VLSI Technology

VMS113

Data Sheet

Revision: 2.1

Revision History

Date	Changes	Revision
1/28/99	Baseline Version	2.0
2/5/99	Updated AC Paramters: TADDRH; TDIOH; TRWH	2.1

Table of Contents

1 Introduction

The VMS113 is a high-speed ciphering engine and random number generator that supports the Data Encryption Standard (DES) algorithm as specified by the National Institute of Standards and Technology Federal Information Processing Standards Publication #46-2 (FIPS PUB 46-2). The VMS113 performs single DES at 284 Mbits/second and 2-key triple DES in excess of 100 Mbits/second in both Electronic Code Book and Cipher Block Chaining modes.

The VMS113 includes VLSI Technology's digital non-deterministic randomizer for Initialization Vector (IV) and key generation, and random number seeding.

VMS113 Architecture

Revision 1.0 6/15/95
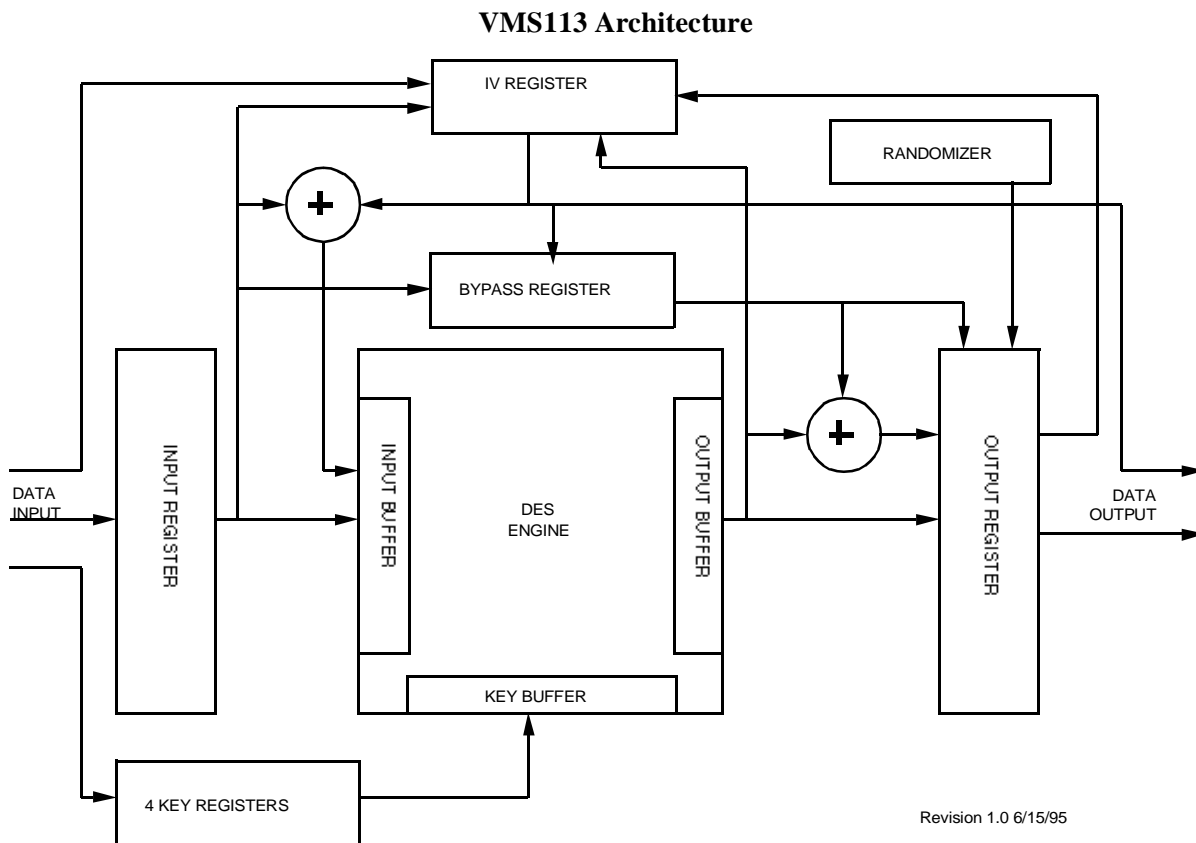
1.1   Features

- Implements FIPS-PUB standard 46-2 Data Encryption Standard (DES)
- Supports Single DES and Triple DES Electronic Codebook (ECB) and Cipher-Block-Chaining (CBC)
- Programmable Bypass
- 16 Bit Bi-directional DATA I/O Port
- Simple register based control
- Clock rate up to 40 Mhz
- Built-in non-deterministic randomizer
- Built-in 4 Key Cache for high speed cryptographic context switching
- Implemented in low power CMOS technology
- Surface Mount 44 pin Plastic Leaded Chip Carrier (PLCC) package

2 Overview

The VMS113 is a high speed ciphering engine that supports the Data Encryption Standard (DES) algorithm as specified by the National Institute of Standards and Technology Federal Information Processing Standards Publication #46-2 (FIPS PUB 46-2). The VMS113 supports single DES Electronic Code Book and Cipher Block Chaining encryption/decryption. The triple DES ECB Mode option uses the following sequence of operation:

Triple DES encryption:

- DES Encrypt w/Key A
- DES Decrypt w/Key B
- DES Encrypt w/Key A

Triple DES decryption:

- DES Decrypt w/Key A
- DES Encrypt w/Key B
- DES Decrypt w/Key A

For CBC mode the IV is wrapped around the three step sequence of Triple DES.

The VMS113 uses a 16 bit bi-directional data bus and appears as a 16 bit peripheral to the host processor. A 5-bit address field is used as the command input and control/status pins are available for host processor control and communication. The VMS 113 is a fully static design and supports clock rates up to 40 Mhz. Pipelined encryption/decryption for continuous blocks of data is implemented for both ECB and CBC modes. The VMS113 also supports a bypass mode (plain/cipher data in, plain/cipher data out) which is cycle consistent with the equivalent encryption/decryption mode.

Two 8-bit status and mode registers are present for current status and configuration/control of the VMS113. The MODE register is used select encrypt/decrypt modes and key usage. The STATUS/CONFIGURATION register is used to update the processor on the current state of the VMS113, set bypass mode, or select the ciphering operational mode; Electronic Codebook or Cipher Block Chaining.

The VMS113 key Cache consists of (4) 56-bit write only registers which allow for high speed key context switching. This multi-key cache will facilitate Single DES operations and Triple DES operations.

The VMS113 also includes VLSI Technology's digital non-deterministic randomizer (patent pending) for Initialization Vector (IV) and key generation, and random number seeding. The randomizer does not require an external seed. The host processor can request and read a random 64-bit word via read-write commands.

