Zilog

Product Specification

T-52-33-17

Z8068/Z9518 Z-DCP Data Ciphering Processor

October 1988

Features

- Encrypts and decrypts data using the National Bureau of Standards encryption algorithm.
- Supports three standard ciphering modes: Electronic Code Book, Chain Block and Cipher Feedback.
- Three separate registers for encryption, decryption, and master keys improve system security and throughput by eliminating frequent reloading of keys.
- Three separate programmable ports (master, slave, and key data) provide hardware separation of encrypted data, clear data, and keys.
- Data rates greater than 1M bytes per second can be handled.
- Key parity check.

General Description

The Z8068/Z9518 Data Ciphering Processors (DCP) are n-channel, silicon-gate LSI devices, which contains the circuitry to encrypt and decrypt daya using national Bureau of Standards encryption algorithms. It is designed to be used in a variety of environments, including dedicated controllers, communication concentrators, terminals, and peripheral task processors in general processor systems.

The DCP provides a high throughput rate using Cipher Feedback, Electronic Code Book, or Cipher Block Chain operating moces. The provisions of separate ports for key input, clear data, and enciphered data enhances security.

The host system communicates with the DCP using commands entered in the master port or through auxiliary control lines. Once set up, data can flow through the DCP at high speeds because input, output and ciphering activities can be performed concurrently. External DMA control can easily be used to enhance throughput in some system configurations.

The Z8068 and Z9518 DCP are designed to interface directly to Zilog's Z-BUS® . Device signal/pin functions are shown in Figure 1; actual pin number assignments are shown in Figure 2.

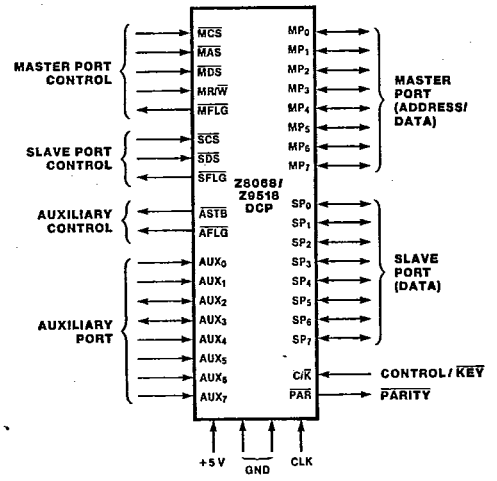
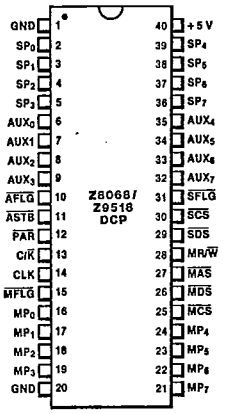


Figure 1. Pin Functions



(DIP) Pin Assignments

Pin Descriptions

$\overline{AFLG}$. *Auxiliary Port Flag* (output, active Low). This output signal indicates that the DCP is expecting key data to be entered on pins AUX_0-AUX_7. This can occur only when C/$\overline{K}$ is Low and a "Load Key Through AUX Port" command has been entered. $\overline{AFLG}$ remains active (Low) during the input of all eight bytes and will go inactive with the leading edge of the eighth strobe ($\overline{ASTB}$).

$\overline{ASTB}$. *Auxiliary Port Strobe* (input, active Low). In Multiplexed Control mode (C/$\overline{K}$ Low), the rising (trailing) edge of $\overline{ASTB}$ strobes the key data on pins AUX_0-AUX_7 into the appropriate internal key register. This input is ignored unless $\overline{AFLG}$ and C/$\overline{K}$ are both Low. One byte of key data is entered on each $\overline{ASTB}$ with the most significant byte entered first.

AUX_0-AUX_7. *Auxiliary Port Bus* (bidirectional, active High). When the DCP is operated in Multiplexed Control mode (C/$\overline{K}$ Low), these eight lines form a key-byte input port, which can be used to enter the master and session keys. This port is the only path available for entering the master key. (Session keys can also be entered via the master port.) AUX_0 is the low-order bit and is considered to be the parity bit in key bytes. The most significant byte is entered first.

When the DCP is operated in Direct Control mode (C/$\overline{K}$ High), the auxiliary port's key-entry function is disabled and five of the eight lines become direct control/status lines for interfacing to high-speed microprogrammed controllers. In this case, AUX_0, AUX_1 and AUX_4 have no function, and the other pins are defined as follows:

AUX_2-$\overline{BSY}$. *Busy* (output, active Low). This status output gives a hardware indication that the ciphering algorithm is in operation. AUX_2-$\overline{BSY}$ is driven by the BSY bit in the Status register such that when the BSY bit is 1 (active), AUX_2-$\overline{BSY}$ is Low.

AUX_3-$\overline{CP}$. *Command Pending* (output, active Low). This status output gives a hardware indication that the DCP is ready to accept the input of key bytes following a Low-to-High transition on AUX_7-K/$\overline{D}$. AUX_3-$\overline{CP}$ is driven by the CP bit in the Status register such that when the CP bit is 1 (active), AUX_3-$\overline{CP}$ is Low.

AUX_5-S/$\overline{S}$. *Start/Stop* (input, Low = Stop). When this pin goes Low (Stop), the DCP follows the normal Stop command sequence. When this pin goes High, a sequence equivalent to a Start Encryption or Start Decryption command is followed. When AUX_5-S/$\overline{S}$ goes High, the level on AUX_6-E/$\overline{D}$ selects either the start encryption or start decryption operation.

AUX_6-E/$\overline{D}$. *Encrypt/Decrypt* (input, Low = Decrypt). When AUX_5-S/$\overline{S}$ goes High, it initiates a normal data ciphering operation whose input specifies whether the ciphering algorithm is to encrypt (E/$\overline{D}$ High) or decrypt (E/$\overline{D}$ Low).

When AUX_7-K/$\overline{D}$ goes High, initiating the entry of key bytes, the level on AUX_6-E/$\overline{D}$ specifies whether the bytes are to be written into the E Key register (E/$\overline{D}$ High) or the D key Register (E/$\overline{D}$ Low).

The AUX_6-E/$\overline{D}$ input is not latched internally and must be held constant whenever one or more of AUX_5-S/$\overline{S}$, AUX_7-K/$\overline{D}$, AUX_2-$\overline{BSY}$, or AUX_3-$\overline{CP}$ are active. Failure to maintain the proper level on AUX_6-E/$\overline{D}$ during loading or ciphering operations results in scrambled data in the internal registers.

AUX_7-K/$\overline{D}$. *Key/Data* (input, Low = Data). When this signal goes High, the DCP initiates a key-data input sequence as if a Load Clear E or D Key Through Master Port command had been entered. The level on AUX_6-E/$\overline{D}$ determines whether the subsequently entered clear-key bytes are written into the E key register (E/D High) or the D key register (E/$\overline{D}$ Low)

AUX_7-K/$\overline{D}$ and AUX_5-S/$\overline{S}$ are mutually exclusive control lines; when one goes active (High), the other must remain inactive (Low) until the first returns to an inactive state. In addition, both lines must be inactive (Low) whenever a transition occurs on C/$\overline{K}$ (entering or exiting Direct Control mode).

C/$\overline{K}$. *Control/Key Mode Control.* (input, Low = Key). This input determines the operating characteristics of the DCP. A Low input on C/$\overline{K}$ puts the DCP into the Multiplexed Control mode, enabling programmed access to internal registers through the master port and enabling input of keys through the master or auxiliary port. A High input on C/$\overline{K}$ specifies operation in Direct Control mode. In this mode, several of the auxiliary port pins become direct control status signals which can be driven/sensed by high-speed controller logic, and access to internal registers through the master port is limited to the Input or Output register.

CLK. *Clock* (input, TTL compatible). An external timing source is input via the CLK pin. The Data Strobe signals ($\overline{MDS}$, $\overline{SDS}$) must change synchronously with this clock input, as must Master Port Address Strobe ($\overline{MAS}$) in Multiplexed Control mode (C/$\overline{K}$ Low), and also AUX_7-K/$\overline{D}$ and AUX_5-S/$\overline{S}$ in Direct Control mode (C/$\overline{K}$ High). In addition, the Auxiliary, Master and Slave Port Flag outputs ($\overline{AFLG}$, $\overline{MFLG}$, and $\overline{SFLG}$) change synchronously with the clock. When using the DCP with the Z8000 CPU in Multiplexed Control mode, the clock input must agree in frequency and phase with the processor clock; however, the DCP does not require the high voltage levels of the processor clock.

Pin Descriptions (Continued)

$\overline{MAS}$. *Master Port Address Strobe* (input, active Low). In Multiplexed Control mode (C/$\overline{K}$ Low), an active (Low) signal on this pin indicates the presence of valid address and chip select information at the master port. This information is latched internally on the rising edge of Master Port Address Strobe ($\overline{MAS}$). When C/$\overline{K}$ is High (Direct Control mode), $\overline{MAS}$ can be High or Low without affecting DCP operation, except that, regardless of the state of C/$\overline{K}$, if both Master Port Address Strobe ($\overline{MAS}$) and Data Strobe ($\overline{MDS}$) are Low simultaneously, the DCP Mode register will be reset to ECB mode. The master port is assigned to clear data, the slave port is assigned to enable data, and all flags remain inactive.

$\overline{MCS}$. *Master Port Chip Select* (input, active High). This signal is used to select the master port. In Multiplexed Control mode (C/$\overline{K}$ Low), the level on $\overline{MCS}$ is latched internally on the rising edge of Master Port Address Strobe ($\overline{MAS}$). This latched level is retained as long as $\overline{MAS}$ is High; when $\overline{MAS}$ is Low, the latch becomes invisible and the internal signal follows the $\overline{MCS}$ input. In Direct Control mode (C/$\overline{K}$ High), no latching of Master Port Chip Select occurs; the level on $\overline{MCS}$ is passed directly to the internal select circuitry, regardless of the state of Address Strobe ($\overline{MAS}$).

