then the Sequencer must execute wait states until the flag becomes active. Once all specified condition flags are active, the Sequencer will complete execution of the BSH instruction, and load the next instruction.

Source Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
POR, COR, AOR, DIR,

CRI

Call/Return/Initialize

The CRI instruction combines three related functions. It can call to an address in the instruction field, return from a call to an original address, or jump to the address specified in the Control Register.

Bit 4 of the CRI field is unused and should remain zero. Only one bit at a time can be changed in OP2 or else the instruction will default to a NOP.

Fields	Bit Value	Description
OP1	1101	CRI Instruction Code
OP2	cri0	Select Field
OP3	addr	Jump Address
OP4	addr	Jump Address

Control Register
The Init parameter of the Control Register is used during a CRI Init execution.

Conditional Execution
The CRI instruction does not use conditional execution.

Where:

OP2 = 1000	Call To Address
OP2 = 0100	Return To Previous Address
OP2 = 0010	Jump To Init Address
OP2 = all others	No Operation Instruction

DEC

Decrement and Branch If Zero

The DEC instruction is the only arithmetic function in the VM007. It takes a 64-bit data operand register, decrements the least significant 16-bit section, and moves the result back to the source register. If the 16-bit section is all zeros following the decrement, the address field of the instruction will be used to fetch the next instruction.

Fields	Bit Value	Description
OP1	1100	DEC Instruction Code
OP2	xsrc	X Source Data
OP3	addr	Jump Address
OP4	addr	Jump Address

Control Register
Parameters in the Control Register do not effect DEC execution.

Conditional Execution
The DEC instruction does not use conditional execution.

ECD

Electronic Codebook Decryption Request

The ECD instruction moves a 64-bit block of data to the input of the DES Unit along with a 64-bit Key. The source of the data can be any of the eight Data Registers (R0-R7), or any active input buffer (AI, PI, CI, or DO). The Key Variable is selected from one of the four Key Registers (K0-K3). After the ECD instruction is executed, the DES Unit will complete the Electronic Codebook (ECB) mode decryption task after eight clock cycles. On the ninth clock cycle following ECD, the decrypted data will be available at the output of the DES Unit. During the decryption task, the RISC Sequencer is free to execute other instructions. See also; ECE, MOV.

Control Register

Parameters in the Control Register do not effect ECD execution.

Fields	Bit Value	Description
OP1	0001	ECD Instruction Code
OP2	xsrc	X Source Data
OP3	00kk	Key Source
OP4	0000	Currently Unused

Conditional Execution

The ECD instruction uses the condition flags associated with the source and destination address to allow completion of the instruction. If a condition flag is not active, then the Sequencer must execute wait states until the flag becomes active.

Source Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
DIR

Where: kk = 00 Key Register 0
kk = 01 Key Register 1
kk = 10 Key Register 2
kk = 11 Key Register 3

ECE

Electronic Codebook Encryption Request

The ECE instruction moves a 64-bit block of data to the input of the DES Unit along with a 64-bit Key. The source of the data can be any of the eight Data Registers (R0-R7), or any active input buffer (AI, PI, CI, or DO). The Key Variable is selected from one of the four Key Registers (K0-K3). After the ECE instruction is executed, the DES Unit will complete the Electronic Codebook (ECB) mode encryption task after eight clock cycles. On the ninth clock cycle following ECE, the encrypted data will be available at the output of the DES Unit. During the encryption task, the RISC Sequencer is free to execute other instructions. See also; ECD, MOV.

Control Register

Parameters in the Control Register do not effect ECE execution.

Fields	Bit Value	Description
OP1	0000	ECE Instruction Code
OP2	xsrc	X Source Data
OP3	00kk	Key Source
OP4	0000	Currently Unused

Conditional Execution

The ECE instruction uses the condition flags associated with the source and destination address to allow completion of the instruction. If a condition flag is not active, then the Sequencer must execute wait states until the flag becomes active.

Source Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
DIR

Where: kk = 00 Key Register 0
kk = 01 Key Register 1
kk = 10 Key Register 2
kk = 11 Key Register 3

JMP

Jump if Flag True

The JMP instruction provides a test and branch ability to the Sequencer. It selects one of 16 flag variables, determines if it is true, and, if so, the address field of the instruction will be used to fetch the next instruction. Otherwise, the instruction fetch continues sequentially. See also; JPN.

Control Register

Parameters in the Control Register do not effect JMP execution.

Conditional Execution

The JMP instruction does not use conditional execution.

Fields	Bit Value	Description
OP1	1111	JMP Instruction Code
OP2	flag	Jump Condition Flag
OP3	addr	Jump Address
OP4	addr	Jump Address (cont.)

JPN

Jump if Flag not True

The JPN instruction provides a test and branch ability to the Sequencer. It selects one of 16 flag variables, determines if it is false, and if so, the address field of the instruction will be used to fetch the next instruction. Otherwise, the instruction fetch continues sequentially. See also; JMP.

Control Register

Parameters in the Control Register do not effect JPN execution.

Conditional Execution

The JPN instruction does not use conditional execution.

Fields	Bit Value	Description
OP1	1110	JPN Instruction Code
OP2	flag	Jump Condition Flag
OP3	addr	Jump Address
OP4	addr	Jump Address (cont.)

LPD

Load Program

The LPD instruction moves the source data block into the user instruction memory. The LPD requires one clock cycle to execute. If the LPD instruction fails to execute due to an unavailable resource, the RISC will execute NOP instructions until the resource becomes available.

Control Register

Parameters in the Control Register do not effect LPD execution.

Conditional Execution

The LPD instruction uses the following flags to evaluate.

Sources Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
AOR

Fields	Bit Value	Description
OP1	1011	LPD Instruction Code
OP2	xsrc	X Source Data
OP3	0000	Currently Unused
OP4	0000	Currently Unused

LRT

Left Rotate

The LRT instruction takes a 64-bit data word, performs a left-rotate, and moves the 64-bit result to the selected destination. The rotate logic can perform a left-rotate of the source operand X by 1, 8, 16, or 32-bits. The size of the rotate is determined by the value in the OP3 field in the instruction. The barrel shift function is essential for the Cipher Feedback (CFB) and Output Feedback (OFB) modes of operation. If the LRT instruction fails to execute due to an unavailable resource, the RISC will execute NOP instructions until the resource becomes available.

Control Register

Parameters in the Control Register do not effect LRT execution.

Fields	Bit Value	Description
OP1	0011	LRT Instruction Code
OP2	xsrc	X Source Data
OP3	00vv	Number of Left-rotate shifts
OP4	dest	Destination Operand

Conditional Execution

The LRT instruction uses the following flags to evaluate.

Data Sources:
PIA, CIA, AIA, DOA

Destination:
POR, COR, AOR, DIR

Where: 00 = 1 bit
01 = 8 bits
10 = 16 bits
11 = 32 bits

MOV

Move Data

The MOV instruction takes a 64-bit data word and moves it to the selected destinations. The instruction supports two destination fields (OP3, OP4). MOV can be used to initiate an encrypt or decrypt task if one of the destination codes is the input to the DES Unit (DI). This is called an implicit cipher request and uses the default settings in the Control Register to select the Key Register and the cipher mode. The MOV is useful for all modes of operation. The MOV executes in one clock cycle if the source and destination registers are available. If the MOV instruction fails to execute due to an unavailable resource, the RISC will execute NOP instructions until the resource becomes available.

Fields	Bit Value	Description
OP1	0100	MOV Instruction Code
OP2	xsrc	X Source Data
OP3	dest	First Destination Operand
OP4	dest	Second Destination Operand

Control Register

The default key parameter in the Control Register is used to select the Key Variable during an implicit cipher command. The default mode parameter (encrypt or decrypt) is selected by the value in the encrypt parameter (bit 6)

Conditional Execution

The MOV instruction uses the following flags to evaluate.

Sources Condition Flags:
PIA, CIA, AIA, DOA

Destination Condition Flags:
POR, COR, AOR, DIR

MVI

Move Data Invert

The MVI instruction takes a 64-bit data word and moves it to the selected destinations in one's compliment form. The instruction supports two destination fields (OP3, OP4). MVI can be used to initiate an encrypt or decrypt task if one of the destination codes is the input to the DES Unit (DI). This is called an implicit cipher request and uses the default settings in the Control Register to select the Key Register and the cipher mode. The MVI is useful for all modes of operation. The MVI executes in one clock cycle if the source and destination registers are available. If the MVI instruction fails to execute due to an unavailable resource, the RISC will execute NOP instructions until the resource becomes available.