The VMS113 is controlled by the host processor via an address field, control/status lines, and data bus. The DATA I/O port is used to input keys, read/write status, input control, and read/write data. The host processor reads, writes, and configures the VMS113 via a 5-bit address field that is decoded by the VMS113 state machine and decoding logic. The VMS113 is memory mapped into the address space. The address command set includes reading the status, writing mode registers, loading cryptographic Keys, and loading and unloading plain and cipher data.

The NRW (not-read/write) and -CS (chip-select) lines control the data flow through the DATA I/O

port. The input and output data registers are used to store complete data blocks to and from the DES core. The BUSY output is used to indicate when a ciphering process is in progress or completed. The IRDY output indicates the VMS113 is ready for input on the DATA I/O port. The ORDY output indicates the VMS113 is ready to output to the DATA I/O port. The RDY output is used to indicate the DATA I/O port is ready to be read or written i.e. the logical "OR" of IRDY and ORDY. The CLOCK input is used to clock in data and synchronize all internal operations to the DES core.

Once the VMS113 is setup, the VMS113 will automatically start a cipher process after the last 16 bit Least Significant Word (LSWord) is written, once the other three data words are written. A start signal is not required to start the cipher process.

The VMS113 is 100% backward pin and software compatible with the VMS110.

3 Register Definitions

The VMS113 is configured and controlled by a set of internal registers as shown below

Internal Registers

DATA I/O REGISTER	64 bits
STATUS/CONFIGURATION	8 BITS
MODE	8 BITS
RANDOMIZER	FLAG
SOFTWARE RESET	16 BITS
IV	64 BITS
KEY 1	64 BITS (56 USED)
KEY 2	64 BITS (56 USED)
KEY 3	64 BITS (56 USED)
KEY 4	64 BITS (56 USED)

The internal registers are accessed through the address pins ADDR[4:0]. The user should refer to "Pipeline Diagram (Single DES)" on page 16 to READ/WRITE to this device when operating as a data pipeline. The following table is given as the internal memory map.

Internal Memory Address Map

Address	Register
00h - 03h	I/O Register Word4 [63:48] - Word1 [15:0] (Read/Write)
04h	Status/Configuration Register (Read/Write)
05h	Mode Register (Write Only)
06h	Randomizer Register (Write Only)
07h	Software Reset Register (Write Only)
08h - 0Bh	Initial Vector (IV) Register [63:48] - [15:0] (Read/Write)
0Ch-0Fh	Reserved
10h-13h	Key 1 Word 4 [63:48] - Key 1 Word 1 [15:0]
14h-17h	Key 2 Word 4 [63:48] - Key 2 Word 1 [15:0]
18h-1Bh	Key 3 Word 4 [63:48] - Key 3 Word 1 [15:0]

Address	Register
1Ch-1Fh	Key 4 Word 4 [63:48] - Key 4 Word 1 [15:0]

3.1 Input/Output Registers (Read/Write)

The input/output registers are accessed through the DATA I/O port interface using the I/O register address. The I/O registers share the same address location, the NRW signal determines which register is accessible. The Output register is accessed during a read only, and the Input register is accessed during a write only. An internal state machine keeps track of the addresses written to for a data transfer. Once the final word, (word 1) is read/written from/to the VMS113, the next encryption operation will begin automatically. Once the output data is read, the following command sequence can be executed:

1. Write data into the VMS113; four 16 bit words.
2. Encrypt/Decrypt operation starts.
3. Read data from the VMS113; four 16 bit words.

The 64-bit read-write Input and Output Registers are setup to appear as four 16 bit words of storage. The Input register is write only and the Output register is read only. The Input and Output registers will be loaded and unloaded with four 16 bit words: Most Significant Words (MSWords) first (WORD 4 is the MSW and WORD 1 is the LSW). The entire 64 bit block must be written or read, partial blocks cannot be processed. The VMS113 will start an encryption/decryption cycle after the LSWord is loaded into the Input register.

The Input and Output registers are considered full when four 16-bit words are present. The I/O registers can be written/read during encryption processing which allows pipelined operation, see "Pipeline Diagram (Single DES)" on page 16. The Output register is considered empty only after words [4:1] are read. The Input register is used for data input only and the Output register is for data output or Randomizer output.

The VMS113 requires four cycles to load four 16-bit blocks of input data, 1 cycle to load the DES engine, eight cycles to encrypt/decrypt the data for single DES, 24 cycles to encrypt/decrypt the data for triple DES, one cycle to load the output register and four cycles to empty the four 16-bit blocks from the output register. This sequence applies to both ECB and CBC modes. In CBC encryption mode the IV, or previous DES output vector, is exclusive OR'd with the input register while loading the DES engine. In CBC decryption mode the IV, or previous DES input vector, is exclusive OR'd with the output register while unloading the DES engine.

Data I/O Bit Descriptions

BITS [63:49]	BITS [47:32]	BITS [31:16]	BITS [15:0]
WORD 4	WORD 3	WORD 2	WORD 1

3.2 Status/Configuration Register (Read/Write)

The contents of the Status/Configuration register can be read or written at any time using the host processor read/write cycle, similar to reading a memory. The Status/Configuration register con-

tents are accessed through the DATA I/O [7:0] data lines. All other DATA I/O bits [15:8] will be set to zero. A software or hardware reset forces all register bits to 0, i.e. 00h

Status/Configuration (READ/WRITE)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	0	BYPASS	BYPASS	CIPHER	BUSY	DRDY

Bits 7-5   Reserved - Always Zero

Bits 4-3   BYPASS - Bypass Select. Both bits set to 1 will enable bypass mode, cipher in => cipher out, plain in => plain out

Bit 2   CIPHER - Cipher Select - The CBC mode will be used when this bit is zero. The ECB mode will be used when this bit is one.

Bit 1   BUSY - Cipher Function Busy - The Busy Bit will be a one when the ciphering DES algorithm is actively encrypting or decrypting data. The Busy bit will return to zero once data has been transferred to the Output Register and the ciphering algorithm is idle.

Bit 0   DRDY - Data Ready - This DRDY bit indicates that the DES engine has data.

3.3 Mode Register (Write Only)

This register can be accessed at anytime. However, if the Mode register is written during a DES processing cycle, the Mode register will be updated after the current DES processing cycle is completed. The Mode register is written as a host processor write cycle similar to writing a memory. The Mode register will be loaded using the data bus DATA I/O [7:0]. All other DATA I/O bits [15:8] will be treated as don't cares (X). A software or hardware reset forces all register bits to 0, i.e. 00h.

Mode (WRITE Only)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
DES MODE	ENCRYPT	Key B [2]	Key B [1]	Key B [0]	Key A [2]	Key A [1]	Key A [0]

Bit 7   DES MODE - 0 for DES (Default), 1 for Triple DES.