$\overline{MDS}$. *Master Port Data Strobe* (input, active Low). When $\overline{MDS}$ is active and Master Port Chip Select ($\overline{MCS}$) is valid, it indicates that valid data is present on MP_0–MP_7 during output. $\overline{MDS}$ and Master Port Address Strobe ($\overline{MAS}$) are normally mutually exclusive; if both go Low simultaneously, the DCP is reset to ECB mode and all flags remain inactive.

$\overline{MFLG}$. *Master Port Flag* (output, active Low). This flag is used to indicate the need for a data transfer into or out of the master port during normal ciphering operation. Depending upon the control bits written to the Mode register, the master port is associated with either the Input register or the Output register.

If data is to be transferred through the master port to the Input register, the $\overline{MFLG}$ reflects the contents of the Input register; after any start command is entered, $\overline{MFLG}$ goes active (Low) whenever the Input register is not full. $\overline{MFLG}$ is forced High by any command other than a start. Conversely, if the master port is associated with the Output register, $\overline{MFLG}$ reflects the contents of the Output register (except in single-port configuration). $\overline{MFLG}$ goes active (Low) whenever the Output register is not empty. In single-port configuration, $\overline{MFLG}$ reflects the contents of the Input register, while the Slave Port Flag ($\overline{SFLG}$) is associated with the Output register.

MP_0-MP_7. *Master Port Bus* (input/output, active High). These eight bidirectional lines are used to specify internal register addresses in Multiplexed Control mode (see C/$\overline{K}$) and to input and output data. The master port provides software access to the Status, Command and Mode registers as well as the Input and Output registers. The 3-state master port outputs are enabled only when the master port is selected by Master Port Chip Select ($\overline{MCS}$) being Low, with Master Port Read/Write (MR/$\overline{W}$) High, and strobed by a Low on the Master Port Data Strobe ($\overline{MDS}$). MP_0 is the low-order bit. Data and key information is entered into this port with most significant byte input first.

MR/$\overline{W}$. *Master Port Read/Write* (input, Low = Write). This signal indicates to the DCP whether the current master port operation is a read (MR/$\overline{W}$ is High) or a write (MR/$\overline{W}$ is Low), thereby indicating whether data is to be transferred from or to an internal register. MR/$\overline{W}$ is not latched internally and must be held stable while Master Port Data Strobe ($\overline{MDS}$) is Low.

$\overline{PAR}$. *Parity* (output, active Low). The DCP checks all key bytes for correct (odd) parity as they are entered through either the master port (Multiplexed or Direct Control mode) or the auxiliary port (Multiplexed Control mode only). If any key byte contains even parity, the PAR bit in the Status register is set to 1 and PAR goes Low. The least significant bit of key bytes is the parity.

$\overline{SCS}$. *Slave Port Chip Select* (input, active Low). This signal is logically combined with Slave Port Data Strobe ($\overline{SDS}$) to facilitate slave port data transfers in a bus environment. $\overline{SCS}$ is not latched internally and can be permanently tied to Low without impairing slave port operation.

$\overline{SDS}$. *Slave Port Data Strobe* (input, active Low). When both $\overline{SDS}$ and $\overline{SCS}$ are Low, it indicates to the DCP either that valid data is on the SP_0–SP_7 lines for an input operation, or that data is to be driven onto the SP_0–SP_7 lines for output. The direction of data flow is determined by the control bits in the Mode register.

$\overline{SFLG}$. *Slave Port Flag* (output, active Low). This output indicates the status of either the Input register or the Output register, depending on the control bits in the Mode register. In single-port configuration, $\overline{SFLG}$ goes active during normal processing whenever the Output register is not empty. In dual-port configuration, $\overline{SFLG}$ reflects the content of whichever register is associated with the slave port. If the input register is assigned to the slave port, $\overline{SFLG}$ goes active whenever the Input register is not full, once any of the start commands has been entered; $\overline{SFLG}$ is forced

Pin Descriptions (Continued)

inactive if any other command is entered. If the slave port is assigned to the Output register, $\overline{SFLG}$ goes active whenever the Output register is not empty. In this case, $\overline{SFLG}$ goes inactive if any command is aborted.

SP_0-SP_7. *Slave Port Bus* (bidirectional). The slave port provides a second data input/output interface to the DCP, allowing overlapped input, output, and ciphering operations. The 3-state slave port outputs are driven only when Slave Port Chip Select ($\overline{SCS}$) and Slave Port Data Strobe ($\overline{SDS}$) are both Low, $\overline{SFLG}$ is 0, and the internal port control configuration allows output to the slave port. SP_0 is the low order bit. The most significant byte of data blocks is entered or retrieved through this port first.

Functional Description

The overall design of the DCP, as shown in Figure 3, is optimized to achieve high data throughput. Data bytes can be transferred through both the master and slave ports, and key bytes can be written through both the auxiliary and master ports. Three 8-bit buses (input, output and C bus) carry data and key bytes between the ports and the internal registers. Three 56-bit, write-only key registers are provided for the Master (M) Key, the Encryption (E) Key and the Decryption (D) Key. Parity checking is provided on incoming key bytes. Two 64-bit registers are provided for initializing vectors (IVE and IVD) that are required for chained (feedback) ciphering modes. Three 8-bit registers (Mode, Command and Status) are accessible through the master port.

Algorithm Processing. The algorithm processing unit of the DCP (Figure 3) is designed to encrypt and decrypt data according to the National Bureau of Standards' Data Encryption Standard (DES), as specified in Federal Information Processing Standards Publication 46. The DES specifies a method for encrypting 64-bit blocks of clear data ("plain text") into corresponding 64-bit blocks of "cipher text."

The DCP offers three ciphering methods, selected by the cipher type field of the Mode register: Electronic Code Book (ECB), Cipher Block Chain (CBC) and Cipher Feedback (CFB). These methods are implemented in accordance with Federal Information Processing Standards, Publication 46.

Electronic Code Book (ECB) is a straightforward implementation of the DES: 64 bits of clear data in, 64 bits of cipher text out, with no cryptographic dependence between blocks.

Cipher Block Chain (CBC) also operates on blocks of 64 bits, but it includes a feedback step which chains consecutive blocks so that repetitive data in the plain text (such as ASCII blanks) does not yield repetitive cipher text. CBC also provides an error extension characteristic which protects against fraudulent data insertions and deletions.

Cipher Feedback (CFB) is an additive stream cipher method in which the DES algorithm generates a pseudorandom binary stream, which is then exclusive-ORed with the clear data to form the cipher text. The cipher text is then fed back to form a portion of the next DES input block. The DCP implements 8-bit cipher feedback, with data input, output,

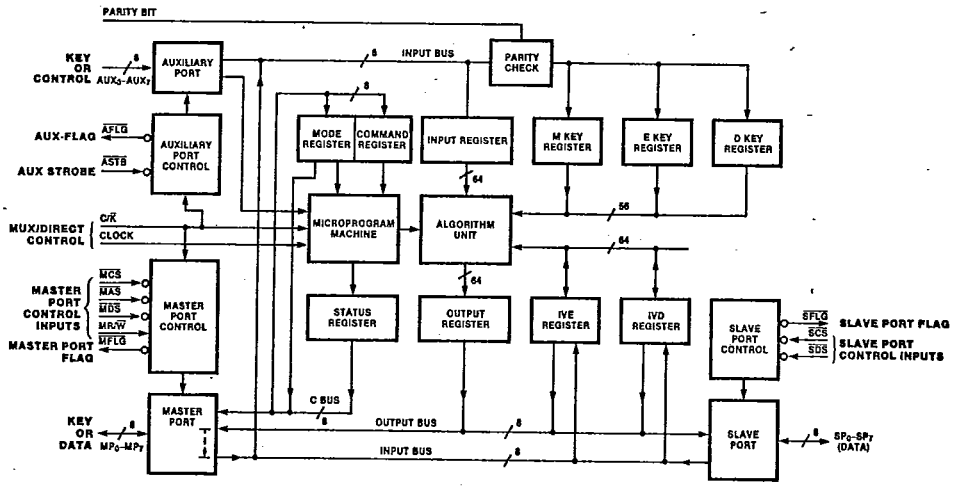


Figure 3. Z8068/Z9518 Block Diagram

Functional Description (Continued)

and feedback paths of one byte wide. This method is useful for low speed, character-at-a-time, serial communications.

Multiple Key Registers. The DCP provides the necessary registers to implement a multiple-key or master-key system. In such an arrangement, a single master key, stored in the DCP M key register, is used to encrypt session keys for transmission to remote DES equipment and to decrypt session keys received from such equipment. The M Key register may be loaded (with plain text) only through the auxiliary port, using the Load Clear Master Key command. In addition to the M Key register, the DCP contains two session key registers: the E key register, used to encrypt clear text, and the D key register, used to decrypt cipher text. All three registers are loaded by writing commands such as Load Clear E Key, through master port, into the Command register, and then writing the eight bytes of key data to the port when the Command Pending bit in the Status register is 1.

Operating Modes: Multiplexed Control vs. Direct Control. The DCP can be operated in either of two basic interfacing modes, determined by the logic level on the C/$\overline{K}$ input pin. In Multiplexed Control mode (C/$\overline{K}$ Low), the DCP is configured internally to allow a master CPU to address five of the internal control/status/data registers directly, thereby controlling the device via mode and command values written to these registers. Also, in this mode, the auxiliary port is enabled for key-byte input.

If the logic level on C/$\overline{K}$ is brought High, the DCP enters Direct Control mode, and the auxiliary port pins are converted into direct hardware status or control signals capable of instructing the DCP to perform a functionally complete subset of its cipher processing at very high throughputs. This operating mode is particularly well suited for ciphering data for high-speed peripheral devices such as magnetic disk or tape.

Data Flow. Bits M_2 and M_3 of the Mode register control the flow of data into and out of the DCP through the master and slave ports. Three basic configurations are provided: one single-port and two dual-port.

Single-Port Configuration. The simplest configuration occurs when the Mode register configuration bits are set to master port only (Figure 4). In this operating configuration, the encrypt/decrypt bit (M_4) controls the processing of data. Data to be encrypted or decrypted is written to the master port Input register address. To facilitate monitoring of the Input register status, the $\overline{MFLG}$ signal goes Low when the Input register is not full. Data is read by the master CPU through the master port Output register address. Pin $\overline{SFLG}$ goes Low when the Output register is not empty. $\overline{MFLG}$ is then redefined as a master input flag and $\overline{SFLG}$ is redefined as a master output flag.