Fields	Bit Value	Description
OP1	0101	MVI Instruction Code
OP2	xsrc	X Source Data
OP3	dest	First Destination Operand
OP4	dest	Second Destination Operand

Control Register

The default key parameter in the Control Register is used to select the Key Variable during an implicit cipher command. The default mode parameter (encrypt or decrypt) is selected by the value in the encrypt parameter (bit 6)

Conditional Execution

The MVI instruction uses the following flags to evaluate.

Sources Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
POR, COR, AOR, DIR

MVL

Move Value

The MVL instruction moves the next specified number of sequential instructions from program memory to the selected destination. MVL can be used to initiate an encrypt or decrypt task if the destination code is the input to the DES Unit (DI). This is called an implicit cipher request and uses the default settings in the Control Register to select the Key Register and the cipher mode. The MVL is the only instruction which may require more than one clock cycle to execute. If the MVL instruction fails to execute due to an unavailable resource, the RISC will execute NOP instructions until the resource becomes available.

Fields	Bit Value	Description
OP1	1001	MVL Instruction Code
OP2	xsrc	X Source Data
OP3	0nnn	Number of Words to Move
OP4	dest	Destination Code

Conditional Execution

The MVL instruction uses the following flags to evaluate.

Source Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
POR, COR, AOR, DIR

Where:

nnn = 000	0 Words Moved
nnn = 001	1 Word Moved
nnn = 010	2 Words Moved
nnn = 011	3 Words Moved
nnn = 100	4 Words Moved
nnn = 101	5 Words Moved
nnn = 110	6 Words Moved
nnn = 111	7 Words Moved

SCR

Set Control Register

The SCR instruction alters the contents of the Control Register. The OP2 field of the instruction selects one of the four bytes of the Control Register (CR) to be altered. The data value in OP3 and OP4 fields are written to the CR upon the completion of the instruction. The SCR requires more one clock cycle to execute and will complete unconditionally.

Control Register

Settings of the Control Register do not effect execution of SCR.

Fields	Bit Value	Description
OP1	1010	SCR Instruction Code
OP2	00rr	Control Register Select
OP3	valu	Data Value
OP4	valu	Data Value

Conditional Execution

The SCR instruction uses the following flags to evaluate.

Source Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
POR, COR, AOR, DIR

Where: rr = 00
CR bits 1-8; I/O Control
rr = 01
CR bits 9-16; Data Size
rr = 10
CR bits 17-24 Defaults
rr = 11
CR bits 25-32 Init Address

SKP

Set Key Parity

The SKP instruction takes a 64-bit data word, inserts the DES key parity bits and moves the result to the selected destination. The instruction is provided to allow the programmer to use data words computed by the DES Unit, or data from an external source (such as a password or random number generator) as a Key Variable for use in DES cipher tasks. A valid DES Key Variable (bits 1-64) uses bits 8, 16, 24, 32, 40, 48, 56, and 64 to store the odd parity of the byte containing the parity bit. These parity bits are used by the DES unit to detect single bit errors in the Key Variable during a cipher task. The SKP instruction substitutes the parity value for each byte of the source data word into the proper DES specified bit locations. A Key Variable modified by SKP can be used by the DES Unit if it is moved to a Key Register. The SKP executes in one clock cycle and is subject to conditional execution.

Fields	Bit Value	Description
OP1	1000	SKP Instruction Code
OP2	xsrc	X Source Data
OP3	0000	Currently Unused
OP4	dest	Destination Operand

Control Register

Parameters in the Control Register do not effect SKP execution.

Conditional Execution

The SKP instruction uses the condition flags associated with the source and destination to allow completion of the instruction. If a condition flag is not active, then the Sequencer must execute wait-states until the flag becomes active.

Source Condition Flags:
PIA, CIA, AIA, DOA
Destination Condition Flags:
POR, COR, AOR, DIR

XOR

Logical Exclusive OR

The XOR instruction takes two 64-bit data words, performs a bit-wise exclusive-or function and moves the result to the selected destination. XOR can be used to initiate an encrypt or decrypt task if the destination code is the input to the DES Unit (DI). This is called an implicit cipher request and uses the default settings in the Control Register to select the Key Register and the cipher mode. The XOR executes in one clock cycle if the source and destination registers are available. If the XOR instruction fails to execute due to an unavailable resource, the RISC will execute NOP instructions until the resource becomes available.

Fields	Bit Value	Description
OP1	0110	XOR Instruction Code
OP2	xsrc	X Source Data
OP3	ysrc	Y Source Data
OP4	dest	Destination Operand

Control Register

The default key parameter in the Control Register is used to select the Key Variable during an implicit cipher requests. The default mode parameter (encrypt or decrypt) is selected by the value in the encrypt parameter (bit 6).

Conditional Execution

The XOR instruction uses the following flags to evaluate.

Data Sources:
PIA, CIA, AIA, DOA

Destination:
POR, COR, AOR, DIR

SYSTEM LIBRARY ROUTINES

The programs contained in the internal library give the user of the VM007 a predefined set of commonly used cryptographic functions. All four of the DES cryptographic modes of operation (as defined by FIPS PUB 81) are provided. These modes are Electronic Codebook (ECB), Cipher Block Chaining (CFB), Cipher Feedback (CFB), and Output Feedback (OFB). Separate programs are provided to perform encryption and decryption for each operating mode. All of these programs use the basic features of the VM007 hardware to implement the modes. The FIPS PUB 81 defines the size of data blocks that are used for each mode. If the user wants to use a word-size different than that supported by the Internal Library Programs, then a user program should be created for use by the VM007 device. Such programs can be loaded to the VM007 after device power-up.

The internal ROM library in the VM007 device is composed of 128 words of 16 bits each. It contains 17 programs that provide all of the basic operations needed to run the chip. The specific details of each program are found under the following titles.

The RISC Sequencer in the VM007 uses a 256-word address space to access ROM and RAM programs. The address space from 0-127 is devoted to the ROM, and the space from 128-255 is used by the RAM. Information concerning the use of the Control Register and ROM program library can be found in the section called "Using the VM007". If a user program is needed, please refer to the section called "Programing Interface". The ROM program library provides useful examples of programs to those who want to create user programs for the VM007.

TABLE 14. SYSTEM LIBRARY ROUTINES

Hex Address	Parameter
00	Main System Interrupt Routine
10	Electronic Codebook Mode (Encrypt)
18	Electronic Codebook Mode (Decrypt)
20	Cipher Block Chaining Mode (Encrypt)
28	Cipher Block Chaining Mode (Decrypt)
30	Cipher Feedback Mode (Encrypt)
38	Cipher Feedback Mode (Decrypt)
40	Output Feedback Mode (Encrypt)
48	Output Feedback Mode (Decrypt)
50	Load Keys from Aux Port
58	Load Keys from Plain-text Port
60	Load IV from Aux Port
64	Load IV from Plain-text Port
68	Load User Program from Aux Port
6C	Load User Program from Plain-text Port
70	Bypass Mode (Bidirectional)
7C	System Purge Routine

MAIN SYSTEM INTERRUPT

The main system interrupt routine is executed following the completion of a system reset, or following the termination of a cryptographic operation routine. It can also be executed from a user program. The function of the routine is to reload the contents of the Control Register (CR) with a 32-bit value supplied to the Plain-text or Auxiliary Input Ports. If no value is supplied before the IRQ pin becomes inactive, the routine will jump to the current initialization address in the Control Register. If a CR is supplied, the routine jumps to the load program routine.