Bit 6   ENCRYPT - Encrypt or Decrypt - The DES engine will decrypt data when set to zero and encrypt data when set to one.

Bits 5-3   KEYB[2:0] - Key B Select - Key B select for the VMS113 are written to BIT 5 to BIT 3. This key B is used in Triple mode only. NOTE: If Key B is the same as KEY A in triple DES mode, A Single DES operation will result. However this operation will take 24 cycles.

- 000 - Key 1
- 001 - Key 2
- 010 - Key 3

- 011 - Key 4
- 1XX - Not Used

Bits 2-0   KEYA[2:0] - Key A Select - Key A select for the VMS113 are written to BIT 2 to BIT 0. This key A is used in Triple and single DES modes.

- 000 - Key 1
- 001 - Key 2
- 010 - Key 3
- 011 - Key 4
- 1XX - Not Used

3.4   Randomizer Register (Write only)

A write to the Randomizer Register, any value, will trigger the randomizer to generate a random bit pattern. The Randomizer can be used to generate random numbers for the IV's, generate keys, or generate seeds for another randomization routine. During randomization, the DATA I/O bus is ignored by the VMS113. The randomizer shifts bits into the Output register continuously at the rate of approx. 1MHZ, until the output register is read. The Output register contents are copied to the IV register when the read is issued. The randomization process will continue until the Output register is read and is completely empty. ORDY will go high to indicate that the Randomizer is operating. The Output register should be empty when starting the Randomizer.

When a write to the Randomizer is executed, the state machine will connect the Randomizer to the Output register. The contents of the Output register will be lost once this command is executed. The Randomizer will begin to load random bits into the Output register using its own clock at a rate of 1 MHz or greater. In order to generate a complete 64-bit number the Randomizer must run for a minimum of 64 micro-seconds. The Randomizer can continue to run after the Output register is full which results in more bits shifting through the Output register. The Randomizer will stay connected to the Output register until the output register is read for the first time. At the end of the random number generation the Output register and the IV register will contain a 64 bit random number.

Since the IV is mirroring the Output register, it is possible to continuously read the VI register. This has the effect of accessing the random number stream in real time since over sampling is permitted.

3.5   Software Reset Register (Write only)

When the location of the Software Reset is written, the VMS113 will initiate a software reset for two CLOCK cycles. It forces the selected VMS113 registers to their default configuration i.e. 00h. The DATA I/O bits [15:4] will be treated as don't cares (X) during reset.

Software Reset (WRITE Only)

BIT [15:4]	BIT 3	BIT 2	BIT 1	BIT 0
DON'T CARE	IV RESET	KEY CACHE RESET	STATUS/CONFIG and MODE RESET	DES and I/O RESET

Bit 15-4:   DON'T CARE
Bit 3:   IV RESET - A "1" Resets the IV Register to default, i.e. 00h.
Bit 2:   KEY CACHE RESET - A "1" Resets all Key Registers to default, i.e. 00h.
Bit 1:   STATUS/CONFIGURATION AND MODE REGISTER RESET - A "1" Resets the Status/Configuration and Mode Registers to default, i.e. 00h and also stops the Randomizer if it is running.
Bit 0:   DES ENGINE AND INPUT/OUTPUT REGISTER RESET - A "1" Resets the I/O register to default, i.e. 00h and clears the DES engine and also stops the Randomizer if it is running.

3.6   Initialization Vector (IV) Register (Read/Write)

The IV must be loaded into the VMS113 before the input register is loaded when using CBC mode encryption/decryption. This will ensure that the IV is valid before the DES encryption/decryption cycle starts. The IV is only used in CBC mode encryption or decryption.

When the Randomizer is used to generate a random number, the IV register is loaded with the random number that is generated, overwriting any previous data. However, the reading of the output register is the event that triggers the end of randomization.

3.7   Key Registers (Write Only)

The FIPS PUB 46-2 specifies that one bit in each byte of the Key is used for Parity. Since the VMS113 does not check for parity, bits 0,8,16,24,32,40,48, and 56 are ignored. The Key registers can be loaded in any order at any time. The Keys are accessed via the DATA I/O port 16-bits at time. The VMS113 provides four generic 56 bit key registers to implement a multi-key system. The key cache consists of write only registers that are loaded by selecting the proper address. The key registers must be loaded with sequential writes of four 16 bit words of Key Data (the most significant word is first) with the proper address code. The Mode register will select which key is used by the DES core, the default key is Key[1] for Key A and Key B. A software or hardware reset will zero all key registers otherwise the contents will remain intact.

