NEWBRIDGE MICROSYSTEMS

CA95C68/18/09

DES DATA CIPHERING PROCESSORS (DCP)

- **Encrypts/Decrypts data using National Bureau of Standards Data Encryption Standard (DES)**
- **High speed, pin and function compatible version of industry standard AMD AM9568, AM9518 and VLSI VM009**
- **Supports four standard ciphering modes: Electronic Code Book (ECB), Cipher Block Chaining (CBC), as well as 1 and 8 bit Cipher Feedback (CFB)**
- **Data rates greater than 11 Mbytes per second (25 MHz) in ECB or CBC modes**
- **Three separate registers for encryption, decryption and master keys improve system security and throughput by eliminating the need to reload keys frequently**
- **Fully static CMOS, TTL I/O compatible device, operates at up to 25MHz**
- **Low power consumption allows battery back-up of internal key registers**
- **Three separate programmable ports (master, slave and key data)**
- **Available in 44 pin PLCC and 40 pin PDIP and 44 pin TQFP packages**

The *Newbridge Microsystems* CA95C68/18/09 DES Data Ciphering Processors (DCPs) implement the National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46 (1-15-1977). The DCPs were designed to be used in a variety of environments where computer and communications security is essential.

The DCPs provide a high throughput rate (up to 11 Mbytes per second) using ECB or CBC modes of operation. The DCPs provide a unique 1 bit CFB mode as well as the standard 8 bit mode. Separate ports for key input, clear data and enciphered data enhance security for your application.

The system communicates with the DCP using commands entered in the Master Port or through auxiliary control lines. Once the DCP is set up, data can flow through at high speeds since input, output and ciphering activities are performed concurrently. External DMA control can easily be used to enhance throughput in many system configurations.

The CA95C68 is designed to interface directly to the iAPX86, 88 CPU bus, and with a minimum of external logic, to the 2900 and 8051 families of processors. The CA95C18 is designed to interface directly with Z8000, 68000 type bus interfaces.

The CA95C09 may be configured to behave as either the CA95C68 or the CA95C18 (see OPTION pin in Table 1), the only difference being the order of the signal names on the device package.

Table of Contents

NEWBS008

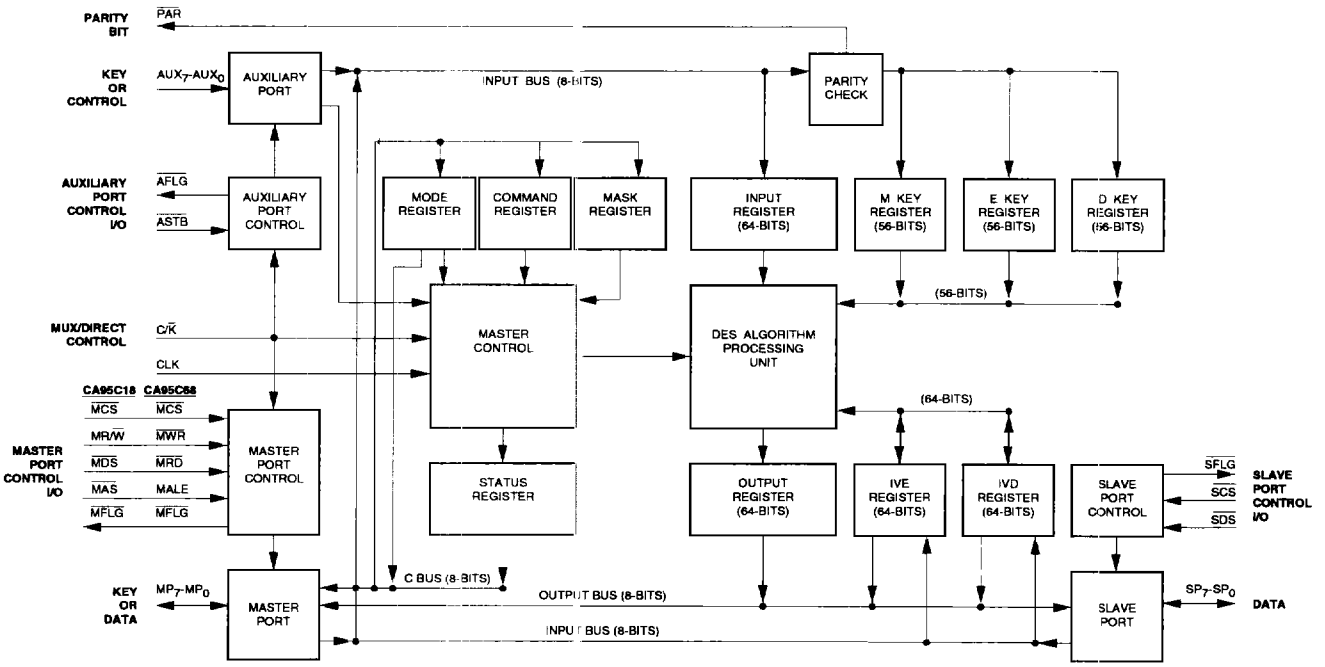


Figure 1 : CA95C68/18/09 Block Diagrams

Table 1 : CA95C68/18/09 Data Transfer Rates

Product Code	Data Transfer Rates ECB or CBC Mode (Mbytes per second)	System Clock (MHz)
CA95Cxx – 5	2.22	5
CA95Cxx – 10	4.44	10
CA95Cxx – 16	7.10	16
CA95Cxx – 20	8.88	20
CA95Cxx – 25	11.11	25