TABLE 15. MAIN SYSTEM INTERRUPT

Address	Data	Mnemonic	Comments
00	A1A3	SCR CR1 → 'hA3	Set CR
01	ED08	JPN ALDP → 'h08	Jump if not ALDP
02	A090	SCR CR0 → 'h90	Enable Aux Port
03	EE07	JPN IRQ → 'h07	Jump if not IRQ
04	E203	JPN AIA → 'h03	Jump if not Aux Data
05	4EEE	MOV AI → CR, CR	Move Aux to CR
06	FF68	JMP UNC → 'h68	Jump to Load Program
07	D200	CRI INIT →	Jump to Init Address
08	A088	SCR CR0 → 'h88	Enable Plain-text Port
09	EE0D	JPN IRQ → 'h0D	Jump if not IRQ
0A	E009	JPN PIA → 'h09	Jump if no Plain-text
0B	4CEE	MOV PI → CR, CR	Move PI to CR
0C	FF6C	JMP UNC → 'h6C	Jump to Load Program
0D	D200	CRI INIT →	Jump to Init Address
0E	FF00	JMP UNC → 'h00	Never Used
0F	FF00	JMP UNC → 'h00	Never Used

Notes:
1. Always enter the routine from address 'h00.
2. Ensure that ALDP pin has the correct value before execution.
3. Ensure that IRQ pin remains active until completion.

ELECTRONIC CODEBOOK MODE (ENCRYPT)

This routine performs the Electronic Codebook (ECB) mode of operation. Data from the Plain-text Input Port is moved to the DES Unit for encryption. The Key Variable used during the encryption process is selected by the default value in the Control Register. The resulting cipher-text is moved it to the Cipher-text Output Port. This routine will not jump to the interrupt routine until the Cipher-text Output Buffer is empty. Unless interrupted, the routine will continuously repeat.

TABLE 16. ELECTRONIC CODEBOOK MODE (ENCRYPT)

Address	Data	Mnemonic	Comments
10	E014	JPN PIA → 'h14	Jump if not PIA
11	4CFF	MOV PI → DI, DI	Move PI to DES
12	4FDD	MOV DO → CO, CO	Move DES to CO
13	D400	CRI RET →	Return if Called
14	EE10	JPN IRQ → 'h10	Jump if not IRQ
15	A001	SCR CR0 → 'h01	Set CR, Disable PI
16	E516	JPN COR → 'h16	Jump if not COR
17	FF00	JMP UNC → 'h00	Jump to Init

Notes:
1. Faster ECB routines can be written by the user if needed.
2. The active Key (K0, K1, K2, K3) is selected by the CR register.

ELECTRONIC CODEBOOK MODE (DECRYPT)

This routine performs the Electronic Codebook (ECB) mode of operation. Data from the Cipher-text Input Port is moved to the DES Unit for decryption. The Key Variable used during the decryption process is selected by the default value in the Control Register. The resulting plain-text is moved to the Plain-text Output Port. This routine will not jump to the interrupt routine until the Plain-text Output Buffer is empty. Unless interrupted, the routine will continuously repeat.

TABLE 17. ELECTRONIC CODEBOOK MODE (DECRYPT)

Address	Data	Mnemonic	Comments
18	E11C	JPN CIA → 'h1C	Jump if not CIA
19	4DFF	MOV CI → DI, DI	Move CI to DES
1A	4FCC	MOV DO → PO, PO	Move DES to PO
1B	D400	CRI RET →	Return if Called
1C	EE18	JPN IRQ → 'h18	Jump if not IRQ
1D	A004	SCR CR0 → 'h04	Set CR, disable CI
1E	E41E	JPN COR → 'h1E	Jump if not COR
1F	FF00	JMP UNC → 'h00	Jump to Init

Notes:
1. Faster ECB routines can be written by the user if needed.
2. The active Key (K0, K1, K2, K3) is selected by the CR register.
3. The Cipher-text Input Port is not disabled until the interrupt routine is reached.

CIPHER BLOCK CHAINING MODE (ENCRYPT)

This routine provides the Cipher Block Chaining (CBC) encrypt mode of operation as specified by FIPS PUB 81. CBC mode always uses 64-bit blocks of data, a 64-bit Initial Variable (IV) and a 64-bit Key Variable. The routine takes data from the Plain-text Input Port and performs an exclusive-OR function with the IV, and moves the result to the DES Unit for encryption. Once the data is encrypted, it is moved to the Cipher-text Output Port and saved temporarily in the R2 Data Register to be used as the next IV. The routine will not respond to interrupts on IRQ until the Cipher-text Output Buffer is empty. Unless interrupted, the routine will continuously repeat.

TABLE 18. CIPHER BLOCK CHAINING MODE (ENCRYPT)

Address	Data	Mnemonic	Comments
20	4022	MOVE R0 → R2, R2	Move IV to R2
21	E025	JPN PIA → 'h25	Jump if not PIA
22	6C2F	XOR PI^R2 → DI	XOR PI and IV, Encrypt
23	4FD2	MOV DO → CO, R2	Move result to CO, R2
24	D400	CRI RET →	
25	EE21	JPN IRQ → 'h21	Jump if not IRQ
26	FF15	JMP UNC → 'h15	Complete Interrupt
27	FF00	JMP UNC → 'h00	Never Used

Notes:
1. Faster CBC routines can be written by the user if needed.
2. The active Key is selected by the CR register.
3. Active I/O buffers must be enabled in CR.

CIPHER BLOCK CHAINING MODE (DECRYPT)

This routine provides the Cipher Block Chaining (CBC) decrypt mode of operation as specified by FIPS PUB 81. CBC mode always uses 64-bit blocks of data, a 64-bit Initial Variable (IV) and a 64-bit Key Variable. The routine takes data from the Cipher-text Input Port and performs an exclusive-OR function with the IV, and moves the result to the DES Unit for encryption. Once the data is encrypted, it is moved to the Cipher-text Output Port and saved temporarily in the R2 Data Register to be used as the next IV. The routine will not respond to interrupts on IRQ until the Plain-text Output Buffer is empty. Unless interrupted, the routine will continuously repeat.

TABLE 19. CIPHER BLOCK CHAINING MODE (DECRYPT)

Address	Data	Mnemonic	Comments
28	4011	MOVE RO → R1, R1	Move IV to R2
29	E12E	JPN CIA → 'h2E	Jump if not CIA
2A	4DF3	MOV CI → DI, R3	Decrypt CI
2B	6F1C	XOR DO^R1 → PO	XOR DO AND IV
2C	4311	MOV R3 → R1, R1	Move new IV to R1
2D	D400	CRI RET →	Return if Called
2E	EE29	JPN IRQ → 'h29	Jump if not IRQ
2F	FF1D	JMP UNC → 'h1D	Complete Interrupt

Notes:
1. Faster CBC routines can be written by the user if needed.
2. The active Key is selected by the CR register.
3. Active I/O buffers must be enabled in CR.

CIPHER FEEDBACK MODE (ENCRYPT)

This routine provides the Cipher Feedback (CFB) encrypt mode of operation as specified by FIPS PUB 81. Unless interrupted, the routine will continuously repeat.

TABLE 20. CIPHER FEEDBACK MODE (ENCRYPT)

Address	Data	Mnemonic	Comments
30	4011	MOVE R0 → R1, R1	Move IV to R1
31	E036	JPN PIA → 'h36	Jump if not PIA
32	41FF	MOV R1 → DI, DI	Move R1 to DES
33	6CF2	XOR PI^DO → R2	XOR PI and DES Output
34	42DD	MOV R2 → CO, CO	Move R2 to CO
35	2121	BSH R1^R2 → R1	Create next IV
36	EE31	JPN IRQ → 'h31	Jump if not IRQ
37	FF15	JMP UNC → 'h15	Complete Interrupt

Notes:
1. Faster CFB routines can be written by the user if needed.
2. The active Key is selected by the CR register.
3. Active I/O buffers must be enabled in CR.

CIPHER FEEDBACK MODE (DECRYPT)

This routine provides the Cipher Feedback (CFB) decrypt mode of operation as specified by FIPS PUB 81. Unless interrupted, the routine will continuously repeat.

TABLE 21. CIPHER FEEDBACK MODE (DECRYPT)

Address	Data	Mnemonic	Comments
38	4011	MOVE R0 → R1, R1	Move IV to R1
39	E13E	JPN CIA → 'h3E	Jump if not PIA
3A	41FF	MOV R1 → DI, DI	Move R1 to DES
3B	4D22	MOV CI → R2, R2	Move CI to R2
3C	62FC	XOR R2^DO → PO	XOR R2 and DES Output
3D	2121	BSH R1^R2 → R1	Create next IV
3E	EE39	JPN IRQ → 'h39	Jump if not IRQ
3F	FF1D	JMP UNC → 'h1D	Complete Interrupt

Notes:
1. Faster CFB routines can be written by the user if needed.
2. The active Key is selected by the CR register.
3. Active I/O buffers must be enabled in CR.