4 Data Flow
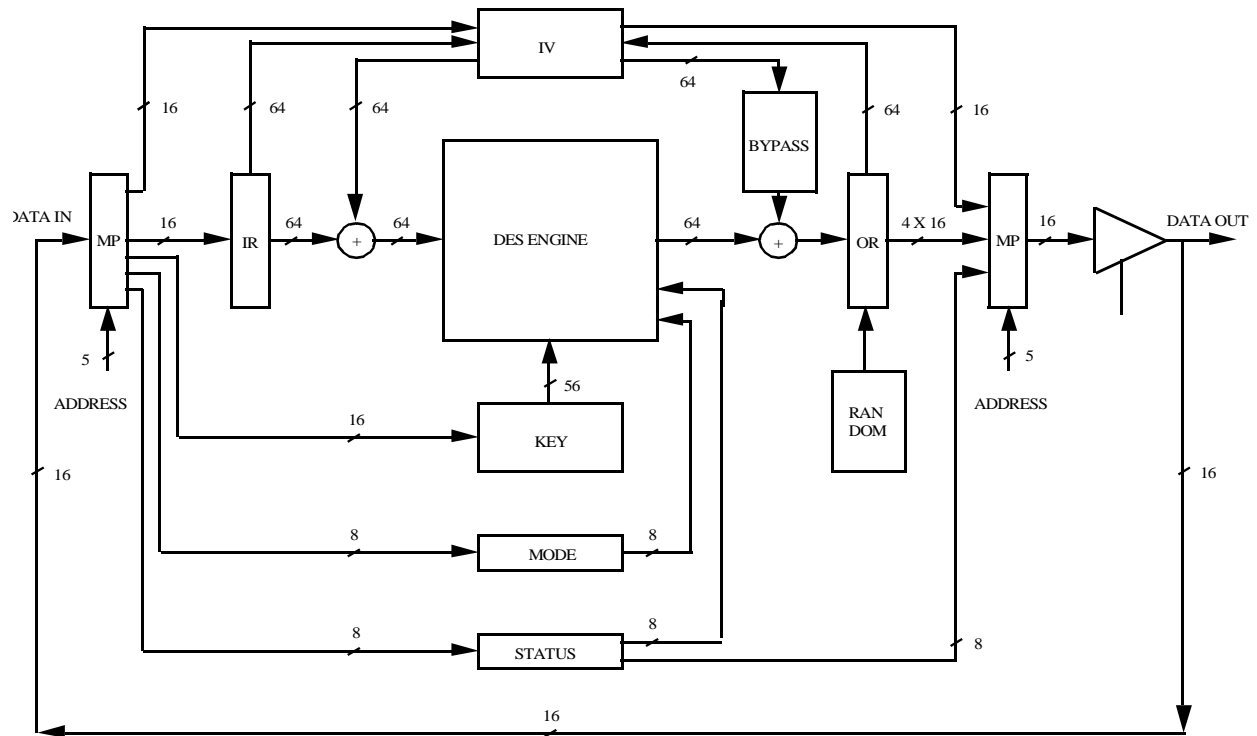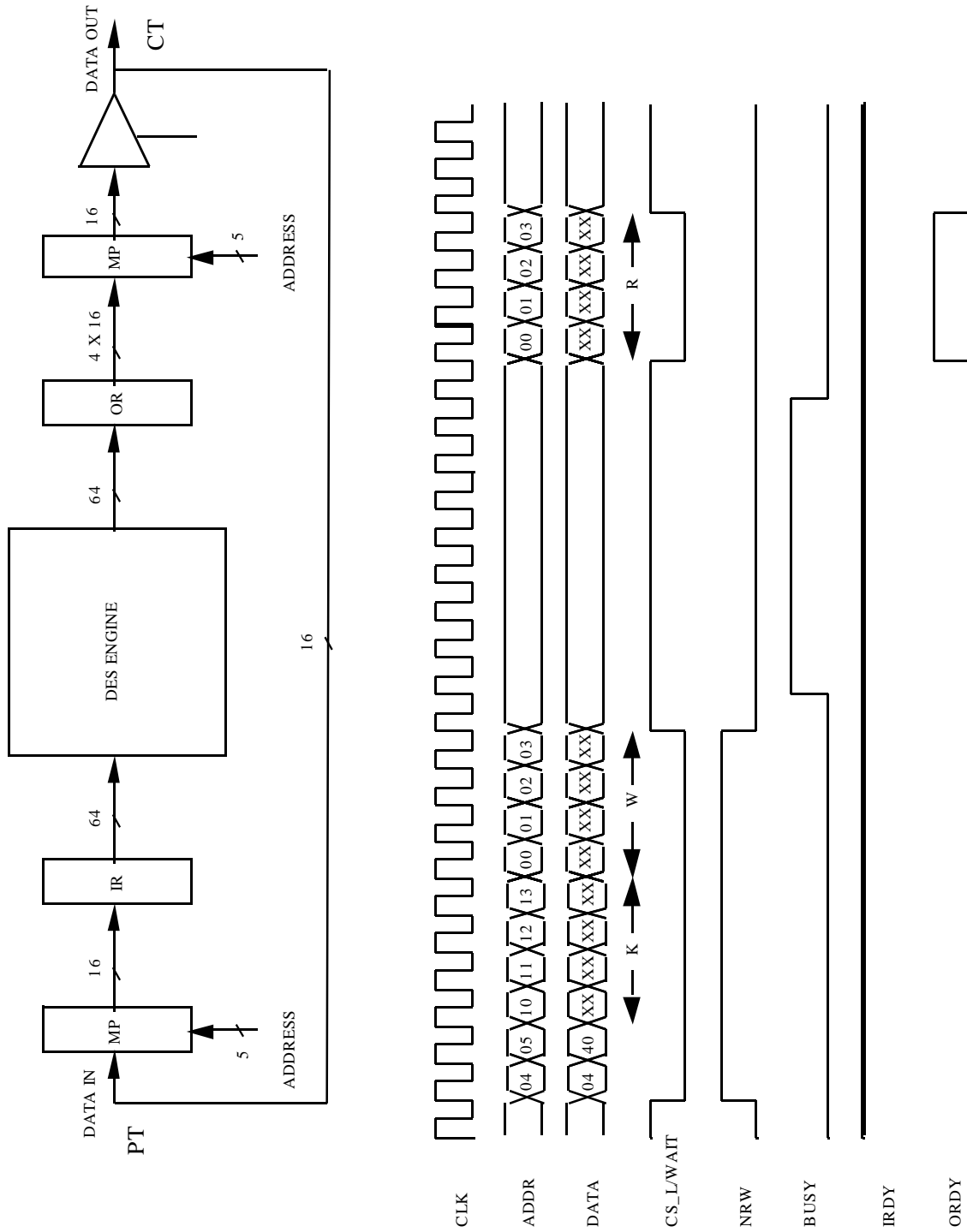
Figure 4 Data Flow Diagram
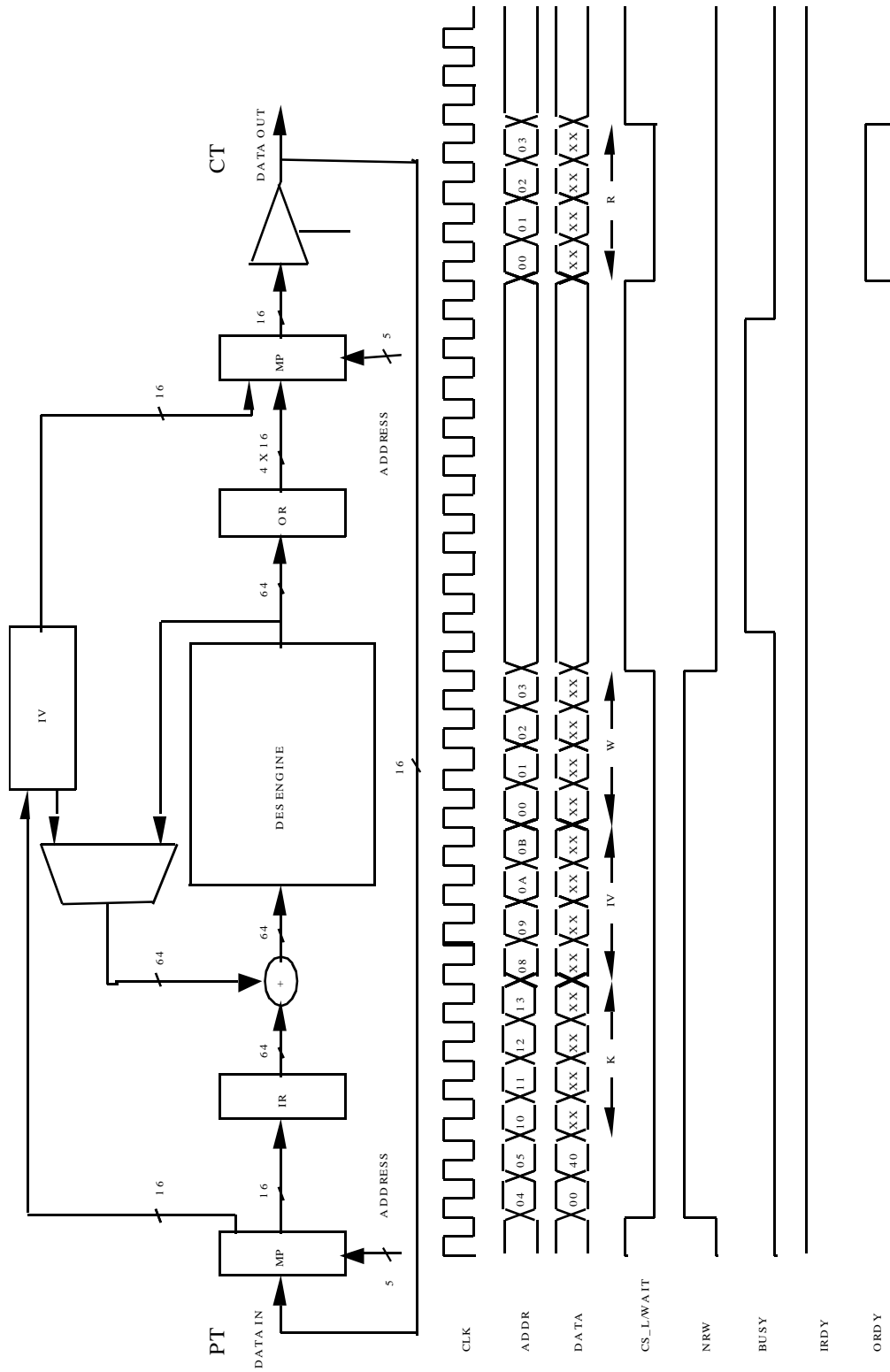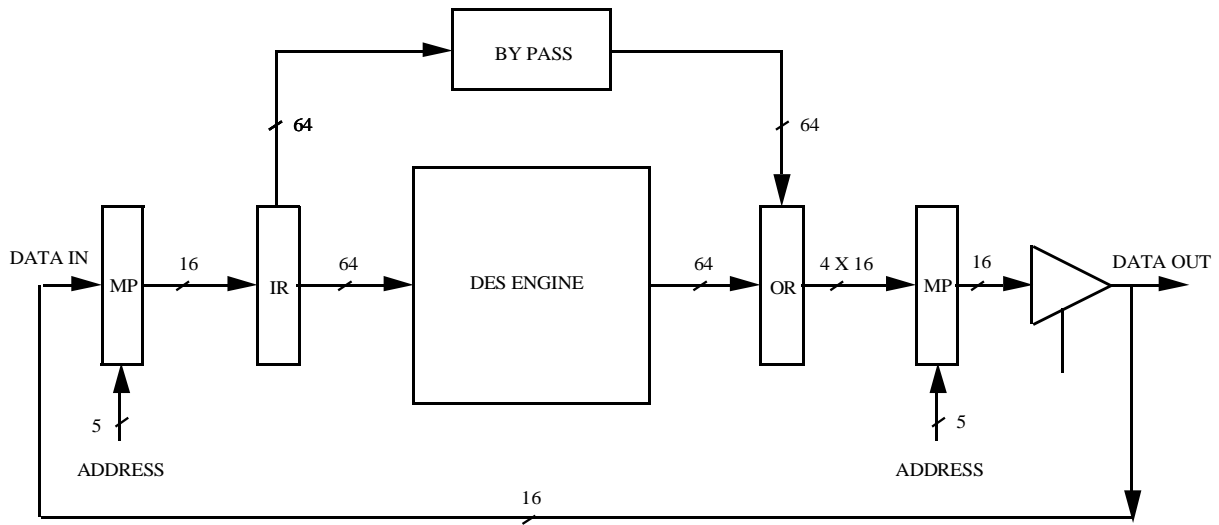
Figure 5 ECB Mode Encryption Timing
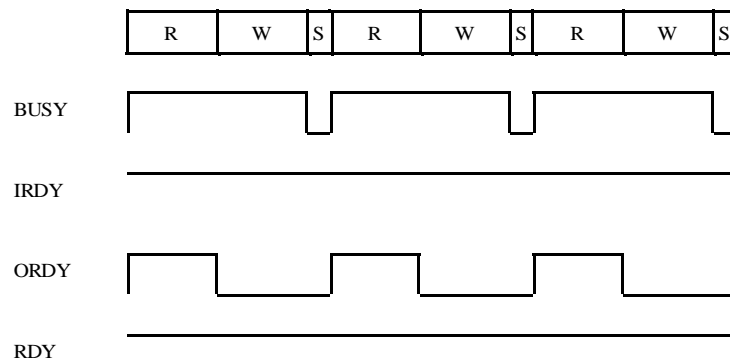
Figure 6 CBC Mode Encryption (Single DES)