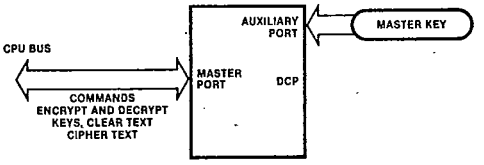


Figure 4. Single-Port Configuration, Multiplexed Control

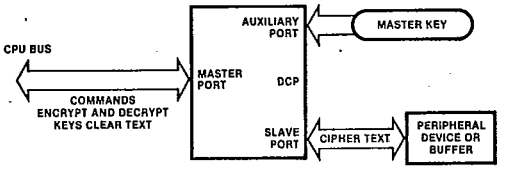


Figure 5a. Dual-Port Configuration, Multiplexed Control

Dual Port, Master Port Clear Configuration. In the dual-port configurations, both the master and slave ports are used for data entry and removal (Figures 5a and 5b). In the master port clear configuration, clear text for encryption can be entered only through the master port, and clear text resulting from decryption can be read only through the master port. Cipher text can be handled only through the slave port. The actual direction of data flow is controlled either by the encrypt/decrypt bit (M_4) in the Mode register or by the Start Encryption or Start Decryption commands. If encryption is specified, clear data will flow through the master port to the Input register, and cipher data will be available at the slave port when it is ready to be read from the Output register. For decryption, the process is reversed, with cipher data written to the Input register

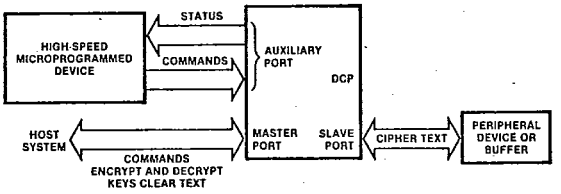


Figure 5b. Dual-Port Configuration, Direct Control

Functional Description (Continued)

through the master port. Slave port and clear text read from the Master port.

In both dual-port configurations, the Master Port Flag ($\overline{MFLG}$) and the Slave Port Flag ($\overline{SFLG}$) are used to indicate the status of the data register associated with the master port and slave port, respectively. For example, during encryption in the master port clear configuration, $\overline{MFLG}$ goes Low (active) when the Input register is not full; $\overline{SFLG}$ goes Low (active) when the Output register is not empty. If cyphering operation changes direction, $\overline{MFLG}$ and $\overline{SFLG}$ switch their register association (see Table 1).

Mode Register Bits				
Encrypt/ Decrypt Bit M4	Port Configuration Bit M3	Bit M2	Input Register Flag	Output Register Flag
0	0	0	$\overline{MFLG}$	$\overline{SFLG}$
0	0	1	$\overline{SFLG}$	$\overline{MFLG}$
0	1	0	$\overline{MFLG}$	$\overline{SFLG}$
1	0	0	$\overline{SFLG}$	$\overline{MFLG}$
1	0	1	$\overline{MFLG}$	$\overline{SFLG}$
1	1	0	$\overline{MFLG}$	$\overline{SFLG}$

Table 1. Association of Master Port Flag (MFLG) and Slave Port Flag (SFLG) with Input and Output Registers

Dual Port, Slave Port Clear Configuration. This configuration is identical to the previously described dual-port, master port clear configuration except that the direction of ciphering is reversed. That is, all data flowing in or out of the master port is cipher text, and all data at the slave port is clear text.

Master Port Read/Write Timing. The master port of the DCP is designed to operate directly with a multiplexed address/data bus such as the Zilog Z-BUS. Several features of the master port logic are:

- The level on Master Port Chip Select ($\overline{MCS}$) is latched internally on the rising (trailing) edge of Master Port Address Strobe ($\overline{MAS}$). This action relieves external address decode circuitry of the responsibility for latching chip select at address time.
- The levels on MP_1 and MP_2 are also latched internally on the rising edge of $\overline{MAS}$ and are subsequently decoded to enable reading and writing of the DCP's internal registers (Mode, Command, Status, Input and Output). This action also eliminates the need for external address latching and decoding.
- Data transfers through the master port are controlled by the levels and transitions on Master Port Data Strobe ($\overline{MDS}$) and Master Port Read/Write ($MR/\overline{W}$). The former controls the timing and the latter controls the transfer direction. Data transfers disturb neither the chip-select nor address latches, so once the DCP and a particular register have been selected, any number of reads or writes of that register can be accomplished without intervening address cycles. This feature greatly speeds up the loading of keys and data, given the necessary transfer control external to the DCP.

Loading Keys and Initializing Vector (IV) Registers. Because the key and Initializing Vector (IV) registers are not directly addressable through any of the DCP's ports, keys and vector data must be loaded (and in the case of vectors, read) via "command data sequences." Most of the commands recognized by the DCP are of this type. A load or read command is written to the Command register through the master port. The command processor responds by asserting the Command Pending output. The user then either writes eight bytes of key or vector data through the master or auxiliary port, as appropriate to the specific command, or reads eight bytes of vector data from the master port.

In Direct Control mode, only the E Key and D Key registers can be loaded; the M Key and IV registers are inaccessible. Loading the E and D Key registers is accomplished by placing the proper state on the AUX_6-$E/\overline{D}$ input (High for E Key, Low for D Key) and then raising the AUX_7-$K/\overline{D}$ input—indicating that key loading is required. The command processor attaches the proper key register to the master port and asserts the AUX_3-$\overline{CP}$ (Command Pending) signal (active Low). The eight key bytes can then be written to the master port. In the Multiplexed Control mode, all key and vector registers can be written to and all but the Master (M) Key register can be loaded with encrypted, as well as clear, data. If the operation is a Load Encrypt command, the subsequent data written to the master or auxiliary port (as appropriate) is routed first to the Input register and decrypted before it is written into the specified key or Initializing Vector register.

Parity Checking of Keys. Key bytes contain seven bits of key information and one parity bit. By DES designation, the low-order bit is the parity bit. The parity-check circuit is enabled whenever a byte is written to one of three key registers. The output of the parity-check circuit is connected to $\overline{PAR}$ and the state of this signal is reflected in Status register bit PAR (S_3). Status register bit PAR goes to 1 whenever a byte with even parity (an even number of 1s) is detected. In addition to the PAR bit, the Status register has a Latched Parity bit (LPAR, S_4) that is set to 1 whenever the Status register PAR bit goes to 1. Once set, the LPAR bit is not cleared until a reset occurs or a new Load Key command is issued.

Functional Description (Continued)

When an encrypted key is entered, the parity-check logic operates only after the decrypted key is available. The encrypted data is not checked for parity. The $\overline{PAR}$ signal reflects the state of the decrypted bytes on a byte-to-byte basis as they are clocked through the parity-check logic on their way to the key register. Thus, the time during which $\overline{PAR}$ indicates the status of a byte of decrypted key data may be as short as four clock cycles. The LPAR bit in the Status register indicates if any erroneous bytes of key data were entered.

Programming

Initialization. The DCP can be reset in several ways:

- By the "Software Reset" command.
- By a hardware reset, which occurs whenever both $\overline{MAS}$ and $\overline{MDS}$ go Low simultaneously.
- By writing to the Mode register.
- By aborting any command.

These sequences initiate the same internal operations, except that loading the Mode register or aborting any command does not subsequently reset the Mode register. Once a reset process starts, the DCP is unable to respond to further commands for approximately five clock cycles. If a power-up hardware reset is used, the leading edge of the reset signal should not occur until approximately 1 ms after V_{CC} has reached normal operating voltage. This delay time is needed for internal signals to stabilize.

Registers. The registers in the DCP that can be addressed directly through the master port are shown with their addresses in Table 2. A brief description of these registers and those not directly accessible follows.

C/$\overline{K}$	MP2	MP1	MR/$\overline{W}$	$\overline{MCS}$	Register Addressed
0	X	0	0	0	Input Register
0	X	0	1	0	Output Register
0	0	1	0	0	Command Register
0	0	1	1	0	Status Register
0	1	1	X	0	Mode Register
X	X	X	X	1	No Register Accessed
1	X	X	0	0	Input Register
1	X	X	1	0	Output Register

Table 2. Master Port Register Addresses

T-52-33-17

Hex Code	Command
90	Load Clear M Key Through Auxiliary Port
91	Load Clear E Key Through Auxiliary Port
92	Load Clear D Key Through Auxiliary Port
11	Load Clear E Key Through Master Port
12	Load Clear D Key Through Master Port
B1	Load Encrypted E Key Through Auxiliary Port
B2	Load Encrypted D Key Through Auxiliary Port
31	Load Encrypted E Key Through Master Port
32	Load Encrypted D Key Through Master Port
85	Load Clear IVE Through Master Port
84	Load Clear IVD Through Master Port
A5	Load Encrypted IVE Through Master Port
A4	Load Encrypted IVD Through Master Port
8D	Read Clear IVE Through Master Port
8C	Read Clear IVD Through Master Port
A9	Read Encrypted IVE Through Master Port
A8	Read Encrypted IVD Through Master Port
39	Encrypt With Master Key
41	Start Encryption
40	Start Decryption
C0	Start
E0	Stop
00	Software Reset

Table 3. Command Codes in Multiplexed Control Mode

Command Register. Data written to the 8-bit, write-only Command register through the master port is interpreted as an instruction. A detailed description of each command is given in the Commands section; the commands and their hexadecimal representations are summarized in Table 3. A subset of these commands can be entered implicitly in Direct Control mode (C/$\overline{K}$ High)—even though the Command register cannot be addressed in that mode—by transitions on auxiliary lines AUX_5-S/$\overline{S}$, AUX_6-E/$\overline{D}$, and AUX_7-K/$\overline{D}$. These implicit commands are summarized in Table 4.