OUTPUT FEEDBACK MODE (ENCRYPT)

This routine provides the Output Feedback (OFB) encrypt mode of operation as specified by FIPS PUB 81. Unless interrupted, the routine will continuously repeat.

TABLE 22. OUTPUT FEEDBACK MODE (ENCRYPT)

Address	Data	Mnemonic	Comments
40	4011	MOVE R0 → R1, R1	Move IV to R1
41	E046	JPN PIA → 'h3E	Jump if not PIA
42	41FF	MOV R1 → DI, DI	Move R1 to DES
43	4F22	MOV DO → R2, R2	Move DO to R2
44	6C2D	XOR PI^R2 → CO	XOR PI and R2
45	2121	BSH R1^R2 → R1	Create next IV
46	EE41	JPN IRQ → 'h41	Jump if not IRQ
47	FF15	JMP UNC → 'h1D	Complete Interrupt

Notes:
1. Faster OFB routines can be written by the user if needed.
2. The active Key is selected by the CR register.
3. Active I/O buffers must be enabled in CR.

OUTPUT FEEDBACK MODE (DECRYPT)

This routine provides the Output Feedback (OFB) Decrypt mode of operation as specified by FIPS PUB 81. Unless interrupted, the routine will continuously repeat.

TABLE 23. OUTPUT FEEDBACK MODE (DECRYPT)

Address	Data	Mnemonic	Comments
48	4011	MOVE R0 → R1, R1	Move IV to R1
49	E14E	JPN CIA → 'h4E	Jump if not PIA
4A	41FF	MOV R1 → DI, DI	Move R1 to DES
4B	4F22	MOV DO → R2, R2	Move DO to R2
4C	6D2C	XOR CI^R2 → PO	XOR CI and DES Output
4D	2121	BSH R1^R2 → R1	Create next IV
4E	EE49	JPN IRQ → 'h49	Jump if not IRQ
4F	FF1D	JMP UNC → 'h1D	Complete Interrupt

Notes:
1. Faster 0FB routines can be written by the user if needed.
2. The active Key is selected by the CR register.
3. Active I/O buffers must be enabled in CR.

LOAD KEY VARIABLES FROM AUXILIARY PORT

This routine is used to load Key Variables from the Auxiliary Input Port to the Key Registers. The routine is designed to load Key Register 0 first, followed by Key Register 1. Each Key Variable is 64 bits long, and is loaded through the Auxiliary Input Port serially. While the routine is in progress, the LOADKEY output pin will be active.

TABLE 24. LOAD KEY VARIABLES FROM AUXILIARY PORT

Address	Data	Mnemonic	Comments
50	A030	SCR CR0 → 'h30	Set CR0
51	FE00	JMP IRQ → 'h00	Jump if IRQ
52	E251	JPN AIA → 'h51	Jump if no Aux Data
53	4E88	MOV AI → K0, K0	Move Key to K0 Register
54	FE00	JMP IRQ → 'h00	Jump if IRQ
55	E255	JPN AIA → 'h55	Jump if no Aux Data
56	4E99	MOV AI → K1, K1	Move Key to K1
57	FF60	JMP UNC → 'h60	Jump to IV Load Code

Notes: 1. The routine does not check the key parity.
2. A bug exists in the code at location 'h55.

LOAD KEY VARIABLES FROM PLAIN-TEXT PORT

This routine is used to load Key Variables from the Plain-text Input Port to the Key Registers. Key Register 0 will be loaded first, followed by Key Register 1. Each Key Variable is 64 bits long, and is loaded through the Plain-text Input Port using the word-size parameter in the Control Register. While the routine is in progress, the LOADKEY output pin will be active.

TABLE 25. LOAD KEY VARIABLES FROM PLAIN-TEXT PORT

Address	Data	Mnemonic	Comments
58	A028	SCR CR0 → 'h28	Enable PI, Loadkey
59	FE00	JMP IRQ → 'h00	Jump if IRQ
5A	E059	JPN PIA → 'h59	Jump if no Plain-text
5B	4C88	MOV PI → K0, K0	Move Key to K0 Register
5C	FE00	JMP IRQ → 'h00	Jump if IRQ
5D	E05C	JPN PIA → 'h5C	Jump if no Plain-text
5E	4C99	MOV PI → K1, K1	Move Key to K1 Register
5F	FF64	JMP UNC → 'h64	Jump to IV Load Code

Notes: 1. The routine does not check the key parity.

LOAD INITIAL VECTOR FROM AUXILIARY PORT

The Load IV routine is used to load a 64-bit IV from the Auxiliary Input Port and move it to the R0 Data Register. Once the transfer is complete, the routine branches to address 'h7E, where it waits until the IRQ pin becomes active.

TABLE 26. LOAD INITIAL VECTOR FROM AUXILIARY PORT

Address	Data	Mnemonic	Comments
60	FE00	JMP IRQ → 'h00	Jump if IRQ
61	E260	JNP AIA → 'h60	Jump if not AIA
62	4E00	MOV AI → R0, R0	Move IV to R0
63	FF7E	JMP UNC → 'h7E	Jump to 7E

Notes: 1. Only one 64-bit IV is loaded.

LOAD INITIAL VECTOR FROM PLAIN-TEXT PORT

The Load IV routine is used to load a 64-bit IV from the Plain-text Input Port and move it to the R0 Data Register. Once the transfer is complete, the routine branches to address 'h7E, where it waits until the IRQ pin becomes active.

TABLE 27. LOAD INITIAL VECTOR FROM PLAIN-TEXT PORT

Address	Data	Mnemonic	Comments
64	FE00	JMP IRQ → 'h00	Jump if IRQ
65	E064	JNP PIA → 'h64	Jump if not PIA
66	4C00	MOV PI → R0, R0	Move IV to R0
67	FF7E	JMP UNC → 'h7E	Jump to 7E

Notes: 1. Only one 64-bit IV is loaded.

LOAD USER PROGRAM FROM AUXILIARY PORT

This routine is used to load the user program memory with data from the Auxiliary Input Port.

TABLE 28. LOAD USER PROGRAM FROM AUXILIARY PORT

Address	Data	Mnemonic	Comments
68	E26A	JPN AIA → 'h6A	Jump if no Aux Data
69	BE00	LDP AI →	Load RAM from AI
6A	FE68	JMP IRQ → 'h68	Jump if IRQ
6B	D200	CRI Init →	Jump to Init

Notes: 1. Routine does not keep track of number of words loaded.

LOAD USER PROGRAM FROM PLAIN-TEXT PORT

This routine is used to load the user program memory with data from the Plain-text Port. The data is loaded two words at a time.

TABLE 29. LOAD USER PROGRAM FROM PLAIN-TEXT PORT

Address	Data	Mnemonic	Comments
6C	E06E	JPN PIA → 'h6E	Jump if no Plain-text
6D	BC00	LDP PI →	Load RAM from PI
6E	FE6C	JMP IRQ → 'h6C	Jump if IRQ
6F	D200	CRI INIT →	Jump to Init

Notes: 1. Routine does not keep track of number of words loaded. If more words are loaded than the space available, then the extra words will be ignored.

Bypass Mode (Bidirectional)

The bypass routine is provided to support data transfers from the Plain-text Port to the Cipher-text Port (and vice versa) where no cipher function is used. While the bypass routine is running, the BYPASS output pin will be active.

TABLE 30. BYPASS MODE (BIDIRECTIONAL)

Address	Data	Mnemonic	Comments
70	A04F	SCR CR0 → 'h4F	Enable all Data Buffers
71	E074	JPN PIA → 'h74	Jump if no Plain-text
72	4CDD	MOV PI → CO, CO	Bypass PI to CO
73	D400	CRI RET →	Return if Called
74	E177	JPN CIA → 'h77	Jump if no Cipher-text
75	4DCC	MOV CI → PO, PO	Bypass CI to PO
76	D400	CRI RET →	Return if Called
77	EE71	JPN IRQ → 'h71	Jump if no Interrupt
78	A045	SCR CR0 → 'h45	Turn-off Data Buffers
79	E479	JPN POR → 'h79	Wait for P-out Empty
7A	E57A	JPN COR → 'h7A	Wait for C-out Empty
7B	FF00	JMP UNC → 'h00	Jump to Interrupt

Notes: 1. This is the default routine upon power-up.
2. This routine can be called from a user program.
3. Routine waits until data buffers are empty before jumping to the interrupt routine.