Figure 7 CBC Mode Decryption (Single DES)

Figure 8 Bypass Mode

DATA IN · MP · 16 · IR · 64 · DES ENGINE · 64 · OR · 4 X 16 · MP · 16 · DATA OUT

BY PASS · 64 · 64

5 · ADDRESS

5 · ADDRESS

16

Figure 9 Pipeline Diagram (Single DES)

W	E / D	R
W	E / D	R
W	E / D	R
W	E / D	R
W	E / D	R

| R | W | S | R | W | S | R | W | S |

BUSY

IRDY

ORDY

RDY
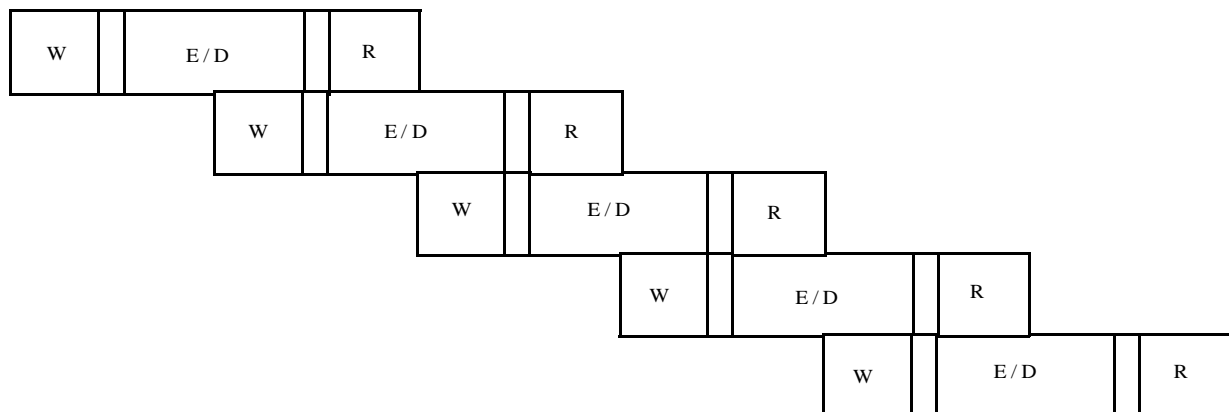
W = Write Cycle   R   = Read Cycle   S = Stall
R = Read Cycle   E/D = Encrypt/Decrypt