	Pins			
C/$\overline{K}$	AUX_7-K/$\overline{D}$	AUX_6-E/$\overline{D}$	AUX_5-S/$\overline{S}$	Command Initiated
H	L	L	↑	Start Decryption
H	L	H	↑	Start Encryption
H	L	X	↓	Stop
H	↑	L	L	Load D Key Clear through master port
H	↑	H	L	Load E Key Clear through master port
H	↓	X	L	End Load Key command
H	H	X	H	Not allowed
L	Data	Data	Data	AUX pins become Key-Byte inputs

Table 4. Implicit Command Sequences in Direct Control Mode

Programming (Continued)

Status Register. The bit assignments in the read-only Status register are shown in Figure 6. The PAR, AFLG, SFLG and MFLG bits indicate the status of the corresponding output pins, as do the busy and command pending bits when the DCP is in a Direct Control mode (C/$\overline{K}$ High). In each case, the output signal will be active Low when the corresponding status bit is a 1. The parity bit indicates the parity of the most recently entered key byte. The LPAR bit indicates whether any key byte with even parity has been encountered since the last Reset or Load Key command.

The Busy bit is 1 whenever the ciphering algorithm unit is actively encrypting or decrypting data, either as a response to a command such as Load Encrypted Key (in which case the Command Pending bit is 1) or in the ciphering of regular text (indicated by the Start/Stop bit being 1). If the ciphered data cannot be transferred to the Output register because that register still contains output from a previous ciphering cycle, the Busy bit remains 1 even after the ciphering is complete. Busy is 0 at all other times, even when ciphering is not possible because data has not been written to the Input register.

The Command Pending bit is set to 1 by any command whose execution requires the transfer of data to or from a nonaddressable internal register, such as when writing key bytes to the E key register or reading bytes from the IVE register. Thus, the Command Pending bit is set following all commands except the three start commands, the Stop command and the Software Reset command. The Command Pending bit returns to 0 after all eight bytes have been transferred following Load Clear, Read Clear, or Read Encrypted commands; and after data has been transferred, decrypted, and loaded into the desired register following Load Encrypt commands.

The Start/Stop bit is set to 1 when one of the start commands is entered and it is reset to 0 whenever a reset occurs or when a new command other than a Start is entered.

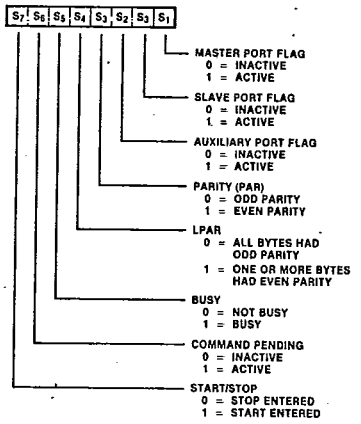


Figure 6. Status Register Bit Assignments

Mode Register. Bit assignments in this 5-bit read/write register are shown in Figure 7. The cipher type bits (M_1 and M_0) indicate to the DCP which ciphering algorithm is to be used. On reset, the Cipher Type mode defaults to Electronic Code Book mode.

Configuration bits (M_3 and M_2) indicate which data ports are to be associated with the Input and Output registers and flags. When these bits are set to the single-port, master-only configuration (M_3 M_2 = 10), the slave port is disabled and no manipulation of Slave Port Chip Select ($\overline{SCS}$) or Slave Data Strobe ($\overline{SDS}$) can result in data movement through the slave port; all data transfers are accomplished through the master port, as previously described in the Functional Description. Both $\overline{MFLG}$ and $\overline{SFLG}$ are used in this configuration; $\overline{MFLG}$ gives the status of the Input register and $\overline{SFLG}$ gives the status of the Output register.

When the configuration bits are set to one of the dual-port configurations (M_3 M_2 = 00 or 01), both the master and slave ports are available for input and output. When M_3, M_2 = 01 (the default configuration), the master port handles clear data while the slave port handles encrypted data. Configuration M_3, M_2 = 00 reverses this assignment. Actual data direction at any particular moment is controlled by the Encrypt/Decrypt bit.

The Encrypt/Decrypt bit (M_4) instructs the DCP algorithm processor to encrypt or decrypt the data from the Input register using the ciphering method specified by the Cipher Type bits. The Encrypt/Decrypt bit also controls data flow within the DCP. For example, when the configuration bits are 0,1 (dual-port, master clear, slave encrypted) and the Encrypt/Decrypt bit is 1 (encrypt), clear data will flow into the DCP through the master port and encrypted data will flow out through the slave port. When the Encrypt/Decrypt bit is set to 0 (decrypt), data flow is reversed.

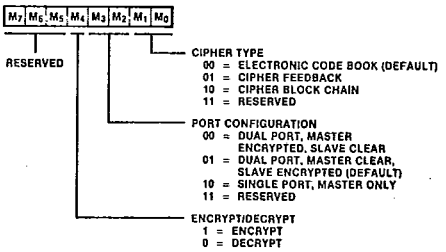


Figure 7. Mode Register Bit Assignments

Programming (Continued)

Input Register. The 64-bit, write-only Input register is organized to appear to the user as eight bytes of pushdown storage. A status circuit monitors the number of bytes that have been stored. The register is considered empty when the data stored in it has been or is being processed; it is considered full when one byte of data has been entered in Cipher Feedback mode or when eight bytes of data have been entered in Electronic Code Book or Cipher Block Chain mode. If the user attempts to write data into the Input register when it is full, the Input register disregards the attempt; no data in the register is destroyed.

Output Register. The 64-bit, read-only Output register is organized to appear to the user as eight bytes of pop-up storage. A status circuit detects the number of bytes stored in the Output register. The register is considered empty when all the data stored in it has been read by the master CPU and is considered full if it still contains one or more bytes of output data. If a user attempts to read data from the Output register when it is empty, the buffers driving the output bus remain in a 3-state condition.

M, E, D Key Registers. The following multibyte key registers cannot be addressed directly, but are loaded in response to commands written to the Command register.

There are three 64-bit, write-only key registers in the DCP: the Master (M) Key register, the Encrypt (E) key register, and the Decrypt (D) key register. The Master key register can be loaded only with clear data through the auxiliary port. The Encrypt and Decrypt Key registers can be loaded in any of four ways: (1) as clear data through the auxiliary port, (2) as clear data through the master port, (3) as encrypted data through the auxiliary port, or (4) as encrypted data through the master port. In the last two cases, the encrypted data is first routed to the Input register, decrypted using the M Key, and finally written to the target key register from the Output register.

Initializing Vector Registers (IVE and IVD). Two 64-bit registers are provided to store feedback values for cipher feedback and chained block ciphering methods. One initializing vector register (IVE) is used during encryption, the other (IVD) is used during decryption. Both registers can be loaded with either clear or encrypted data through the master port (in the latter case, the data is decrypted before being loaded into the IV register), and both may be read out either clear or encrypted through the master port.

Commands

All operations of the DCP result from command inputs, which are entered in Multiplexed Control mode by writing a command byte to the Command register. Command inputs are entered in Direct Control mode by raising and lowering the logic levels on the AUX_7-K/$\overline{D}$, AUX_6-E/$\overline{D}$, and AUX_5-S/$\overline{S}$ pins. Table 3 shows all commands that can be given in Multiplexed Control mode. Table 4 shows a subset of the implicit commands that can be executed in the Direct Control mode.

Load Clear M Key Through Auxiliary Port (90H).
Load Clear E Key Through Auxiliary Port (91H).
Load Clear D Key Through Auxiliary Port (92H).

These commands may be used only for multiplexed operations; they override the data flow specifications set in the Mode register and cause the Master (M) Key, Encrypt (E) Key, or Decrypt (D) Key register to be loaded with eight bytes written to the auxiliary port. After the Load command is written to the Command register, the Auxiliary Port Flag ($\overline{AFLG}$) goes active (Low) and the corresponding bit in the Status register (S_2) becomes 1, indicating that the device is able to accept key bytes at the auxiliary port pins. Additionally, the Command Pending bit (S_6) becomes 1 during the entire loading process.

Each byte is written to its respective key register by placing an active Low signal on the Auxiliary Port Strobe ($\overline{ASTB}$) once data has been set up on the auxiliary port pins. The actual write process occurs on the rising (trailing) edge of $\overline{ASTB}$. (See Switching Characteristics section for exact setup, strobe width, and hold times.)

The Auxiliary Port Flag ($\overline{AFLG}$) goes inactive immediately after the eighth strobe goes active (Low). However, the Command Pending bit (S_6) remains 1 for several more clock cycles, until the key loading process is completed. All key bytes are checked for correct (odd) parity as they are entered.

Load Clear E Key Through Master Port (11H).
Load Clear D Key Through Master Port (12H).

These commands are available in both Multiplexed Control and Direct Control modes. They override the data flow specifications set in the Mode register and attach the master port inputs to the Encrypt (E) Key or Decrypt (D) Key register, as appropriate, until eight key bytes have been written. In Multiplexed Control mode, the command is initiated by writing the Load command to the Command register. In Direct Control mode, the command is initiated by raising the AUX_7-K/$\overline{D}$ control input while the AUX_5-S/$\overline{S}$

Commands (Continued)

input is Low. In this latter case, the level on AUX_6-E/$\overline{D}$ determines which key register is written (High = E register).

Once the command has been recognized, the Command Pending bit (S_6 in the Status register) becomes 1. In Direct Control mode, AUX_3-$\overline{CP}$ goes active (Low), indicating that key entry may proceed. The host system then writes exactly eight bytes to the master port (at the Input register address in Multiplexed Control mode). When the key register has been loaded, the Command Pending bit returns to 0. In Direct Control mode, the AUX_3-$\overline{CP}$ output goes inactive, indicating that the DCP can accept the next command.

Load Encrypted E Key Through Auxiliary Port (B1H).
Load Encrypted D Key Through Auxiliary Port (B2H).

These commands are used in Multiplexed Control mode only. Their execution is similar to that of the Load Clear E (D) Key Through Auxiliary Port command, except that key bytes are first decrypted using the electronic code book algorithm and the Master (M) Key register. The key bytes are then loaded into the appropriate key register, after having passed through the parity-check logic.

The Command Pending bit (S_6) is 1 during the entire decrypt-and-load operation. In addition, the Busy bit (S_5) is 1 during the actual decryption process.