SYSTEM PURGE

This routine is used to completely erase and initialize the data flow area of the device. It does not effect the RISC Sequencer or its CR register. The CR Register bits 11 and 12 provide control over the asynchronous reset lines which go to all data areas of the device.

TABLE 31. SYSTEM PURGE

Address	Data	Mnemonic	Comments
7C	A260	SCR CR2 → 'h60	Start Reset
7D	A250	SCR CR2 → 'h50	End Reset
7E	EE7E	JPN IRQ → 'h7E	Wait for IRQ
7F	FF00	JMP UNC → 'h00	Return to Int Routine

Notes: 1. Bits 3 and 4 of CR2 control reset signal override.
2. After system purge is completed, Keys and IV must be reloaded.

FIGURE 2. INITIALIZATION PROCEDURE

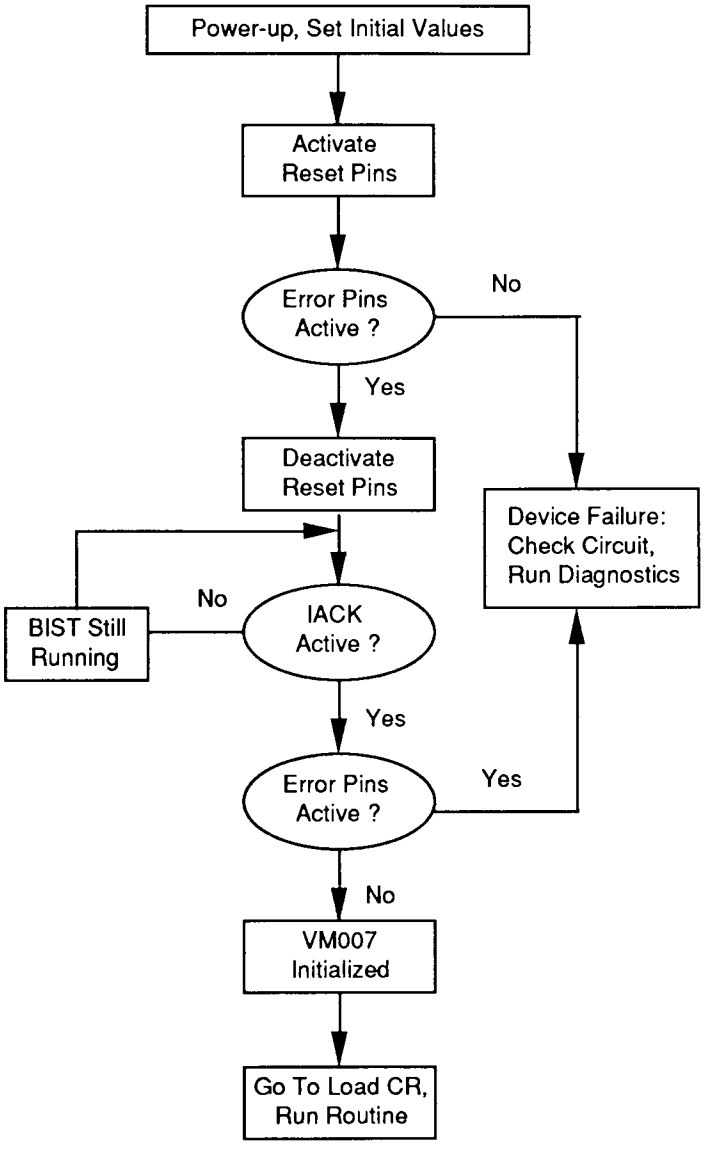
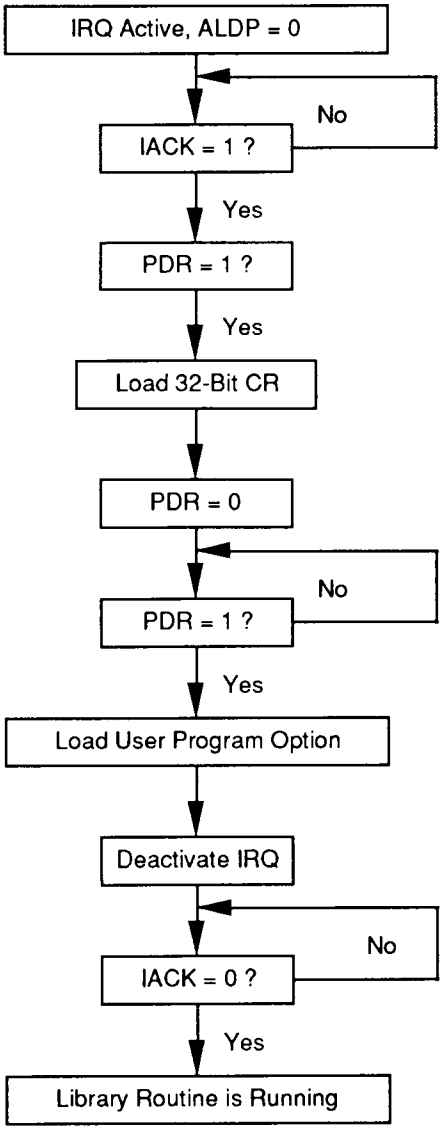


FIGURE 3. LOAD CONTROL REGISTER RUN LIBRARY ROUTINE



AC CHARACTERISTICS: TA = –55°C to +125°C, VDD = 5 V ±10%, VSS = 0 V

Symbol	Parameter	Min	Max	Unit	Conditions (See Note)
tDS	Data Setup Time	10		ns	
tDH	Data Hold Time	10		ns	
tDRI	Data Request goes Inactive Time	7	40	ns	
tSH	STRB Time High	10		ns	
tSL	STRB Time Low	10		ns	
tDAI	Data Available goes Inactive Time	7	40	ns	
tOELF	Output Enable Low to Bus Floating		22	ns	
tOEHD	Output Enable High to Bus Driven		19	ns	
tDR	Clock to Data Request Rising		37	ns	
tDA	Clock to Data Available Rising		40	ns	
tPS	Port Select Setup	15		ns	
tPSH	Port Select Hold	10		ns	
tRAS	RADD Setup	15		ns	
tRAH	RADD Hold	10		ns	
tCKH	CLK width High	10		ns	
tCKL	CLK width Low		20	ns	
tC	CLK Period	30		ns	
tIRQH	IRQ Hold	10		ns	
tIAH	IACK High from CLK High		10	ns	
tIAL	IACK Low from CLK High		10	ns	
tERR	ERROR pins active from CLK High		10	ns	
tERRG	ERROR pins Inactive from CLK High	7	15	ns	
tIRQS	IRQ Setup	10		ns	

Max = 5.5 V, +125°C. Min = 4.5 V, –55°C.
Note: All output conditions are measured under a 50 pF load.