Figure 10 Pipeline Operation Detail (Single DES)
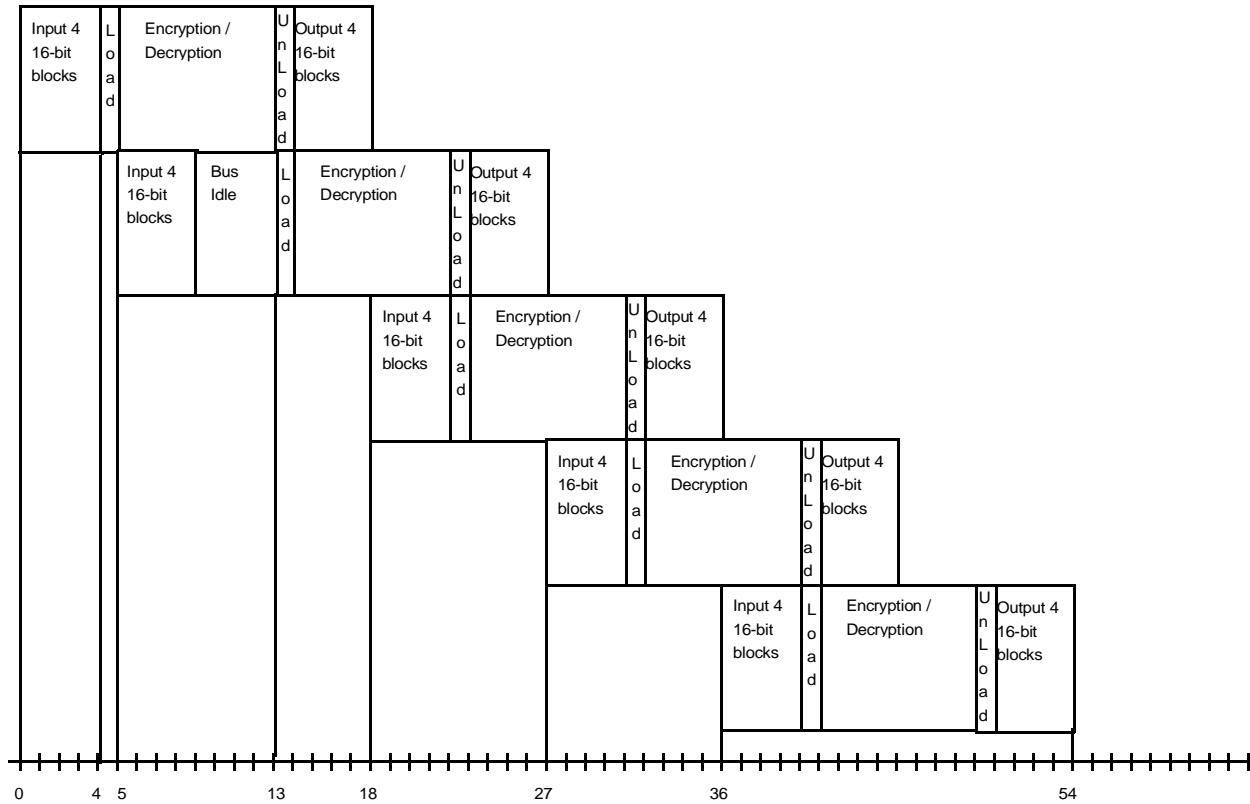
Data throughput for single DES is calculated as follows:

n = number of 64-bit blocks of data

f = frequency in MHz

cycles required = 9*(n+1)

Mbits/second = (64*n)/(9*(n+1)*(1/f)), as n -> • Mbits/second -> f(64/9) or 7.11111*f

NOTE: Triple DES cipher operations require 24 clock cycles instead of 8 clock cycles for single DES ciphers.

Figure 11 Pipeline with bypass (Single DES)

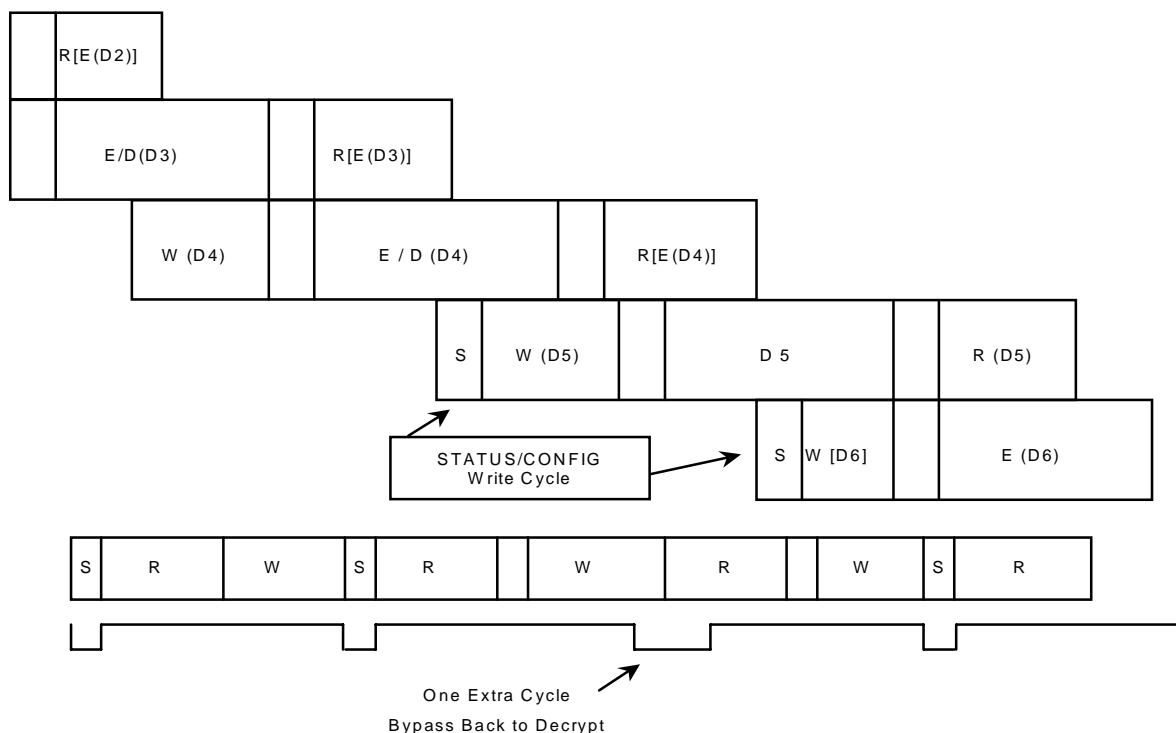## 4.1   Pipeline With Bypass Description