Load Encrypted E Key Through Master Port (31H).
Load Encrypted D Key Through Master Port (32H).

These commands are used in Multiplexed Control mode only. Their execution is similar in effect to that of the Load Clear E (D) Key Through Master Port command. The commands differ in that key bytes are initially decrypted using the electronic code book algorithm and the Master (M) Key register. Once decrypted, they are loaded byte-by-byte into the target key register, after having passed through the parity-check logic.

The command pending bit (S_6) is 1 during the entire decrypt-and-load operation. In addition, the busy bit (S_5) is 1 during the actual decryption process.

Load Clear IVE Register Through Master Port (85H)
Load Clear IVD Register Through Master Port (84H)

These commands are used in Multiplexed Control mode only. Their execution is virtually identical to that of the Load Clear E (or D) Key Through Master Port command. The commands differ in that the data written to the input register address is routed to either the Encryption Initializing Vector (IVE) or Decryption Initializing Vector (IVD) register instead of a key register. No parity checking occurs. The Command Pending bit (S_6) is 1 during the entire loading process.

T-52-33-17

Load Encrypted IVE Register Through Master Port (A5H).
Load Encrypted IVD Register Through Master Port (A4H).

These commands are analogous to the Load Encrypted E (or D) Key Through Master Port command. The data flow specifications set in the Mode register are overridden and the eight vector bytes are decrypted using the Decryption (D) Key register and the electronic code book algorithm. The resulting clear vector bytes are loaded into the target Initializing Vector register. No parity checking occurs. The Busy bit (S_5) does not become 1 during the decryption process, but the Command Pending bit (S_6) is 1 during the entire decryption-and-load operation.

Read Clear IVE Register Through Master Port (8DH).
Read Clear IVD Register Through Master Port (8CH).

In the Multiplexed Control mode, these commands override the data flow specifications set in the Mode register and connect the appropriate Initializing Vector register to the master port at the Output register address. In this state, each IV register appears as eight bytes of FIFO storage. The first byte of data is available six clocks after loading the Command register. The Command Pending bit in the Status register remains a 1 until sometime after the eighth byte is read out. The host system is responsible for reading exactly eight bytes.

Read Encrypted IVE Register Through Master Port (A9H).
Read Encrypted IVD Register Through Master Port (A8H).

In the Multiplexed Control mode only, these commands override the specifications set in the Mode register and encrypt the contents of the specified Initializing Vector register using the electronic code book algorithm and the Encrypt (E) key. The resulting cipher text is placed in the output register, where it can be read as eight bytes through the master port. During the actual encryption process, the Busy bit (S_5) is 1. When the Busy bit becomes 0, the encrypted vector bytes are ready to be read out. The Command Pending bit (S_6) is 1 during the entire encryption and output process; it becomes 0 when the eighth byte is read out. The host system is responsible for reading exactly eight bytes.

Encrypt with Master (M) Key (39H).

In the Multiplexed Control mode, this command overrides the data flow specifications set in the Mode register and causes the DCP to accept eight bytes from the master port, which are written to the Input register. When eight bytes have been received, the DCP encrypts

Commands (Continued)

the input using the Master (M) Key register. The encrypted data is loaded into the Output register, where it can be read out through the master port. The Command Pending bit (S_6) and the Busy (S_5) bit are used as status indicators in the three phases of this operation.

The Command Pending bit becomes 1 as soon as the Input register can accept data. When exactly eight bytes have been entered, the Busy bit becomes and remains 1 until the encryption process is complete. When Busy becomes 0, the encrypted data is available to be read out. The Command Pending bit returns to 0 when the eighth byte has been read.

Start Encryption (41H)
Start Decryption (40H)
Start (C0H).

The three start commands begin normal data ciphering by setting the Status register's Start/Stop bit (S_7) to 1. The Start Encryption and Start Decryption commands explicitly specify the ciphering direction by forcing the Encrypt or Decrypt bit (M_4) in the Mode register to 1 or 0, respectively. The Start command, however, uses the current state of the Encrypt/Decrypt bit, as specified in a previous Mode register load.

When a start command has been entered, the port status flag ($\overline{MFLG}$ or $\overline{SFLG}$) associated with the Input register becomes active (Low), indicating that data may be written to the Input register to begin ciphering.

In Direct Control mode, the Start command is issued by raising the level on the AUX_5-$S/\overline{S}$ input (Table 4). The ciphering direction is specified by the level on AUX_6-$E/\overline{D}$. If AUX_6-$E/\overline{D}$ is High when AUX_5-$S/\overline{S}$ goes High, the command is Start Encryption; if AUX_6-$E/\overline{D}$ is Low, it is Start Decryption.

Stop (E0H).

The Stop command clears the Start/Stop bit (S_7) in the Status register. This action causes the input flag ($\overline{MFLG}$ or $\overline{SFLG}$) to become inactive and inhibits the loading of any further input into the algorithm unit. If ciphering is in progress [Busy bit (S_5) is 1 or AUX_2-$\overline{BSY}$ is active], it is allowed to finish, and any data in the Output register remains accessible.

In Direct Control mode, the Stop command is implied when the signal level on the AUX_5-$S/\overline{S}$ input goes from High to Low (Table 4).

Software Reset (00).

This command has the same effect as a hardware reset ($\overline{MAS}$ and $\overline{MDS}$ Low): it forces the DCP back to its default configuration, and all processing flags go into Inactive mode. The default configuration includes setting the Mode register to Electronic Code Book ciphering mode and establishes a dual-port configuration with master port clear and slave port encrypted.

Timing Requirements

The control and/or data signals and the timing requirements for clock/reset, Direct Control mode, Multiplexed Control mode (master port), master (slave) port read/write, and auxiliary port key entry functions are illustrated in Figures 8 through 12. The ac switching characteristics of the signals involved in the above functions are described in the AC Characteristics. The specific timing periods described are identified by numerics (1 through 48), which are referenced in both the timing diagrams and in the AC Characteristics.

A two-to-seven character symbol is listed in AC Characteristics for each period described. The symbol specifies the signal(s) involved, the state of each signal, and optionally, the port associated with a signal. Symbols are encoded as follows:

General Form: Ta Ab (Cb)

Where:

(1) T is a constant.

(2) a represents any one of the following symbols:

Symbol	*Meaning*
c	Clock
d	Delay
f	Fall Time
h	Hold Time
r	Rise Time
s	Setup Time
w	Width

(3) A,C represent any of the following signal names:

Symbol	*Signal Name*
A	Address Strobe
B	$\overline{BSY}$, Busy
C	Clock
D*	Data In or the address at the master port.
E	$E/\overline{D}$, Enable/Disable
F*	Flag ($\overline{MFLG}$, $\overline{SFLG}$, or ($\overline{AFLG}$)
G*	Data Strobe ($\overline{MDS}$, $\overline{SDS}$, or $\overline{ASTB}$)
K	$K/\overline{D}$, Key/Data
M	$C/\overline{K}$, Control/Key Mode
N	$S/\overline{S}$, Start/Stop
P	$\overline{PAR}$, Parity
Q*	Data Out (master or slave port)
R	$\overline{CP}$, Clock Pulse
S*	Chip Select (master or slave port)
W	$MR/\overline{W}$, Master Port read/write

Timing Requirements (Continued)

(4) b represents any one of the following signal state descriptors (symbol).

Symbol	*State Indicated*
h	High
l	Low
v	Valid
x	Invalid
z	High Impedance

*These signal names may be modified by the following optional numeric port identifiers:

Identifier	*Port*
1	Master Port
2	Slave Port
3	AUX (Key) Port

For example: D1 specifies data in at Master Port; F2 specifies Slave Port flag-SFLG.

T-52-33-17

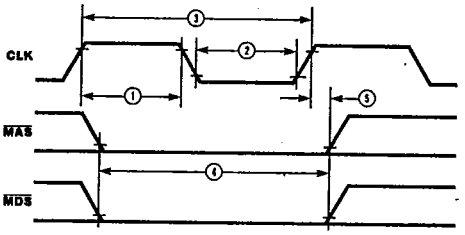


Figure 8. Clock and Reset

MAXIMUM RATINGS (Above which useful life may be impaired)

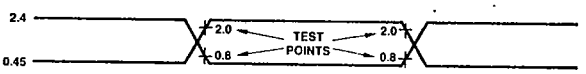
Storage Temperature	−65 to +150°C
Ambient Temperature Under Bias	0 to +70°C
Voltage on Any Pin with Respect to Ground	−0.5 to +7.0V
Power Dissipation	1.5W

The products described by this specification include internal circuitry designed to protect input devices from damaging accumulations of static charge. It is suggested nevertheless, that conventional precautions be observed during storage, handling and use in order to avoid exposure to excessive voltages.

Z8068, Z9518 ELECTRICAL CHARACTERISTICS (over operating range unless otherwise specified)

T_A = 0 to 70°C, V_{CC} = +5.0V ±5%, V_{SS} = 0V

Parameters	Description	Test Conditions	Min	Typ	Max	Units
V_{IL}	Input Low Voltage		−0.5		.8	Volts
V_{IH}	Input High Voltage		2.2		V_{CC}	Volts
V_{OL}	Output Low Voltage	I_{OL} = 3.2mA			.40	Volts
V_{OH}	Output High Voltage	I_{OH} = −400μA	2.4			Volts
I_I	Input Leakage Current	$V_{SS} \leq V_{IN} \leq V_{CC}$			±10	μA
I_{OZ}	Output Leakage Current	V_{SS} + .40 ≤ $V_{IN} \leq V_{CC}$			±10	μA
I_{CC}	Supply Current (AVER.)			150	250	mA



INPUT WAVEFORMS FOR A.C. TESTS

Z8068/Z9518 SWITCHING CHARACTERISTICS (Note 1)

The table below specifies the guaranteed performance of this device over the commercial operating range of 0 to +70°C with V_{CC} from 4.75 to 5.25V. All data are in nanoseconds. Switching tests are made with inputs and outputs measured at 0.8V for a LOW and 2.0V for a HIGH. Outputs are fully loaded, with $C_L \geq$ 50pF. See switching waveform figures following table for graphic illustration of timing parameters.