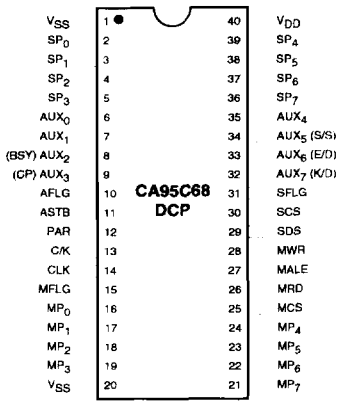


Figure 2 : CA95C68 40-Pin DPIP

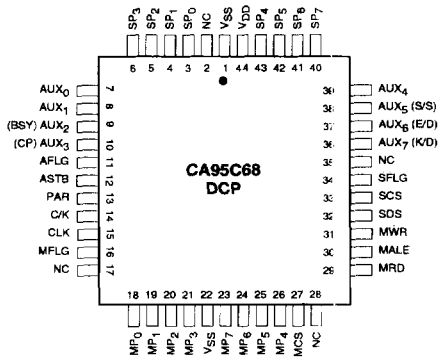


Figure 3 : CA95C68 44-Pin PLCC

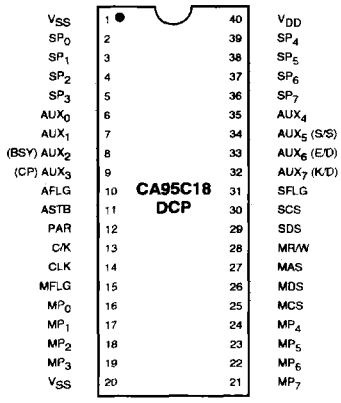


Figure 4 : CA95C18 40-Pin PDIP

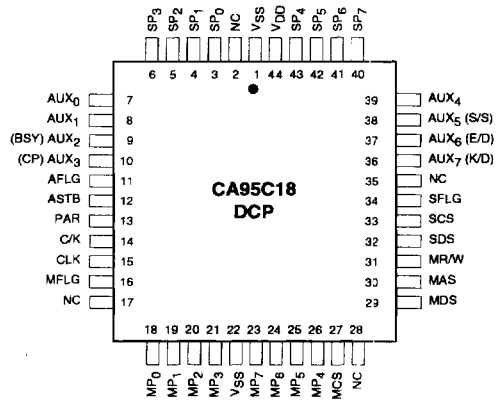


Figure 5 : CA95C18 44-Pin PLCC

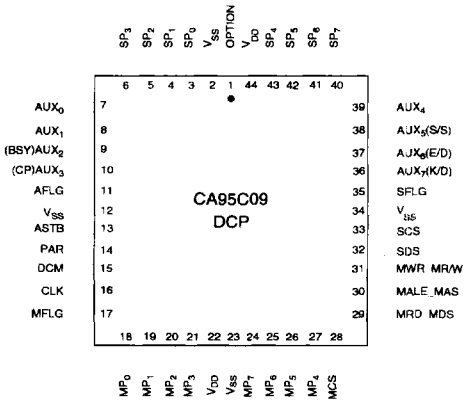


Figure 6 : CA95C09 44-Pin PLCC

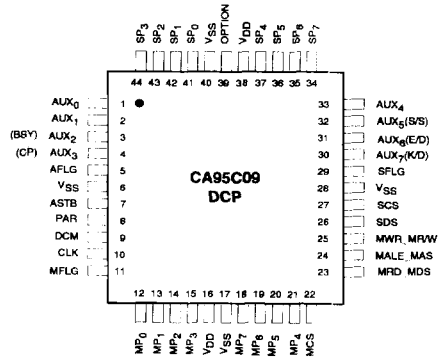


Figure 7 : CA95C09 44-Pin TQFP

Table 2 : Pin Description

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
CLK	14	15	16	10	I	**Clock**: An external timing source is input via this pin. The Master and Slave Port data strobe signals ($\overline{MWR}$, $\overline{MRD}$, $\overline{SDS}$ for CA95C68 and $\overline{MDS}$, $\overline{SDS}$ for CA95C18) must change synchronously with the clock input. In Direct Control Mode the AUX_5-$S/\overline{S}$ must also be synchronous. The output flags for the three ports ($\overline{AFLG}$, $\overline{MFLG}$, $\overline{SFLG}$) will all change synchronously with the clock.
$C/\overline{K}$	13	14	–	–	I	**Control/Key Mode Control**: This input controls the mode of operation of the DCP. The DCP enters into Multiplexed Control Mode when a low input is placed on the $C/\overline{K}$ pin, enabling programmed access to internal registers through the Master Port and enabling input of keys through the Auxiliary Port. In Direct Control Mode ($C/\overline{K}$ HIGH), 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 and Output Registers.
DCM	–	–	15	9	I	**Direct Control Mode**: (**For CA95C09**) This input functions identical to the $C/\overline{K}$ input. (See $C/\overline{K}$ pin description).
$MP_7 - MP_0$	21-24 19-16	23-26 21-18	24-27 21-18	18-21 15-12	I/O	**Master Port Bus**: These eight bi-directional signals are used to input and output data, as well as specify the internal register addresses in Multiplexed Control Mode. The Master Port provides software access to the Status, Command, Mode, Mask, Input and Output Registers. For the CA95C68, the tri-state Master Port outputs will be enabled only when the Master Port is selected by Master Port Chip Select ($\overline{MCS}$) LOW, and when Master Port Read ($\overline{MRD}$) is strobed LOW. For the CA95C18, the Master Port outputs are enabled when selected by $\overline{MCS}$, and when $MR/\overline{W}$ is HIGH and $\overline{MDS}$ is LOW. MP_0 is the low-order bit. Data and key information are entered into this port with the most significant byte first.
$\overline{MCS}$	25	27	28	22	I	**Master Port Chip Select**: This active LOW input 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 falling edge of Master Port Address Latch Enable (MALE). This latched level is maintained as long as MALE is LOW; when MALE is HIGH, the latch becomes transparent and the internal signal will follow the $\overline{MCS}$ input. No latching of $\overline{MCS}$ occurs in Direct Control Mode ($C/\overline{K}$ HIGH). The level on $\overline{MCS}$ is passed directly to the internal select circuitry regardless of the state of Master Port Address Latch Enable (MALE).