FIGURE 4. READ DATA FROM PLAIN-TEXT/CIPHER TEXT PORT

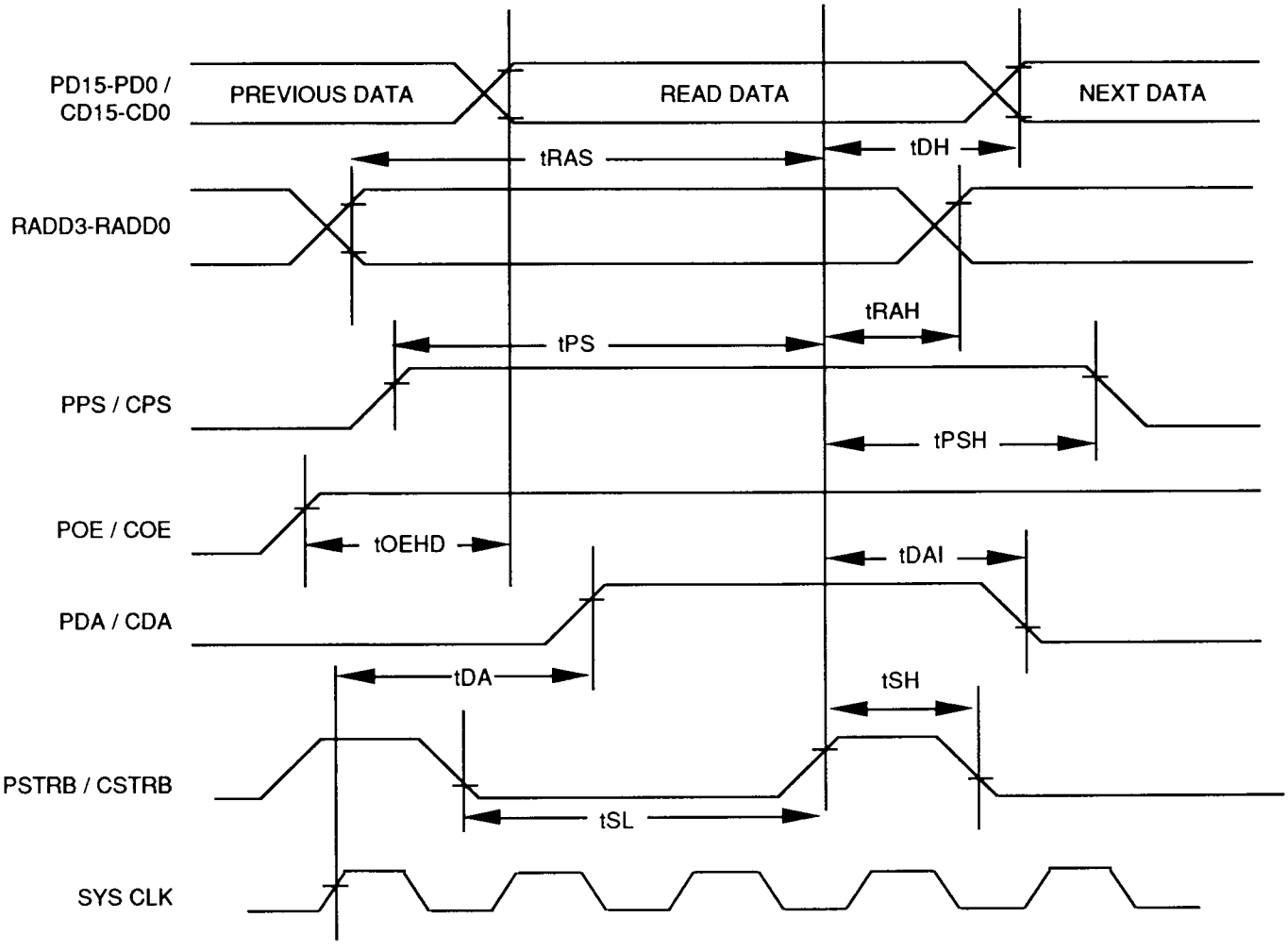


FIGURE 5. WRITE DATA TO PLAIN-TEXT/CIPHER-TEXT PORT

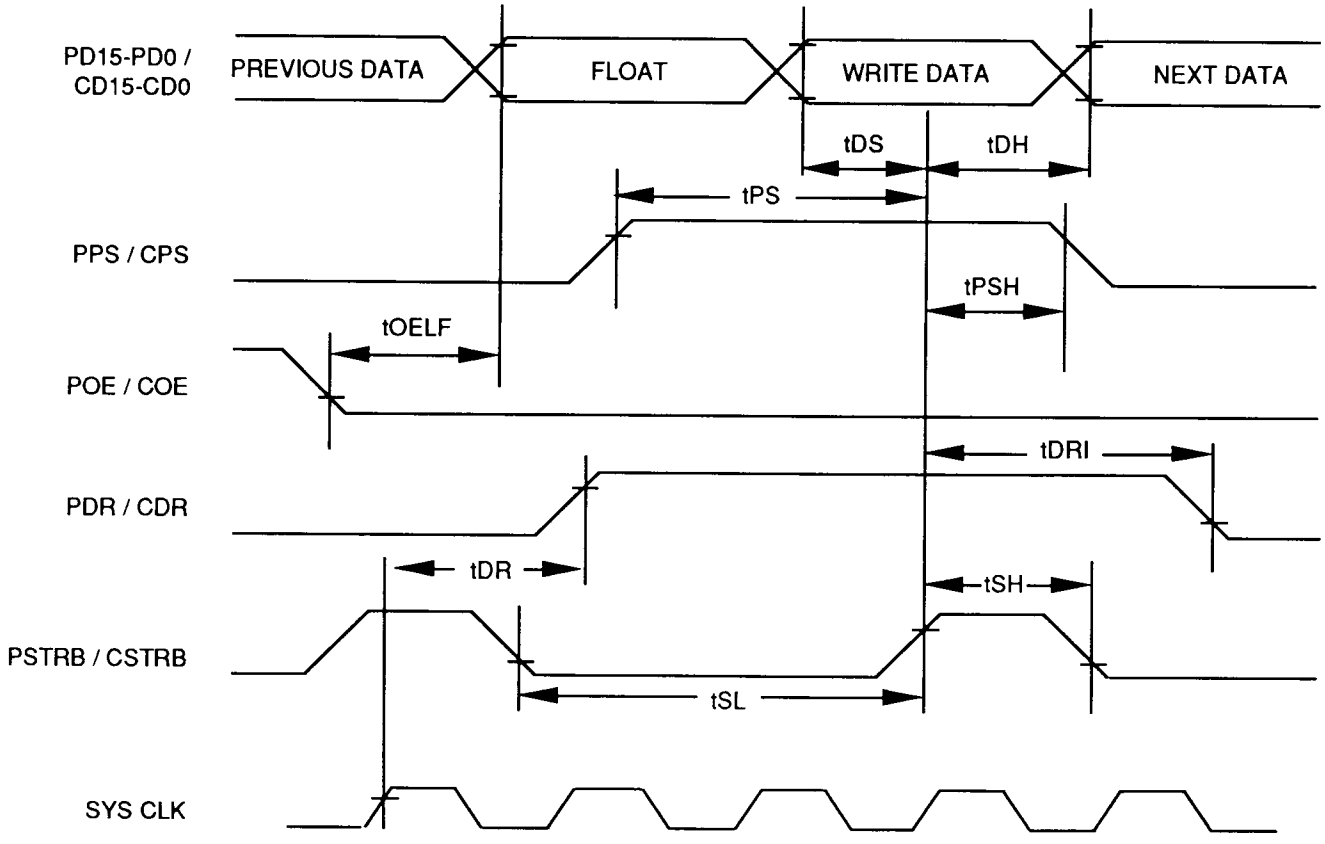
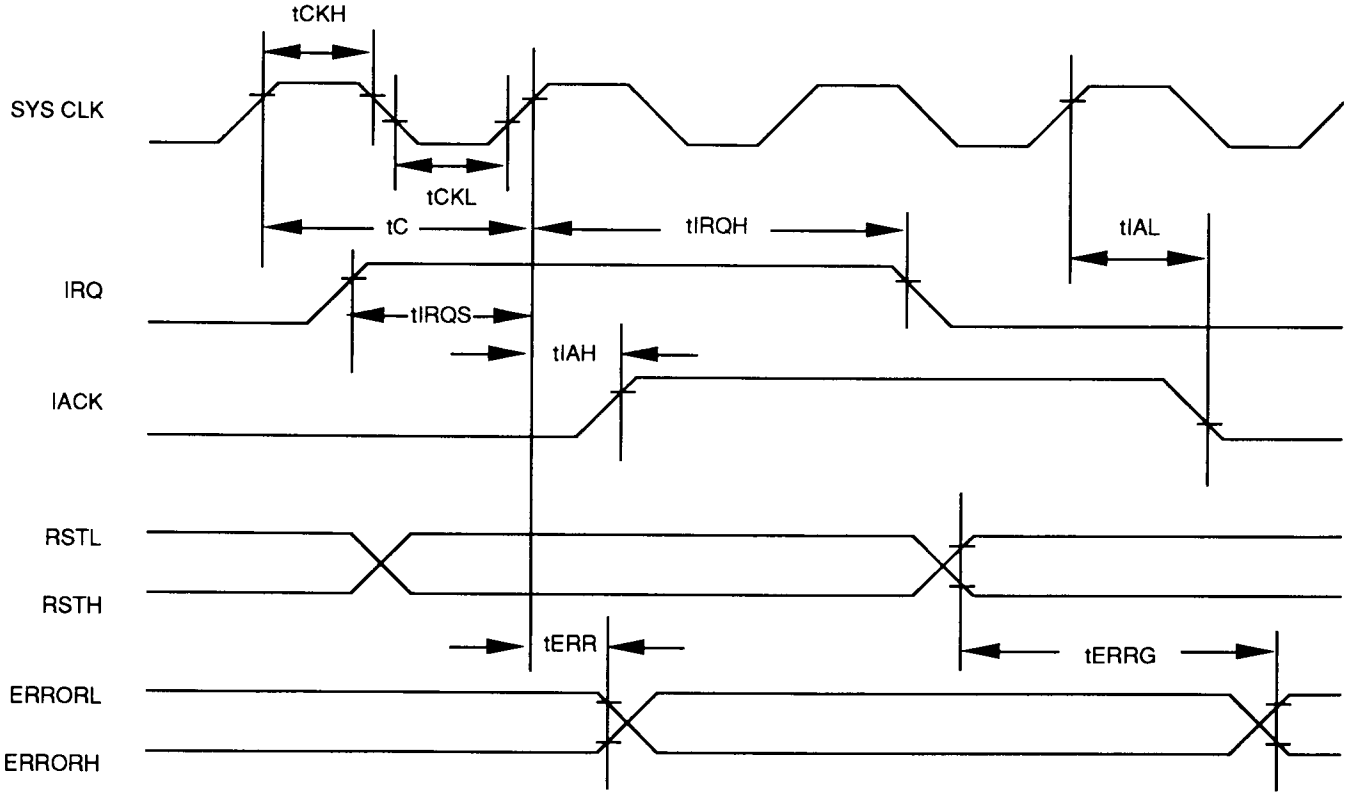