SWITCHING CHARACTERISTICS over operating range

Parameter	Number	Description	Z8068 Min	Z8068 Typ	Z8068 Max	Z9518 Min	Z9518 Typ	Z9518 Max	Units
Clock									
TWH	1	Clock Width (HIGH)	115			150			ns
TWL	2	Clock Width (LOW)	115			150			ns
TC	3	Clock HIGH to Next Clock HIGH (Clock Cycle)	250		1000	320		1000	ns
Reset									
TG1LG1H	5	$\overline{MDS} \cdot \overline{MAS}$ LOW to $\overline{MDS} \cdot \overline{MAS}$ HIGH (Reset Pulse Width)	TC			TC			ns
TCHG1H	6	Clock HIGH to $\overline{MDS} \cdot \overline{MAS}$ HIGH	0		50	0		50	ns
Direct Control Mode									
TNLMH	9	S/$\overline{S}$ LOW to C/$\overline{K}$ HIGH (Setup)	3TC			3TC			ns
TKLMH	10	K/$\overline{D}$ LOW to C/$\overline{K}$ HIGH (Setup)	3TC			3TC			ns
TMHNH	11	C/$\overline{K}$ HIGH to S/$\overline{S}$ HIGH	6TC			6TC			ns
TMHKH	12	C/$\overline{K}$ HIGH TO K/$\overline{D}$ HIGH	6TC			6TC			ns
TEVKH	14	E/$\overline{D}$ VALID to K/$\overline{D}$ HIGH (Setup)	3TC			3TC			ns
TKHRL	15	K/$\overline{D}$ HIGH to $\overline{CP}$ LOW			300			300	ns
TKLEX	17	K/$\overline{D}$ LOW to E/$\overline{D}$ INVALID (Hold)	TC			TC			ns
TCLNV	19	Clock LOW to S/$\overline{S}$ VALID	20		80	20		80	ns
TEVNH	20	E/$\overline{D}$ VALID to S/$\overline{S}$ HIGH (Setup)	3TC			3TC			ns
TNHF1L	21	S/$\overline{S}$ HIGH to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Input Flag)			230			300	ns
TCHF1L	22	Clock HIGH to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Input Flag) (Note 2)			230			300	ns
TCHBL	24	Clock HIGH to $\overline{BSY}$ LOW			300			400	ns
TCLBH	25	Clock LOW to $\overline{BSY}$ HIGH			230			300	ns
TCHF1L	27	Clock HIGH to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Output Flag)			230			300	ns
TNLF1H	28	S/$\overline{S}$ LOW to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Port Input Flag) (Note 3)			230			300	ns
Multiplexed Control Mode – Master Port									
TWA	32	$\overline{MAS}$ Width (LOW)	80			115			ns
TS1LAH	34	$\overline{MCS}$ LOW to $\overline{MAS}$ HIGH (Setup)	0			0			ns
TAHS1H	35	$\overline{MAS}$ HIGH to $\overline{MCS}$ HIGH (Hold)	60			60			ns
TD1VAH	36	Address-In VALID to $\overline{MAS}$ HIGH (Address Setup Time)	55			90			ns
TAHD1X	37	$\overline{MAS}$ HIGH to Address-In INVALID (Address Hold Time)	60			60			ns

AC SWITCHING CHARACTERISTICS

Parameter	Number	Description		Z8068 Min	Z8068 Typ	Z8068 Max	Z9518 Min	Z9518 Typ	Z9518 Max	Units
Master (Slave) Port Read/Write										
TS1LG1L	40	$\overline{MCS}$ ($\overline{SCS}$) LOW to $\overline{MDS}$ ($\overline{SDS}$) LOW (Select Setup) (Note 4)		100			100			ns
TG1HS1H	41	$\overline{MDS}$ ($\overline{SDS}$) HIGH to $\overline{MCS}$ ($\overline{SCS}$) HIGH (Select Hold Time) (Note 4)		25			25			ns
TWVG1L	42	MR/$\overline{W}$ VALID to $\overline{MDS}$ LOW (Setup)		100			100			ns
TG1HWX	43	$\overline{MDS}$ HIGH to MR/$\overline{W}$ INVALID (Hold)		25			25			ns
TG1LG1H	44	$\overline{MDS}$ ($\overline{SDS}$) LOW to $\overline{MDS}$ ($\overline{SDS}$) HIGH	Width – Write, Data Read	125		1000	160		1000	ns
			Width – Status Register Read	200		1000	300		1000	
TCLG1H	45	Clock LOW to $\overline{MDS}$ ($\overline{SDS}$) HIGH (Note 11)		0		TWL – 65	0		TWL – 100	
TGIHG1L	46	$\overline{MDS}$ ($\overline{SDS}$) HIGH to $\overline{MDS}$ ($\overline{SDS}$) LOW (Data Strobe Recovery Time)		125			160			ns
TD1VG1H	47	Write-Data VALID $\overline{MDS}$ ($\overline{SDS}$) HIGH	Setup Time – Key Load (Note 8)	125			160			ns
			Setup Time – Data Write	125			160			
			Setup Time – Command/ Mode Register Write	125			160			
TG1HD1X	48	$\overline{MDS}$ ($\overline{SDS}$) HIGH to Write-Data INVALID (Hold Time – All Writes)		25			25			ns
TG1LQ1V	49	$\overline{MDS}$ ($\overline{SDS}$) LOW to Read-Data VALID	Read Access Time – Status Register			200			300	ns
			Read Access Time – Data			120			150	
TG1HQ1V	50	$\overline{MDS}$ ($\overline{SDS}$) HIGH to Read-Data INVALID (Read Hold Time)		5			5			ns
TG1LF1H	51	$\overline{MDS}$ ($\overline{SDS}$) LOW to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Last Strobe) (Note 5)				125			160	ns
TG1LRH	52	$\overline{MDS}$ HIGH to CP HIGH	Last Strobe, Key Load			TC+500			TC+500	ns
TG1HNL	53	$\overline{MDS}$ ($\overline{SDS}$) HIGH to S/$\overline{S}$ LOW (Hold Time) (Note 9)		4TC			4TC			ns
TG1HPV	54	$\overline{MDS}$ HIGH to $\overline{PAR}$ VALID (Key Write)				200			250	ns
Auxiliary Port Key Entry										
TG3LG3H	61	$\overline{ASTB}$ LOW to $\overline{ASTB}$ HIGH (Width)		160			160			ns
TCLG3H	62	Clock LOW to $\overline{ASTB}$ HIGH		0		50	0		50	ns
TG3HG3L	63	$\overline{ASTB}$ HIGH to Next $\overline{ASTB}$ LOW (Recovery Time)		250			320			ns
TD3VG3H	64	Write-Data VALID to $\overline{ASTB}$ HIGH (Data Setup Time)		200			300			ns
TG3HD3X	65	$\overline{ASTB}$ HIGH to Write-Data INVALID (Data Hold Time)		80			80			ns
TG3HPV	66	$\overline{ASTB}$ HIGH to $\overline{PAR}$ VALID				200			300	ns
TG3LF3H	67	$\overline{ASTB}$ LOW to $\overline{AFLG}$ HIGH (Last Strobe)				230			300	ns

Notes:
1. All input transition times assumed ≤20ns.
2. Parameter TCHF1L applies to all input blocks except the first (when S/$\overline{S}$ first goes HIGH).
3. When S/$\overline{S}$ goes inactive (LOW) in direct control mode, the flag associated with the input port will turn off.
4. Direct control mode only.
5. In Cipher Feedback, the port flag ($\overline{MFLG}$ or $\overline{SFLG}$) will go inactive following the leading edge of the first data strobe ($\overline{MDS}$ or $\overline{SDS}$); in all other modes and operations, the flags go inactive on the eighth data strobe.
6. Do not remove K/$\overline{D}$ until CP is inactive (HIGH).
7. Do not change E/$\overline{D}$ until $\overline{MFLG}$ ($\overline{SFLG}$) is inactive (HIGH).
8. 300ns Min if parity check is needed.
9. In Cipher Feedback mode $\overline{BSY}$ must be inactive before S/$\overline{S}$ goes LOW.
10. $\overline{AFLG}$ must go active (LOW) before $\overline{ASTB}$ goes active (LOW).
11. This limit is valid when the clock frequency is 4MHz. At slower clock rates, the range is wider.

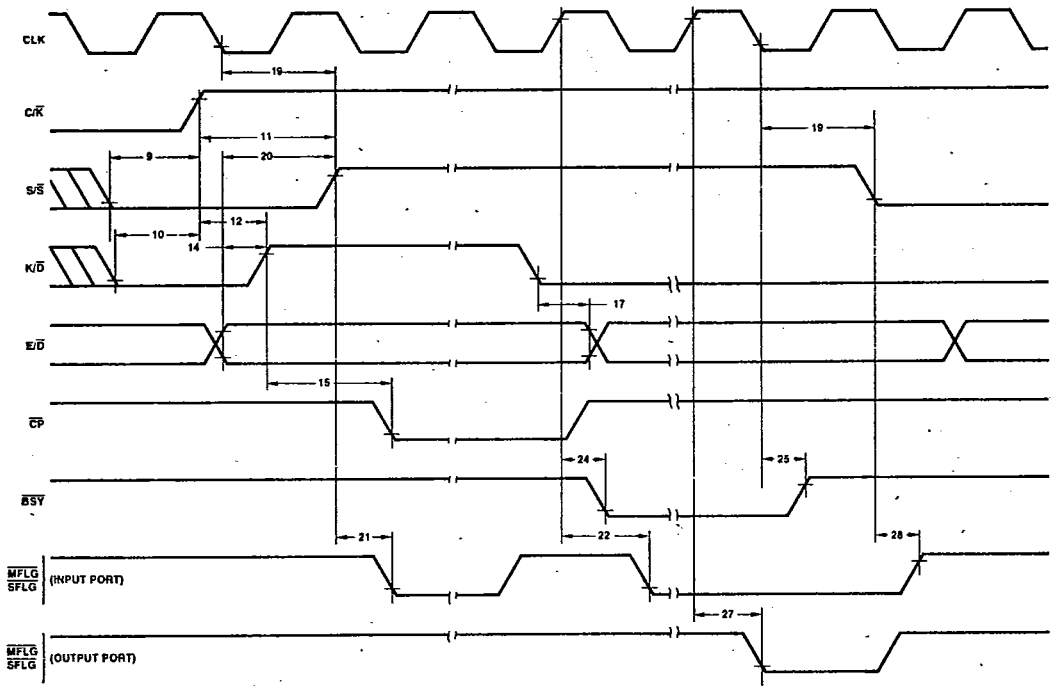


Figure 9. Control and Status Signals (Direct Control Mode)