Table 2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
MALE	27	30	–	–	I	**Master Port Address Latch Enable**: **(For CA95C68)** In Multiplexed Control Mode (C/$\overline{K}$ LOW), an active HIGH signal on this pin indicates the presence of valid address and chip select information at the Master Port. This information will be latched internally on the falling edge of MALE. When C/$\overline{K}$ is HIGH (Direct Control Mode), MALE has no affect on DCP operation.
$\overline{MRD}$	26	29	–	–	I	**Master Port Read**: **(For CA95C68)** This active LOW input is used with a valid $\overline{MCS}$ to indicate that data is to be output on the Master Port bus. Master Port Read ($\overline{MRD}$) and Master Port Write ($\overline{MWR}$) are normally mutually exclusive; if both become active simultaneously, the DCP is reset to ECB Mode and all flags go inactive.
$\overline{MWR}$	28	31	–	–	I	**Master Port Write**: **(For CA95C68)** This active low input signal indicates to the DCP that valid data is present on MP_7-MP_0 for an input operation. The rising edge of $\overline{MWR}$ latches the data into the selected internal register. If $\overline{MWR}$ and $\overline{MRD}$ both go LOW simultaneously, the DCP is reset.
$\overline{MAS}$	27	30	–	–	I	**Master Port Address Strobe**: **(For CA95C18)** In Multiplexed Control Mode (C/$\overline{K}$ HIGH), a LOW on $\overline{MAS}$ indicates the presence of a valid chip select signal and address information. This information will be latched on the rising edge of $\overline{MAS}$. In Direct Control Mode, $\overline{MAS}$ has no affect on the DCP operation. The DCP will be reset if $\overline{MAS}$ and $\overline{MDS}$ both go low simultaneously.
$\overline{MDS}$	26	29	–	–	I	**Master Port Data Strobe**: **(For CA95C18)** This active low input is used in conjunction with a valid Master Port Chip Select ($\overline{MCS}$) to indicate that valid data is present on the MP_7-MP_0 bus for an input operation or that data is to be placed on the Master Port Bus during output. $\overline{MDS}$ and $\overline{MAS}$ are mutually exclusive; if they both go active simultaneously, the DCP is reset to ECB mode and all flags go inactive.
MR/$\overline{W}$	28	31	–	–	I	**Master Port Read/Write**: **(For CA95C18)** This input signal indicates to the DCP whether the current Master Port operation is a read (HIGH) where data is transferred from the device, or a write (LOW) where data is stored to an internal register. MR/$\overline{W}$ is not latched internally and must be held stable while $\overline{MDS}$ is LOW.