"Pipeline Diagram (Single DES)" on page 16 and "Pipeline Operation Detail (Single DES)" on page 17 show the recommended data access sequence for pipeline operation. To achieve the maximum throughput, a block of data is written into the input register while the DES engine is busy processing the previously entered block of data. Once the engine finishes, the processed (encrypted or decrypted) block of data is unloaded into the output register at the same time the block of data in the input register is loaded into the engine. The processed block of data can then be read from the output register before a new block of data is written into the input register. This read and write sequence takes exactly eight clock cycles. This means the loading/unloading of data to/from the engine takes place right after the LSW is written into the input register. Notice that the engine is always busy except during the load/unload cycles.

With bypass mode, a STATUS/CONFIGURATION write cycle is required before the data to be bypassed is written into the input register. "Pipeline with bypass (Single DES)" on page 18 shows the insertion of this write cycle between the processed block 3 read cycles and the bypassed block 5 write cycles. The last write cycle of block 5 is completed during the unloading cycle of block 4. This results in one extra clock required for the loading of block 5 before the engine starts again. Notice that the BUSY signal is de-asserted for two clock cycles. During the loading of block 5 however, the MSW of the processed block 4 is read from the output register saving one clock cycle. If block 5 is the only block bypassed, this extra cycle can be used for the STATUS/CONFIGURATION write cycle. In this case, one extra clock cycle is not required to start processing block 6.

5 DC Paramaters

DC Parameter

Symbol	Parameter	Min	Max	Units	Notes
VDD	Supply Voltage	VSS-0.3	VSS+7.0	V	1
VIP	Voltage Applied to Any Pin	VSS-0.3	VDD+0.3	V	1
TS	Storage Temperature	-40	+125	×C	1

Recommended DC Operating Conditions

Symbol	Parameter	Min	Max	Units	Notes
VDD	Supply Voltage	4.75	5.25	V	2
VIH	Input HIGH Voltage	2.4	VDD	V	2
VIL	Input LOW Voltage	0	0.8	V	2
T	Operating Temperature	0	+70	×C	

DC Characteristics

Symbol	Parameter	Min	Max	Units	Notes
IDD	Supply Current		TBD	A	
ILATCH	DC latch-up current 70× C	-400	400	mA	
IIN	Input Leakage Current		TBD	uA	
VOL	Output LOW Voltage		0.3 VDD	V	
VOH	Output HIGH Voltage	0.7 VDD	VDD	V	
CIN	Input Capacitance		TBD	pF	

Notes:

1. These are stress ratings only. Exceeding the absolute maximum ratings may permanently damage the device. Operating the device at absolute maximum ratings for extended periods may affect device reliability, and void warranty.
2. Voltages measured with respect to VSS.

6 AC Parameters and Timing

Timing

| Symbol	Parameter	Min	Max	Units	Notes
PWR	AC Power Consumption		TBD	mA/MHz	
TCLKH	Clock width high phase	8		ns	
TCLKL	Clock width low phase	8		ns	
TPRD	Clock period	25		ns	
TADDRS	Address set-up time	7		ns	1,3
TADDRH	Address hold time	0.5		ns	1,3
TWAITS	Wait set-up time	6		ns	1,3
TWAITH	Wait hold time	1		ns	1,3
TDIOS	DATA I/O [15:0] set-up time	2		ns	1,3
TDIOH	DATA I/O [15:0] hold time	1.5		ns	1,3
TCSS	Chip select set-up time	6		ns	1,3
TCSH	Chip select hold time	1		ns	1,3
TRWS	Not-Read/Write set-up time	6		ns	1,3
TRWH	Not-Read/Write hold time	1.0		ns	1,3
TADO	Address to valid data output		14	ns	1,3
TRWDO	Not-Read/Write to valid data I/O		11	ns	1,3
TCSDO	Chip select to valid data output		11	ns	1,3
TORDY	Clock to ORDY output delay		14	ns	2,3
TIRDY	Clock to IRDY output delay		16	ns	2,3
TBUSY	Clock to BUSY output delay		16	ns	2,3
TRDY	Clock to RDY output delay		16	ns	2,3
TRST	Asynchronous reset pulse width	1		cycle	
TSTRT	Start delay after reset	3		cycles	

Notes:

1. Timings simulated using a 50 pF load.
2. Timings simulated using a 20 pF load.
3. Typical output capacitance at any given pin is 7pF.