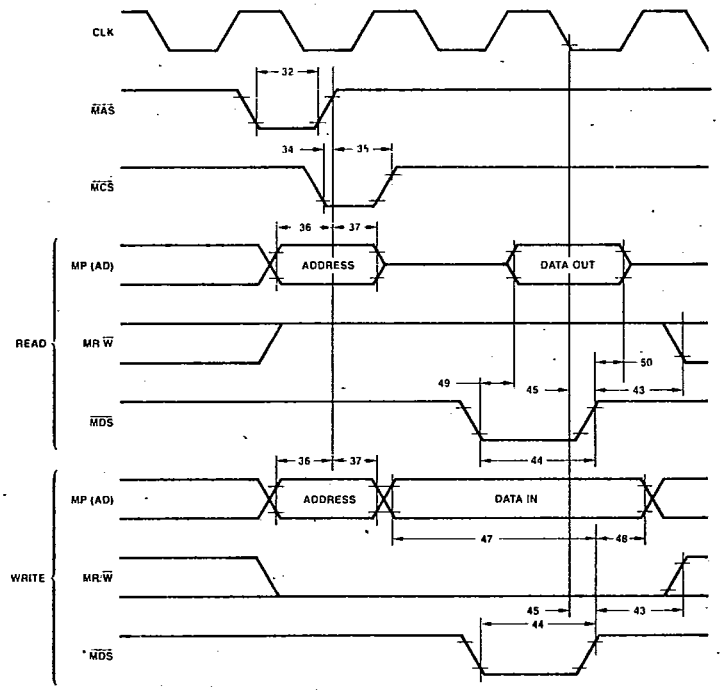


Figure 10. Master Port, Multiplexed Control Mode Read/Write Timing

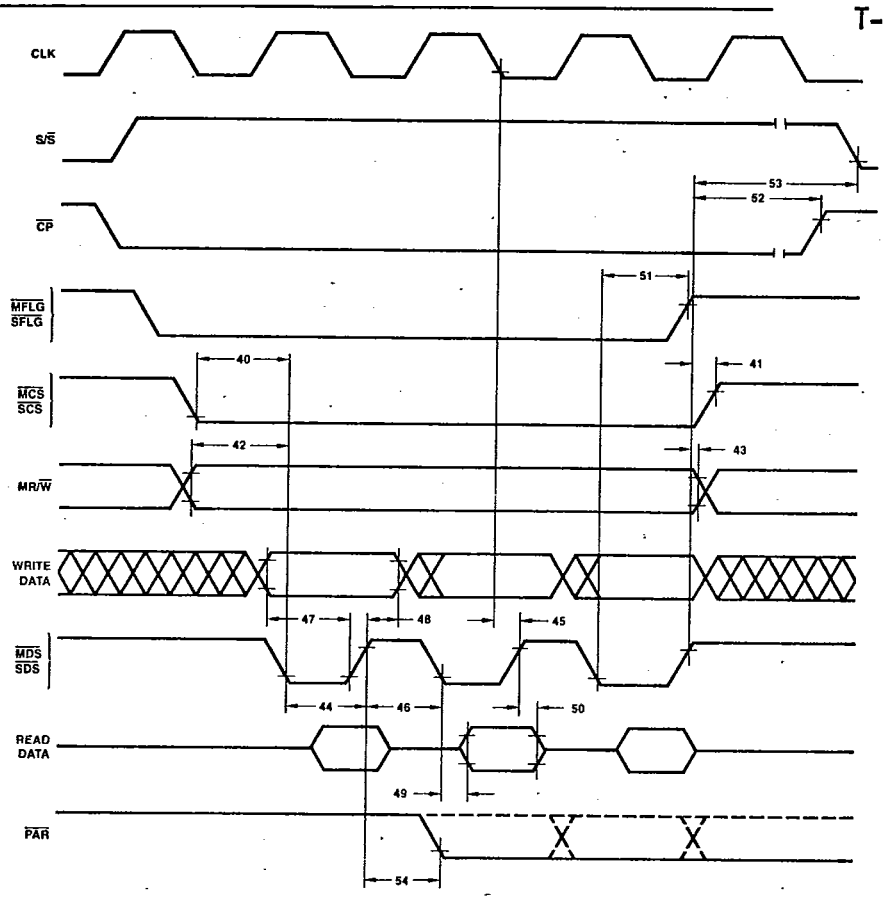


Figure 11. Master (Slave) Port Read/Write

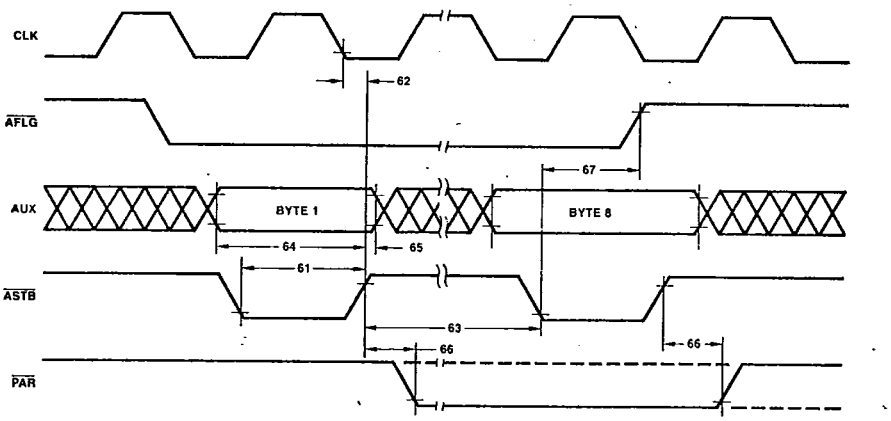
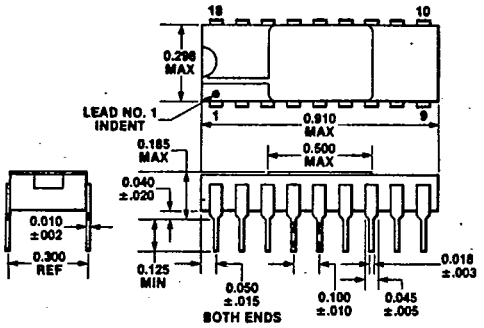


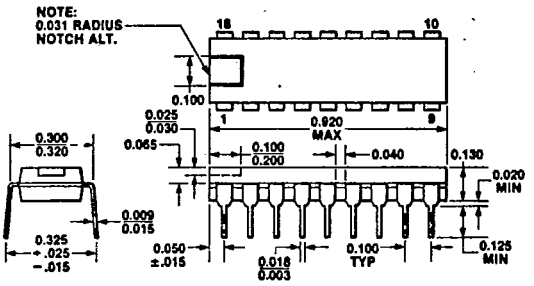
Figure 12. Auxiliary Port Key Entry

T-90-20

PACKAGE INFORMATION

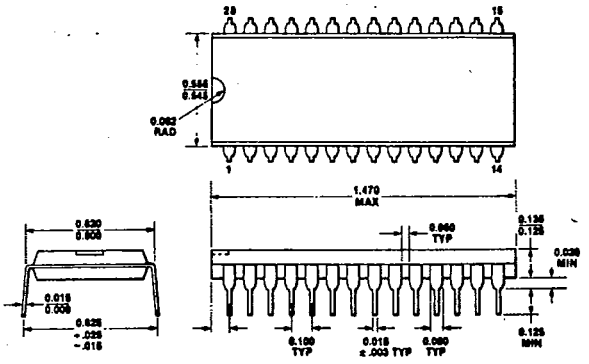


18-Pin Ceramic Package



18-Pin Plastic Package

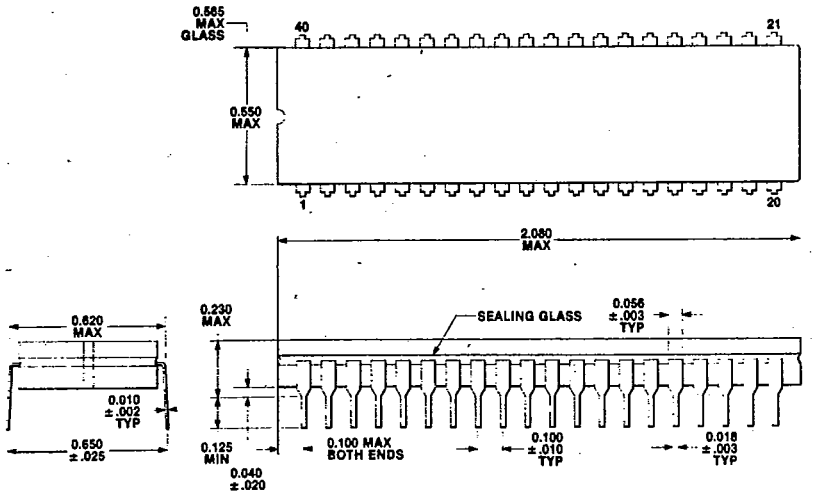
NOTE: Package dimensions are given in inches. To convert to millimeters, multiply by 25.4



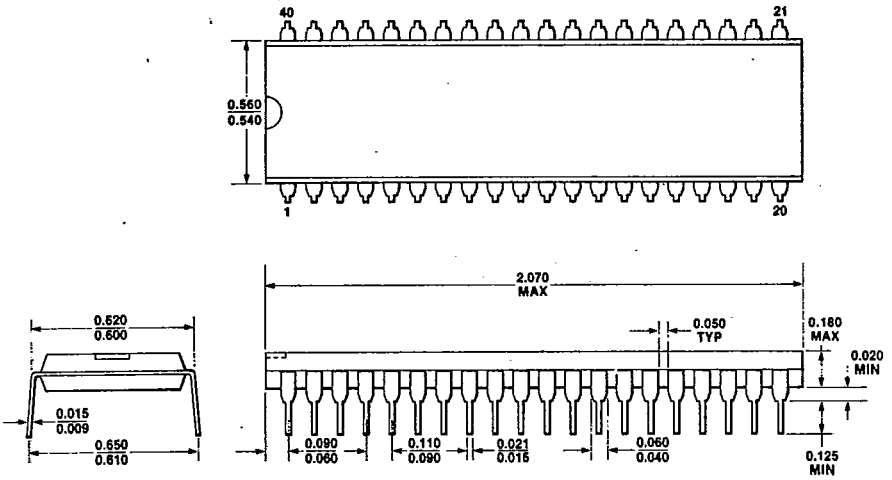
28-Pin Plastic Package

NOTE: Package dimensions are given in inches. To convert to millimeters, multiply by 25.4.