Table 2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
$\overline{MRD}$ – $\overline{MDS}$	–	–	29	23	I	**Master Port Read or Master Port Data Strobe**: (**For CA95C09**) When the OPTION pin is HIGH this input functions as $\overline{MRD}$. When the OPTION pin is LOW this input functions as $\overline{MDS}$. (See appropriate pin description).
MALE – $\overline{MAS}$	–	–	30	24	I	**Master Port Address Latch Enable or Master Port Address Strobe**: (**For CA95C09**) When the OPTION pin is HIGH this input functions as MALE and when OPTION is LOW it functions as $\overline{MAS}$. (See the appropriate pin description).
$\overline{MWR}$ – MR/$\overline{W}$	–	–	31	25	I	**Master Port Write or Master Port Read/Write**: (**For CA95C09**) When the OPTION pin is HIGH this input functions as $\overline{MWR}$ and when OPTION is LOW it functions as MR/$\overline{W}$. (See the appropriate pin description).
$\overline{MFLG}$	15	16	17	11	O	**Master Port Flag**: This active LOW flag indicates the need for a data transfer into or out of the Master Port during normal ciphering operation. The Master Port will be associated with either the Input or Output Register depending upon the setting of the Control bits in the Mode Register (See Register Description). If data is to be transferred through the Master Port to the Input Register, then $\overline{MFLG}$ reflects the contents of the Input Register. After any Start command is entered, $\overline{MFLG}$ will go 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; see Functional Description). Whenever the Output Register is not empty $\overline{MFLG}$ will be active (LOW). In single port mode of operation, the Master Port flag reflects the contents of the Input Register, while the Slave Port Flag ($\overline{SFLG}$, see below) is associated with the Output Register.
SP_7–SP_0	36-39 5-2	40-43 6-3	40-43 6-3	34-37 44-41	I/O	**Slave Port Bus**: This 8 bit bi-directional data bus provides a second input/output interface to the DCP, allowing overlapped input, ciphering and output operations. The tri-state Slave Port will be accessed only when the Mode Register is configured for dual port operation, Slave Port Chip Select ($\overline{SCS}$) and Slave Port Data Strobe ($\overline{SDS}$) are both LOW and $\overline{SFLG}$ =0. Data entered or retrieved through this port is the most significant byte in/out first (SP_7 is the most significant bit).

Table 2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
$\overline{SCS}$	30	33	33	27	I	**Slave Port Chip Select**: This active LOW signal is logically combined with the Slave Port Data Strobe ($\overline{SDS}$) to facilitate Slave Port data transfers in a bus environment. $\overline{SCS}$ is not latched internally, and may be tied permanently LOW without impairing Slave Port operation.
$\overline{SDS}$	29	32	32	26	I	**Slave Port Data Strobe**: This active LOW input, in conjunction with Slave Port Chip Select ($\overline{SCS}$) LOW indicates to the DCP that valid data is on the SP_7-SP_0 lines for an input operation, or that data is to be driven onto SP_7-SP_0 lines for output. The direction of data flow is determined by Control bits in the Mode Register. (See Register Description).
$\overline{SFLG}$	31	34	35	29	O	**Slave Port Flag**: This active LOW output indicates the state of either the Input Register or the Output Register, depending on the Mode Register configuration. In single port configuration, $\overline{SFLG}$ will go active whenever the Output Register is not empty during normal processing. In dual port configuration, $\overline{SFLG}$ will reflect the content of whichever register is associated with the Slave Port. If the Input Register is assigned to the Slave Port, $\overline{SFLG}$ will go active whenever the Input Register is not full, once any of the Start commands has been entered; $\overline{SFLG}$ will be forced inactive if any other command is entered. Conversely, if the Slave Port is assigned to the Output Register, $\overline{SFLG}$ will go active whenever the Output Register is not empty.
AUX_7-AUX_0	32-35 9-6	36-39 10-7	36-39 10-7	30-33 4-1	I/O	**Auxiliary Port Bus**: In Multiplexed Control Mode (C/$\overline{K}$ LOW), these eight lines form a key byte input port which may be used to enter the Master and Session Keys. The Master Key can only be entered through this port but Session Keys may alternatively 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 of the key 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 (they may be tied HIGH) and the other pins are defined on the following pages.
AUX_5 –S/$\overline{S}$	34	38	38	32	I	**Start/Stop**: In Direct Control Mode, when this pin goes LOW (Stop) the DCP will follow the sequence that would normally occur when a Stop Command is entered. Conversely, when this input goes HIGH, a sequence equivalent to a Start Encryption or Start Decryption command will be followed. At the time AUX_5-S/$\overline{S}$ goes HIGH, the level on AUX_6-E/$\overline{D}$ selects either the Start Encryption or Start Decryption ciphering operation.
AUX_6 –E/$\overline{D}$	33	37	37	31	I	**Encrypt/Decrypt**: In Direct Control Mode, this input specifies whether the ciphering algorithm is to encrypt (E/$\overline{D}$ HIGH) or decrypt (E/$\overline{D}$ LOW) when AUX_5-S/$\overline{S}$ goes HIGH to initiate a normal data ciphering operation. When AUX_7-K/$\overline{D}$ goes HIGH, initiating 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. Corrupted data in the internal registers will occur if the proper level on AUX_6-E/$\overline{D}$ is not maintained during loading or ciphering operations.