FIGURE 6. SYSTEM INTERFACE



ABSOLUTE MAXIMUM RATINGS

Ambient Operating Temperature	See "Ordering Information"
Storage Temperature without Bias	–65°C to +150°C
Supply Voltage to Ground	–0.5 V to 7.0 V
Applied Output Voltage	–0.5 V to VDD + 0.3 V
Applied Input Voltage	–0.5 V to VDD + 0.3 V

Stresses above those listed may cause permanent damage to the device. These are stress ratings only. Functional operation of this device at these or any other conditions above those indicated in this data sheet is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

DC CHARACTERISTICS: TA = –55°C to +125°C, VDD = 5 V ±10%, VSS = 0 V

Symbol	Parameter	Min	Max	Unit	Conditions
VIL	Input Low Voltage	–0.5	0.8	V	TTL Level Inputs
VIH	Input High Voltage	2	VDD + 0.5	V	TTL Level Inputs
VOL	Output Low Voltage		0.4	V	IOL = 2mA
VOH	Output High Voltage	2.4		V	IOH = –2mA
ILI	Input Leakage Current	–10	10	µA	Note 1
IIL	Input Leakage Current	–250	–10	µA	Note 2
IHI	Input Leakage Current	–10	10	µA	Note 3
IIH	Input Leakage Current	10	250	µA	Note 4
IOZ	Three-State Output Leakage Current	–10	10	µA	Note 5
IDDS	Static Power Supply Current		1	mA	
CI	Input or I/O Capacitance		15	pF	
CO	Output Capacitance		15	pF	

Notes: 1. Pins: CLK, –RSTL, IRQ, POE, PSTRB, PPS, RADD1, RADD2, RADD3, RADD4, ASTRB, APS, AD, ALDP, CPS, CSTRB, COE.
2. Pins: RSTH.
3. Pins: CLK, IRQ, POE, PSTRB, PPS, RADD1, RADD2, RADD3, RADD4, ASTRB, APS, AD, ALDP, CPS, CSTRB, COE, RSTH.
4. Pins: –RSTL.
5. Pins: PD1-PD16, CD1-CD16.

VLSI CORPORATE OFFICES

CORPORATE HEADQUARTERS • COMMUNICATIONS PRODUCTS DIVISION AND SPECIAL PRODUCTS DIVISION
VLSI Technology, Inc. • 1109 McKay Drive • San Jose, CA 95131 • 408-434-3100

PERSONAL COMPUTER PRODUCTS DIVISION AND GOVERNMENT PRODUCTS DIVISION
VLSI Technology, Inc. • 8375 South River Parkway • Tempe, AZ 85284 • 602-752-8574

VLSI SUBSIDIARY

COMPASS DESIGN AUTOMATION, INC.
1865 Lundy Avenue • San Jose, CA 95131 • 408-433-4880

VLSI SALES OFFICES AND TECH CENTERS

ARIZONA
8375 South River Parkway
Tempe, AZ 85284
602-752-6450
FAX 602-752-6001

CALIFORNIA
1110 Ringwood Court
San Jose, CA 95131
408-922-5200
FAX 408-922-5252
Mail:
1109 McKay Drive
San Jose, CA 95131

6345 Balboa Blvd.,
Building 1, Suite 100
Encino, CA 91316
818-609-9981
FAX 818-609-0535

30 Corporate Park,
Stes. 100-102
Irvine, CA 92714
714-250-4900
FAX 714-250-9041

FLORIDA
2200 Park Central N., Ste. 600
Pompano Beach, FL 33064
305-971-0404
FAX 305-971-2086

GEORGIA
3200 Peachtree Industrial Blvd.
Duluth, GA 30136
404-476-8574
FAX 404-476-3790

ILLINOIS
3100 Higgins Rd., Ste. 155
Hoffman Estates, IL 60195
708-884-0500
FAX 708-884-9394

MARYLAND
8424 Veterans Highway
Millersville, MD 21108
301-987-8777
FAX 301-987-4489

MASSACHUSETTS
261 Ballardvale St.
Wilmington, MA 01887
508-658-9501
FAX 508-657-6420

NEW JERSEY
311C Enterprise Dr.
Plainsboro, NJ 08536
609-799-5700
FAX 609-799-5720

NORTH CAROLINA
1000 Park Forty Plaza, Ste. 300
Durham, NC 27713
919-544-1891/92
FAX 919-544-6667

TEXAS
850 E. Arapaho Rd., Ste. 270
Richardson, TX 75081
214-231-6716
FAX 214-669-1413

WASHINGTON
405 114th Ave. SE, Ste. 300
Bellevue, WA 98004
206-453-5414
FAX 206-453-5229

FRANCE
2, Allee des Garays
F-91124 Palaiseau Cedex
France
1-69 93 26 00
FAX 1-64 47 04 80

GERMANY
Rosenkavalierplatz 10
D-8000 Muenchen 81
Germany
89-92795-0
FAX 89-92795-145

HONG KONG
Shui On Centre 1504-07
6-8 Harbour Road
Wanchai, Hong Kong
852-802-7755
FAX 852-802-7959

ITALY
Italia S.R.L.
Centro Direzionale Colleoni
Palazzo Cassiopeia, 3
I-20041 Agrate Brianza (MI)
39-6056791
FAX 39-6056808

JAPAN
Shuwa-Kioicho TBR Bldg., #101
Kojimachi 5-7, Chiyoda-Ku
Tokyo, Japan 102
03-3239-5211
FAX 03-3239-5215

Shinsaibashi MID Bldg., 7F
Minami Senba 3-2-29
Chuo-ku, Osaka, 542, Japan
06-243-6041
FAX 06-243-6960

TAIWAN
Unit 7, 7th Floor, Lotus Bldg.
136 Jen-Ai Rd., Section 3
Taipei, Taiwan, R.O.C.
886-2-325-4422
FAX 886-2-325-4411

UNITED KINGDOM
486-488 Midsummer Blvd.
Saxon Gate West, Central Milton
Keynes, MK9 2EQ
United Kingdom
09 08/66 75 95
FAX 09 08/67 00 27

VLSI SALES OFFICES

ALABAMA
2614 Artie St., Ste. 36
Huntsville, AL 35805
205-539-5513
FAX 205-536-8622

CONNECTICUT
850 North Main St., Bldg. 1, 2C
Wallingford, CT 06492
203-265-6698
FAX 203-265-3653

FLORIDA
Ste. 483, 4th Floor
18167 U. S. 19 North
Clearwater, FL 34624
818-538-0681

MINNESOTA
5831 Cedar Lake Rd.
St. Louis Park, MN 55416
612-545-1490
FAX 612-545-3489