PACKAGE INFORMATION (Continued)



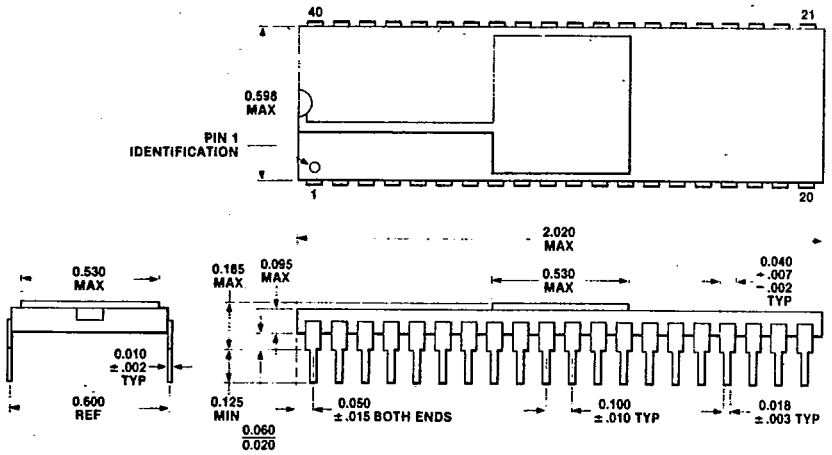
40-Pin Dual-In-Line Package (DIP), Cerdip



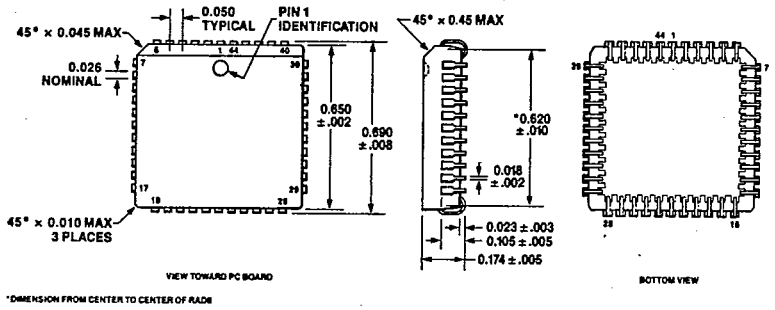
40-Pin Dual-In-Line Package (DIP), Plastic

NOTE: Package dimensions are given in inches. To convert to millimeters, multiply by 25.4.

PACKAGE INFORMATION (Continued)

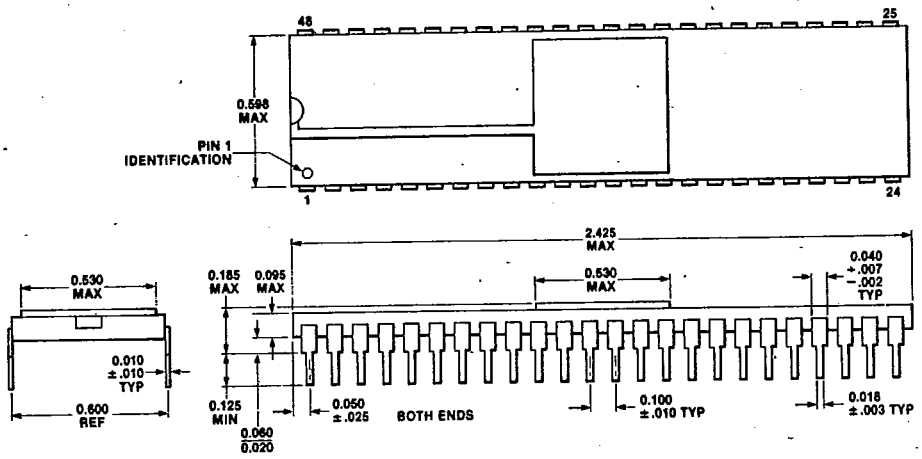


40-Pin Dual-In-Line Package (DIP), Ceramic

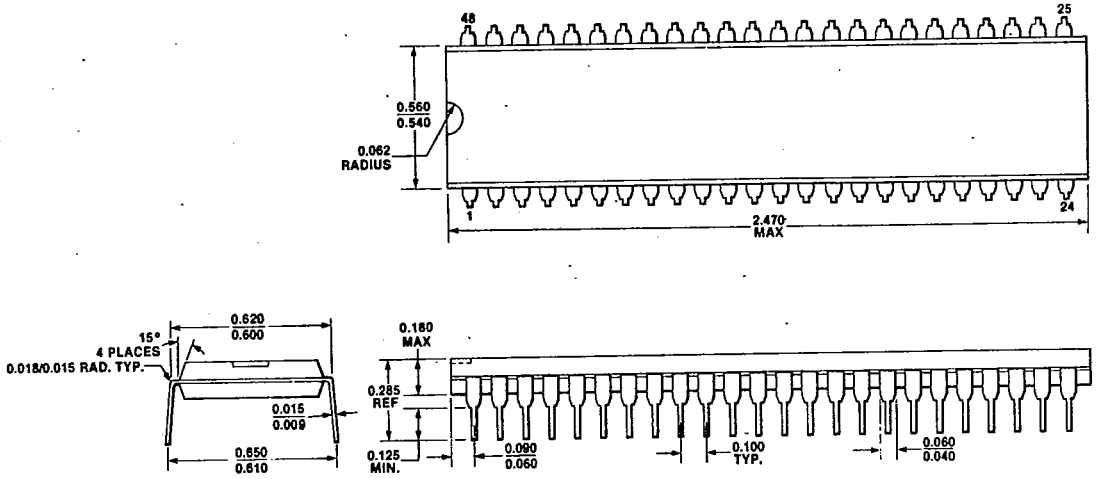


44-Pin Plastic Chip Carrier (PCC)

PACKAGE INFORMATION (Continued)

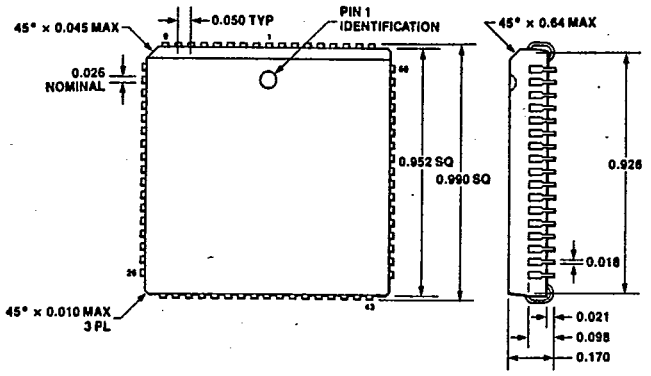


48-Pin Dual-in-Line Package (DIP), Ceramic

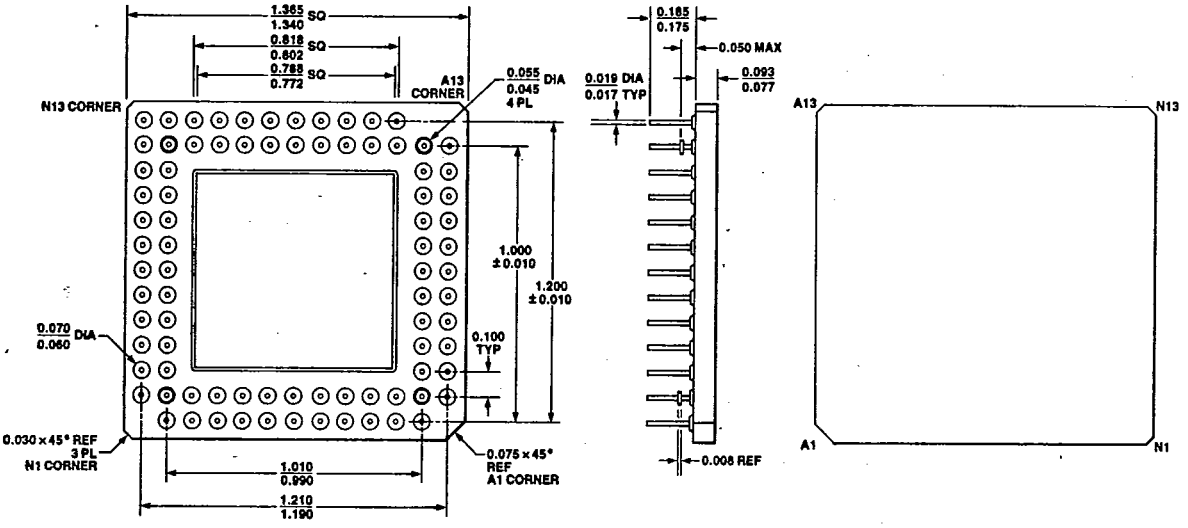


48-Pin Dual-in-Line Package (DIP), Plastic

PACKAGE INFORMATION (Continued)



68-Pin Plastic Chip Carrier (PCC)



84-Pin Grid Array (PGA), Bottom View

View toward PC Board

NOTE: Package dimensions are given in inches. To convert to millimeters, multiply by 25.4.