Table 2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
AUX_7 -K/$\overline{D}$	32	36	36	30	I	**Key/Data**: In Direct Control Mode, when this signal goes HIGH, the DCP initiates a key-data input sequence as if a Clear E (or D) Key through the Master Port command had been entered. The level on AUX_6-E/$\overline{D}$ will determine whether the subsequently entered clear-key bytes are written into the E Key Register (E/$\overline{D}$ 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 be inactive (LOW) and remain in this state until the first signal returns to an inactive state. Whenever a transition occurs on C/$\overline{K}$ (switching between Direct Control Mode and Multiplexed Control Mode) both of these signals must be inactive (LOW).
AUX_2 -$\overline{BSY}$	8	9	9	3	O	**Busy**: In Direct Control Mode, this active LOW status output gives a hardware indication that the ciphering algorithm is in operation. This status line 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 -$\overline{CP}$	9	10	10	4	0	**Command Pending**: In Direct Control Mode, this active LOW status output gives a hardware indication that the DCP is ready to accept input of key bytes following a LOW-to-HIGH transition on AUX_7-K/$\overline{D}$. This signal line is driven by the $\overline{CP}$ bit in the Status Register, such that when the $\overline{CP}$ bit is "1" (active), AUX_3-$\overline{CP}$ is LOW.
$\overline{ASTB}$	11	12	13	7	I	**Auxiliary Port Strobe**: The rising edge of $\overline{ASTB}$ strobes the key-data on pins AUX_7-AUX_0 into the appropriate internal key register in Multiplexed Control Mode (C/$\overline{K}$ LOW). This input is ignored unless $\overline{AFLG}$ and C/$\overline{K}$ are both LOW. One byte of key-data (most significant byte first) is entered on each $\overline{ASTB}$.

Table 2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
$\overline{AFLG}$	10	11	11	5	O	**Auxiliary Port Flag**: This active LOW output signal indicates that the DCP is expecting key-data to be entered on the Auxiliary Port Bus. This can occur only when C/$\overline{K}$ is LOW (Multiplexed Control Mode) and a Load Key Through AUX Port command has been entered. $\overline{AFLG}$ will remain active (LOW) during input of all eight bytes, and will go inactive with the falling edge of the eighth $\overline{ASTB}$.
$\overline{PAR}$	12	13	14	8	O	**Parity**: 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 a "1" and $\overline{PAR}$ goes active (LOW). (See Parity Checking of Keys.). The Parity bit is the least significant bit of the key byte.
OPTION	–	–	1	39	I	**Option**: (**For CA95C09**) This input allows the user to configure the Master Port Control interface to function as either a CA95C68 or a CA95C18. When the OPTION pin is tied to V_{DD}, the device will function with the interface of a CA95C68. Conversely, tying the OPTION pin to V_{SS} will cause the DCP to function as a CA95C18. This OPTION pin must be tied to either V_{SS} or V_{DD}, or erratic operation of the device will occur. The CA95C09 DCP will perform identically to the CA95C68 or the CA95C18 (depending on the OPTION pin) with the only difference being the order of the signal names on the device package.
V_{DD}	40	44	44,22	16, 38	PWR	**Power Supply**: +5 Volts.
V_{SS}	1, 20	1, 22	2, 12 23, 34	6, 17 28, 40	GND	**Ground**: 0 Volts.

Table 3a: AC Characteristics (T_A + 0 to 70° C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V)

Number	Description
Clock	
t_1	CLK Width HIGH (t_{WH})
t_2	CLK Width LOW (t_{WL})
t_3	CLK HIGH to Next Clock HIGH (Clock Cycle, t_C)
Reset	
t_5	$\overline{MRD}$ • $\overline{MWR}$ LOW to $\overline{MRD}$ • $\overline{MWR}$ HIGH (Reset Pulse Width), (Note 11)
Direct Control Mode	
t_9	S/$\overline{S}$ LOW to C/$\overline{K}$ HIGH (Setup), (Note 11)
t_{10}	K/$\overline{D}$ LOW to C/$\overline{K}$ HIGH (Setup), (Note 11)
t_{11}	C/$\overline{K}$ HIGH to S/$\overline{S}$ HIGH (Note 11)
t_{12}	C/$\overline{K}$ HIGH to K/$\overline{D}$ HIGH (Note 11)
t_{14}	E/$\overline{D}$ VALID to K/$\overline{D}$ HIGH (Setup) (Note 11)
t_{15}	K/$\overline{D}$ HIGH • CLK ↓ to $\overline{CP}$ LOW
t_{17}	K/$\overline{D}$ LOW to E/$\overline{D}$ INVALID (Hold), (Note 11)
t_{20}	E/$\overline{D}$ VALID to S/$\overline{S}$ HIGH (Setup), (Note 11)
t_{21}	S/$\overline{S}$ HIGH • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Input Flag)
t_{23}	S/$\overline{S}$ LOW to E/$\overline{D}$ INVALID (Hold) (Note 11)
t_{24}	CLK LOW to $\overline{BSY}$ LOW
t_{25}	CLK LOW to $\overline{BSY}$ HIGH
t_{27}	ALGORITHM completed • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Output Flag)
t_{28}	S/$\overline{S}$ LOW • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Port Input Flag), (Note 3)
Multiplexed Control Mode - Master Port	
t_{32}	For CA95C68: MALE Width (HIGH) For CA95C18: $\overline{MAS}$ Width (LOW)
t_{34}	For CA95C68: $\overline{MCS}$ LOW to MALE LOW (Setup) For CA95C18: $\overline{MCS}$ LOW to $\overline{MAS}$ HIGH (Setup)
t_{35}	For CA95C68: MALE LOW to $\overline{MCS}$ HIGH (Hold) For CA95C18: $\overline{MAS}$ HIGH to $\overline{MCS}$ HIGH (Hold)
t_{36}	For CA95C68: Address INVALID to MALE LOW (Address Setup Time) For CA95C18: Address INVALID to $\overline{MAS}$ HIGH (Address Setup Time)
t_{37}	For CA95C68: MALE LOW to Address INVALID (Address Hold Time) For CA95C18: $\overline{MAS}$ HIGH to Address INVALID (Address Hold Time)
Master/Slave Port Read/Write	
t_{40}	For CA95C68: $\overline{MCS}$ LOW to $\overline{MRD}$, $\overline{MWR}$ LOW (Select Setup), (Note 4) For CA95C18: $\overline{MCS}$ LOW to $\overline{MDS}$ LOW (Select Setup), (Note 4) For CA95C68/18: $\overline{SCS}$ LOW to $\overline{SDS}$ LOW (Select Setup)