6.1 Timing Diagrams

Figure 4 Input / Output Access
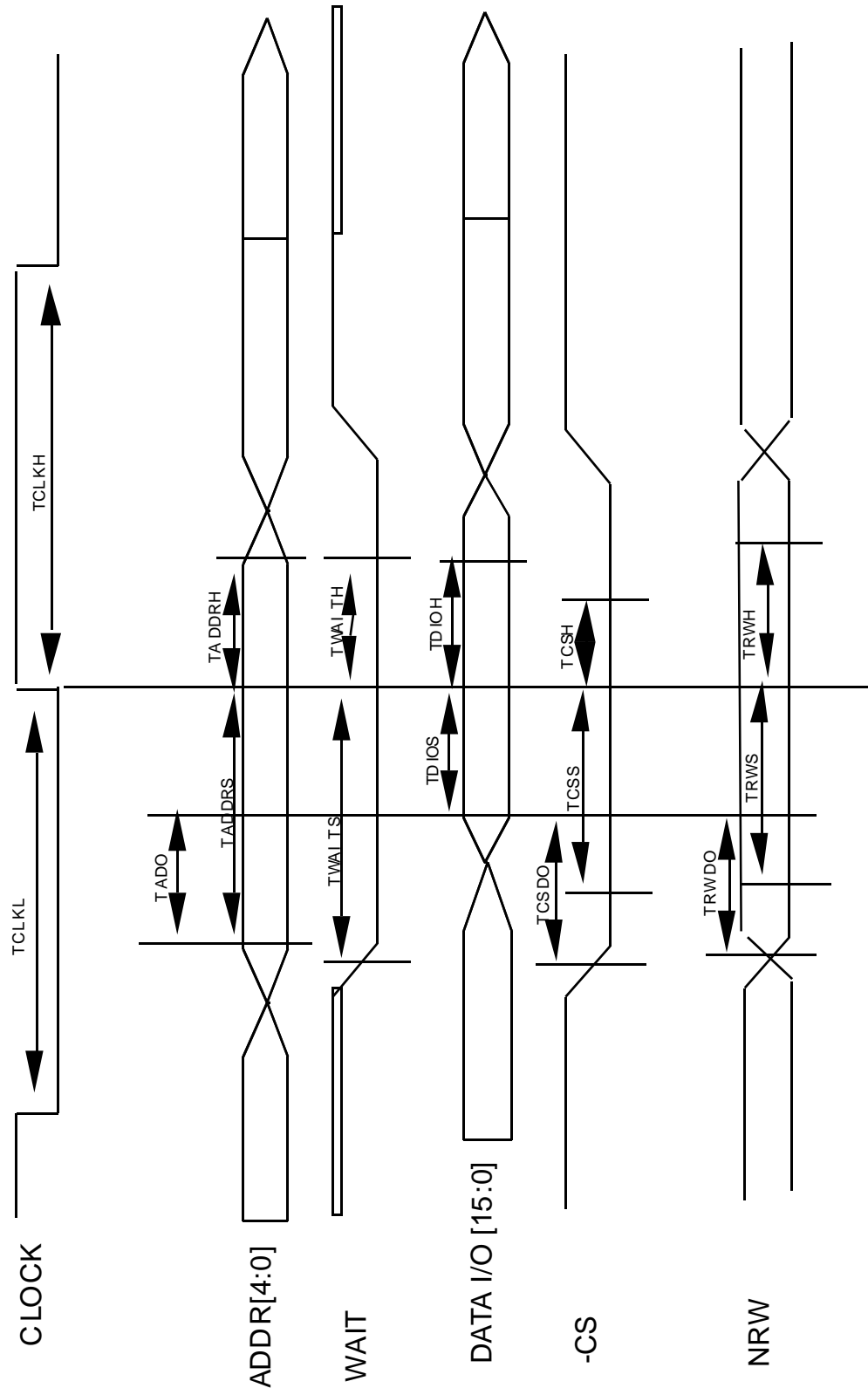
Figure 5 Control Signals
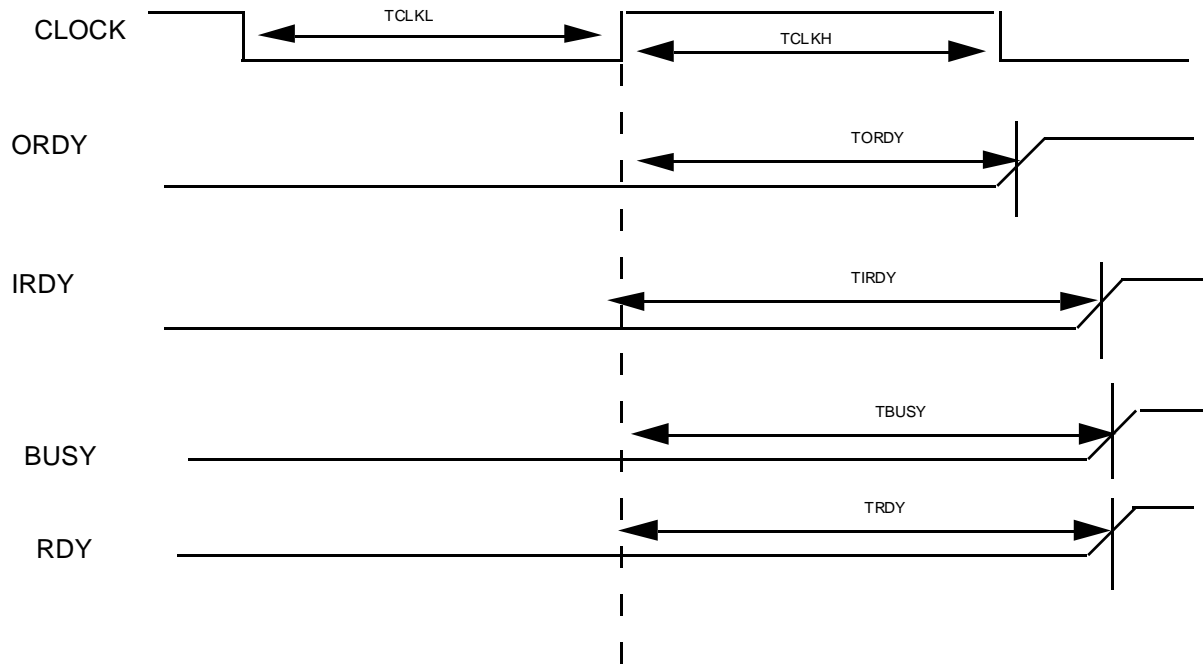
7 Pinout

The VMS113 is packaged in a 44 pin PLCC.

Signal Description

Signal Name	Pin	Type	Signal Description
-RESET	25	ITS	RESET: (Active Low) Used to reset all internal registers to 00h. This signal is asynchronous to CLOCK input and must be held low for 1 complete cycle.
CLOCK	16	IT	CLOCK
ADDR[4:0]	11, 10 ,9, 8 ,7	IT	ADDRESS: These inputs are used to select the internal registers of the VMS110
WAIT	26	IT	WAIT: Is used to hold off DATA I/O bus read or write cycles. WAIT must be low to strobe data into the or strobe new data out of the VMS110. WAIT must be low for the VMS110 to see CLOCK for I/O operations
ORDY	22	OC	OUTPUT READY: Indicates that the output register can be unloaded.
IRDY	21	OC	INPUT READY: Indicates that the input register can be loaded.
RDY	19	OC	READY: Logical "OR" or ORDY and IRDY signals
BUSY	20	OC	BUSY: Indicates an encryption/decryption cycle is in progress
-CS	15	IT	CHIP SELECT: (Active Low) This signal is used to select the DATA I/O port of the chip. This input signal must be synchronous to CLOCK.
NRW	14	IT	READ/WRITE: This signal is used to indicate which type of operation is being performed on the DATA I/O port. When low a read is performed, turning on the Data I/O drivers. When high, a write is performed, turning off the DATA I/O drivers This input must be synchronous to CLOCK.
DATA I/O[15:0]	27,28,29,30, 33,34,35,36, 41,42,43,44, 3,4,5,6	ITOC	DATA INPUT/OUTPUT: 16-bit bi-directional port used to pass data and keys in and out of the chip.
VDD	2,13,18, 23,32,38,40	PWR	Power Connection +5 VDC
VSS	1,12,17, 24,31,37,39	GND	Ground Connection 0 VDC

7.1 Physical Pinout Description

Package Diagram