NEW YORK
349 W. Commercial St.
Ste. 2272
E. Rochester, NY 14445
716-586-0670
FAX 716-586-0672

OHIO
4 Commerce Park Square
23200 Chagrin Blvd., Ste.600
Cleveland, OH 44122
216-292-8235
FAX 216-464-7609

OREGON
10300 S.W. Greenburg Rd.,
Ste. 478
Portland, OR 97223
503-244-9882
FAX 503-245-0375

TEXAS
9600 Great Hills Trail,
Ste. 150W
Austin, TX 78759
512-343-8191
FAX 512-343-2759

JAPAN
Shuwa-Kioicho Park Bldg., #503
Kioicho 3-6, Chiyoda-Ku
Tokyo, Japan 102
03-3262-0850
FAX 03-3262-0881

SINGAPORE
627 Aljunied Rd. #05-01
Pacific Building
Singapore 1438
65-742-2314
FAX 65-741-1979

VLSI AUTHORIZED DESIGN CENTERS

COLORADO
SIS MICROELECTRONICS, INC.
Longmont, 303-776-1667

ILLINOIS
ASIC DESIGNS
Naperville, 708-717-5841

MAINE
QUADIC SYSTEMS, INC.
South Portland, 207-871-8244

PENNSYLVANIA
INTEGRATED CIRCUIT
SYSTEMS, INC.
King of Prussia, 215-265-8690

EIRE AND U.K.
PA TECHNOLOGY
Herts, 76-261222

SYMBIONICS
Cambridge, 223-421025

FRANCE
CETIA
Toulon Cedex, 9-42-12005

SOREP
Chateaubourg, 99-623955

INDIA
ARCUS TECHNOLOGY LTD.
Bangalore, 91-812-217307

JAPAN
ADC CORPORATION
Tokyo, 03-3492-1251

LSI SYSTEMS, INC.
Kanagawa, 0462-29-3220

NIPPON STEEL CORPORATION
Tokyo, 03-5566-2141

KOREA
ANAM VLSI DESIGN CENTER
Seoul, 82-2-553-2106

NORWAY
NORKRETS AS
Oslo, 47-2360677/8

VLSI SALES REPRESENTATIVES

ARIZONA
LUSCOMBE ENGINEERING
Scottsdale, 602-949-9333

CALIFORNIA
EMERGING TECHNOLOGY
San Jose, 408-263-9366
Cameron Park, 916-676-4387

COLORADO
LUSCOMBE ENGINEERING
Longmont, 303-772-3342

IDAHO
EMERGING TECHNOLOGY
Boise, 208-378-4680

IOWA
SELTEC SALES
Cedar Rapids, 319-364-7660

KANSAS
ELECTRI-REP
Overland Park, 913-649-2168

MICHIGAN
APPLIED DATA MANAGEMENT
Ann Arbor, 313-741-8558
Ypsilanti, 313-485-2974

MISSOURI
ELECTRI-REP
St. Louis, 314-993-4421

NEW YORK
ADVANCED COMPONENTS
Syracuse, 315-437-6700

OHIO
APPLIED DATA MANAGEMENT
Cincinnati, 513-579-8108

OREGON
ELECTRA TECHNICAL SALES
Beaverton, 503-643-5074

UTAH
LUSCOMBE ENGINEERING
Salt Lake City, 801-565-9885

WASHINGTON
ELECTRA TECHNICAL SALES
Kirkland, 206-821-7442

AUSTRALIA
GEORGE BROWN GROUP
Adelaide, 61-8-352-2222
Brisbane, 61-7-252-3876
Melbourne, 61-3-878-8111
Newcastle, 61-49-69-6399
Perth, 61-9-362-1044
Sydney, 61-2-638-1888

AUSTRIA
THOMAS NEUROTH
Wien, 0043-222-82 56 45

CANADA
DAVETEK MARKETING, INC.
British Columbia, 604-430-3680

INTELATECH, INC.
Mississauga, 416-629-0082

HONG KONG
LESTINA INTERNATIONAL, LTD
Tsimshatsui, 852-7351736

ISRAEL
RDT ELECTRONICS ENG. LTD
Tel-Aviv, 23-4832119

SINGAPORE
DYNAMIC SYSTEMS PTE, LTD
Singapore, 65-742-1986

TAIWAN
PRINCETON TECH CORP.
Taipei, 886-2-917-8856

WEIKENG INDUSTRIAL CO.
Taipei, 886-2-776-3998

THAILAND
TRON ELECTRONICS CO. LTD
Bangkok, 66 2 260-3913

VLSI DISTRIBUTORS

United States represented by **ARROW/SCHWEBER** except where noted

ALABAMA
Huntsville, 205-837-6955

ARIZONA
Phoenix, 602-431-0030

CALIFORNIA
Arrow Pacific, 408-432-7171
Los Angeles, 818-880-9686
Orange County, 714-838-5422
San Diego, 619-565-4800
San Francisco, 408-441-9700

COLORADO
Denver, 303-799-0258

CONNECTICUT
Wallingford, 203-265-7741

FLORIDA
North Florida, 407-333-9300
South Florida, 305-429-8200

GEORGIA
Atlanta, 404-497-1300

ILLINOIS
Chicago, 708-250-0500

INDIANA
Indianapolis, 317-299-2071

IOWA
Cedar Rapids, 319-395-7230

KANSAS
Kansas City, 913-541-9542

MARYLAND
Baltimore, 301-596-7800

MASSACHUSETTS
Boston, 508-658-0900

MICHIGAN
Detroit, 313-462-2290

MINNESOTA
Minnesota, 612-941-5280

MISSOURI
St. Louis, 314-567-6888

NEW JERSEY
Philadelphia, 609-596-8000
North Jersey, 201-227-7880

NEW YORK
Rochester, 716-427-0300
Metro, 516-231-1000

NORTH CAROLINA
Raleigh, 919-876-3132

OHIO
Dayton, 513-435-5563
Cleveland, 216-248-3990

OKLAHOMA
Tulsa, 918-252-7537

OREGON
ALMAC/ARROW
Portland, 503-629-8090

PENNSYLVANIA
Pittsburgh, 412-963-6807

TEXAS
Austin, 512-835-4180
Dallas, 214-380-6464
Houston, 713-530-4700

UTAH
Salt Lake City, 801-973-6913

WASHINGTON
ALMAC/ARROW
Seattle, 206-643-9992
Spokane, 509-924-9500

WISCONSIN
Milwaukee, 414-792-0150

BELGIUM/LUXEMBURG
MICROTRON
Mechelen, 215-212223

CANADA
ARROW/SCHWEBER
Montreal, 514-421-7411
Ottawa, 613-226-6903
Toronto, 416-670-7769
Vancouver, 604-421-2333

SEMAD
Calgary, 403-252-5664
Markham, 416-475-8500
Montreal, 514-694-0860
Ottawa, 613-727-8325
British Columbia, 604-420-9889

DENMARK
DELCO
Lynge, 45 42-189533

ENGLAND
HAWKE COMPONENTS
Bramley, NR Basingstoke
256-880800

KUDOS-THAME LTD
Berks, 734-351010

FINLAND
COMDAX
Helsinki, 80-670277

FRANCE
ASAP s.a.
Montigny-le-Bretonneux,
1-30438233

GERMANY
DATA MODUL GmbH
Muenchen, 089-560170

ELECTRONIC 2000 AG
Muenchen, 089-420010

EAST GERMANY
ZENTRUM MIKROELEKTRONIK
Dresden, 0037-51-588464

ITALY
INTER-REP S.P.A.
Torino, 11-2165901

JAPAN
ASAHI GLASS CO. LTD
Tokyo, 03-3218-5854

TOKYO ELECTRON, LTD
Tokyo, 03-3340-8111

TOMEN ELECTRONICS
Tokyo, 03-3506-3650

NETHERLANDS
TME
Aa Heeswijk-Dinther,
4139-8895

PUERTO RICO
ISLA CARIBE ELECTRO SALES
Guaynabo, 809-720-4430

SWEDEN
TRACO AB
Farsta, 8-930000

SPAIN AND PORTUGAL
SEMICONDUCTORES s.a.
Barcelona, 3-21723 40

SWITZERLAND
DECTRO SWISS ELECTRONIC
DESIGN AG
Zuerich, 0041-1-3868-600

3/92