Table 3b: AC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 5 %, V_{SS} = 0V

Number	5 MHz Limits		10 MHz Limits		16 MHz Limits		20 MHz Limits		25 MHz Limits		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
Clock											
t_1	85	–	40	–	27	–	20	–	17	–	ns
t_2	85	–	40	–	27	–	20	–	17	–	ns
t_3	200	–	100	–	62.5	–	50	–	40	–	ns
Reset											
t_5	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
Direct Control Mode											
t_9	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{10}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{11}	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	ns
t_{12}	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	ns
t_{14}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{15}	–	75	–	60	–	45	–	40	–	30	ns
t_{17}	40	–	20	–	15	–	10	–	5	–	ns
t_{20}	40	–	20	–	15	–	10	–	5	–	ns
t_{21}	–	75	–	60	–	45	–	40	–	30	ns
t_{23}	40	–	20	–	15	–	10	–	5	–	ns
t_{24}	–	75	–	60	–	45	–	40	–	30	ns
t_{25}	–	100	–	75	–	60	–	50	–	40	ns
t_{27}	–	75	–	60	–	45	–	40	–	30	ns
t_{28}	–	75	–	60	–	45	–	40	–	30	ns
Multiplexed Control Mode - Master Port											
t_{32}	75	–	50	–	30	–	20	–	12	–	ns
	75	–	50	–	30	–	20	–	12	–	ns
t_{34}	25	–	15	–	5	–	0	–	0	–	ns
	25	–	15	–	5	–	0	–	0	–	ns
t_{35}	35	–	30	–	20	–	15	–	10	–	ns
	35	–	30	–	20	–	15	–	10	–	ns
t_{36}	35	–	30	–	20	–	15	–	10	–	ns
	35	–	30	–	20	–	15	–	10	–	ns
t_{37}	35	–	30	–	20	–	15	–	15	–	ns
	35	–	30	–	20	–	15	–	15	–	ns
Master/Slave Port Read/Write											
t_{40}	30	–	20	–	10	–	5	–	0	–	ns
	30	–	20	–	10	–	5	–	0	–	ns
	30	–	20	–	10	–	5	–	0	–	ns

Table 3a: AC Characteristics (T_A + 0 to 70° C, V_{DD} = +5.0V ± 5 %, V_{SS} = 0V) Cont'd

Number	Description
Master/Slave Port Read/Write Cont'd	
t_{41}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$ HIGH to $\overline{MCS}$ HIGH (Select Hold), (Note 4) For CA95C18: $\overline{MDS}$ HIGH to $\overline{MCS}$ HIGH (Select Hold), (Note 4) For CA95C68/18: $\overline{SDS}$ HIGH to $\overline{SCS}$ HIGH (Select Hold)
t_{42}	MR/$\overline{W}$ VALID to $\overline{MDS}$ LOW (Setup)
t_{43}	$\overline{MDS}$ HIGH to MR/$\overline{W}$ INVALID (Hold)
t_{44}	For CA95C68: $\overline{MRD}$, $\overline{MRW}$ LOW to $\overline{MRD}$, $\overline{MRW}$ HIGH (Width-Write, Read) For CA95C18: $\overline{MDS}$ LOW to $\overline{MDS}$ HIGH (Width-Write, Read) For CA95C68/18: $\overline{SDS}$ LOW to $\overline{SDS}$ HIGH (Read, Write)
t_{45}	For CA95C68: CLK LOW to $\overline{MRD}$, $\overline{MWR}$ HIGH (Note 11) For CA95C18: CLK LOW to $\overline{MDS}$ HIGH (Note 11) For CA95C68/18: CLK LOW to $\overline{SDS}$ HIGH (Note 11)
t_{46}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$ HIGH to $\overline{MRD}$. $\overline{MWR}$ LOW (Data Strobe Recovery Time) For CA95C18: $\overline{MDS}$ HIGH to $\overline{MDS}$ LOW (Data Strobe Recovery Time) For CA95C68/18: $\overline{SDS}$ HIGH to $\overline{SDS}$ LOW (Data Strobe Recovery Time)
t_{47}	For CA95C68: Write Data VALID to $\overline{MWR}$ ($\overline{SDS}$) HIGH (Write Setup Time) For CA95C18: Write Data VALID to $\overline{MDS}$ ($\overline{SDS}$) HIGH (Write Setup Time)
t_{48}	For CA95C68: $\overline{MWR}$ HIGH to Write Data INVALID (Hold Time) For CA95C18: $\overline{MDS}$ HIGH to Write Data INVALID (Hold Time) For CA95C68/18: $\overline{SDS}$ HIGH to Write Data INVALID (Hold Time)
t_{49}	For CA95C68: $\overline{MRD}$ LOW to Read Data VALID (Read Access Time) For CA95C18: $\overline{MDS}$ LOW to Read Data VALID (Read Access Time) For CA95C68/18: $\overline{SDS}$ LOW to Read Data VALID (Read Access Time)
t_{50}	For CA95C68: $\overline{MRD}$ ($\overline{SDS}$) HIGH to Read Data INVALID (Hold Time) For CA95C18: $\overline{MRD}$ ($\overline{SDS}$) HIGH to Read Data INVALID (Hold Time)
t_{51}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$ LOW • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Last Strobe), (Note 5) For CA95C18: $\overline{MDS}$ LOW • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Last Strobe), (Note 5)
t_{52}	For CA95C68: $\overline{MWR}$ HIGH • CLK ↓ to $\overline{CP}$ HIGH (Note 4,11), (Last Strobe-Key Load) For CA95C18: $\overline{MDS}$ HIGH • CLK ↓ to $\overline{CP}$ HIGH (Note 4,11), (Last Strobe-Key Load)
t_{53}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$ ($\overline{SDS}$) HIGH to S/$\overline{S}$ LOW (Hold Time) (Note 11) For CA95C18: $\overline{MDS}$ ($\overline{SDS}$) HIGH to S/$\overline{S}$ LOW (Hold Time) (Note 11)
t_{54}	For CA95C68: $\overline{MWR}$ HIGH • CLK ↓ to $\overline{PAR}$ VALID (Key Write) For CA95C18: $\overline{MDS}$ HIGH • CLK ↓ to $\overline{PAR}$ VALID (Key Write)
t_{55}	For CA95C68: S/$\overline{S}$ HIGH to $\overline{MRD}$, $\overline{MWR}$, ($\overline{SDS}$) HIGH (Setup Time) (Note 11) For CA95C18: S/$\overline{S}$ HIGH to $\overline{MDS}$, $\overline{SDS}$ HIGH (Setup Time) (Note 11)
t_{57}	$\overline{MRD}$, $\overline{MWR}$ HIGH to MALE HIGH
t_{58}	MALE LOW to $\overline{MRD}$, $\overline{MWR}$ LOW
t_{59}	Address Valid to $\overline{MRD}$, $\overline{MWR}$ LOW (to guarantee t_{49})
t_{60}	MALE HIGH to $\overline{MRD}$, $\overline{MWR}$ LOW

Table 3b: AC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 5 %, V_{SS} = 0V Cont'd

Number	5 MHz Limits		10 MHz Limits		16 MHz Limits		20 MHz Limits		25 MHz Limits		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
Master/Slave Port Read/Write Cont'd											
t_{41}	35	–	30	–	20	–	10	–	5	–	ns
	35	–	30	–	20	–	10	–	5	–	ns
	35	–	30	–	20	–	10	–	5	–	ns
t_{42}	35	–	30	–	20	–	15	–	10	–	ns
t_{43}	35	–	30	–	20	–	15	–	15	–	ns
t_{44}	140	–	70	–	50	–	35	–	30	–	ns
	140	–	70	–	50	–	35	–	30	–	ns
	140	–	70	–	50	–	35	–	30	–	ns
t_{45}	5	t_C -25	5	t_C -25	5	t_C -25	5	t_C -20	3	t_C -20	ns
	5	t_C-25	5	t_C-25	5	t_C-25	5	t_C-20	3	t_C-20	ns
	5	t_C-25	5	t_C-25	5	t_C-25	5	t_C-20	3	t_C-20	ns
t_{46}	30	–	20	–	15	–	10	–	10	–	ns
	30	–	20	–	15	–	10	–	10	–	ns
	30	–	20	–	15	–	10	–	10	–	ns
t_{47}	60	–	30	–	20	–	15	–	10	–	ns
	60	–	30	–	20	–	15	–	10	–	ns
t_{48}	20	–	20	–	15	–	15	–	10	–	ns
	20	–	20	–	15	–	15	–	10	–	ns
	20	–	20	–	15	–	15	–	10	–	ns
t_{49}	–	60	–	50	–	45	–	35	–	35	ns
	–	60	–	50	–	45	–	35	–	35	ns
	–	60	–	50	–	45	–	35	–	35	ns
t_{50}	10	–	10	–	5	–	5	–	5	–	ns
	10	–	10	–	5	–	5	–	5	–	ns
t_{51}	–	75	–	50	–	40	–	35	–	30	ns
	–	75	–	50	–	40	–	35	–	30	ns
t_{52}	–	75	–	50	–	40	–	35	–	30	ns
	–	75	–	50	–	40	–	35	–	30	ns
t_{53}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{54}	–	75	–	50	–	40	–	35	–	30	ns
	–	75	–	50	–	40	–	35	–	30	ns
t_{55}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{57}	140	–	70	–	30	–	20	–	10	–	ns
t_{58}	80	–	40	–	20	–	15	–	10	–	ns
t_{59}	120	–	70	–	40	–	30	–	20	–	ns
t_{60}	110	–	100	–	50	–	35	–	25	–	ns

Table 3a: AC Characteristics (T_A + 0 to 70° C, V_{DD} = +5.0V ± 5 %, V_{SS} = 0V) Cont'd

Number	Description
Auxiliary Port Key Entry	
t_{61}	$\overline{ASTB}$ LOW to $\overline{ASTB}$ HIGH (Width)
t_{62}	CLK LOW to $\overline{ASTB}$ HIGH (Note 11)
t_{63}	$\overline{ASTB}$ HIGH to Next $\overline{ASTB}$ LOW (Recovery Time)
t_{64}	Write-Data VALID to $\overline{ASTB}$ HIGH (Data Setup TIme)
t_{65}	$\overline{ASTB}$ HIGH to Write-Data INVALID (Data Hold TIme)
t_{66}	$\overline{ASTB}$ HIGH • CLK ↓ to $\overline{PAR}$ VALID
t_{67}	$\overline{ASTB}$ LOW • CLK ↓ to $\overline{AFLG}$ HIGH (Last Strobe)

Table 3b: AC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 5 %, V_{SS} = 0V Cont'd

Number	5 MHz Limits		10 MHz Limits		16 MHz Limits		20 MHz Limits		25 MHz Limits		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
Auxiliary Port Key Entry											
t_{61}	80	–	40	–	30	–	20	–	15	–	ns
t_{62}	5	t_C-20	5	t_C-20	5	t_C-20	5	t_C-15	5	t_C-15	ns
t_{63}	30	–	20	–	15	–	10	–	10	–	ns
t_{64}	40	–	20	–	15	–	10	–	5	–	ns
t_{65}	20	–	20	–	15	–	15	–	5	–	ns
t_{66}	–	75	–	50	–	40	–	35	–	30	ns
t_{67}	–	75	–	50	–	40	–	35	–	30	ns

Notes:

1. All input transition times assumed <5ns, except clock which is <3ns (for 25 MHz timing).
2. The appropriate input flag ($\overline{MFLG}$, $\overline{SFLG}$, $\overline{AFLG}$) goes active LOW after 1 CLK ↓ +30ns from the writing of a "Load" or "Start" command.
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 ($\overline{MCS}$ must be LOW for one falling falling edge during a read/write cycle).
5. In Cipher Feedback, the Port Flag ($\overline{MFLG}$ or $\overline{SFLG}$) will go inactive following the leading edge of the first data strobe ($\overline{MRD}$, $\overline{MWR}$, $\overline{MDS}$, or $\overline{SDS}$), in all other modes and operations, the flags go inactive on the eighth data strobe.
6. Do not change K/$\overline{D}$ until $\overline{CP}$ is inactive (HIGH).
7. Do not change E/$\overline{D}$ until $\overline{MFLG}$ ($\overline{SFLG}$) is inactive (HIGH).
8. In Cipher Feedback, $\overline{BSY}$ must be inactive (HIGH) before S/$\overline{S}$ goes inactive (LOW).
9. $\overline{AFLG}$ must go active (LOW) before $\overline{ASTB}$ goes active (LOW).
10. t_{WL} is the clock width LOW (number t_2).
11. t_C is the clock cycle time (number t_3).
12. All output timing specifications reflect the following: High output >1.5V, Low output <1.5V.
13. All output timings assume C_{LOAD} = 50pF.
14. When operating in Direct Control Mode, you must ensure that the K/$\overline{D}$ input is valid one clock cycle before you begin to load the key, or perform any data operations with the device.

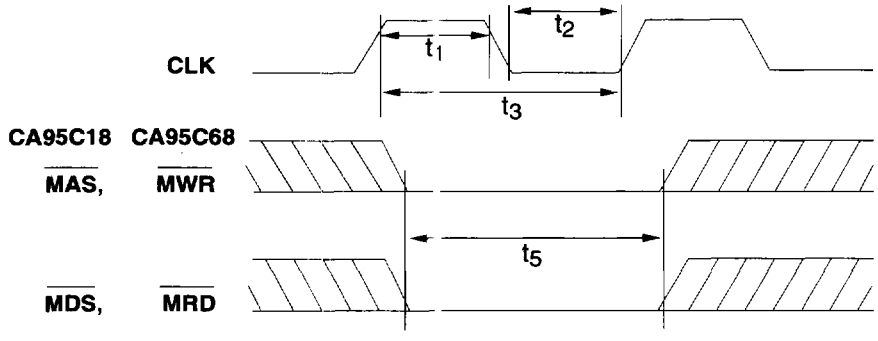


Figure 8 : CA95C68/18 Clock and Reset Timing

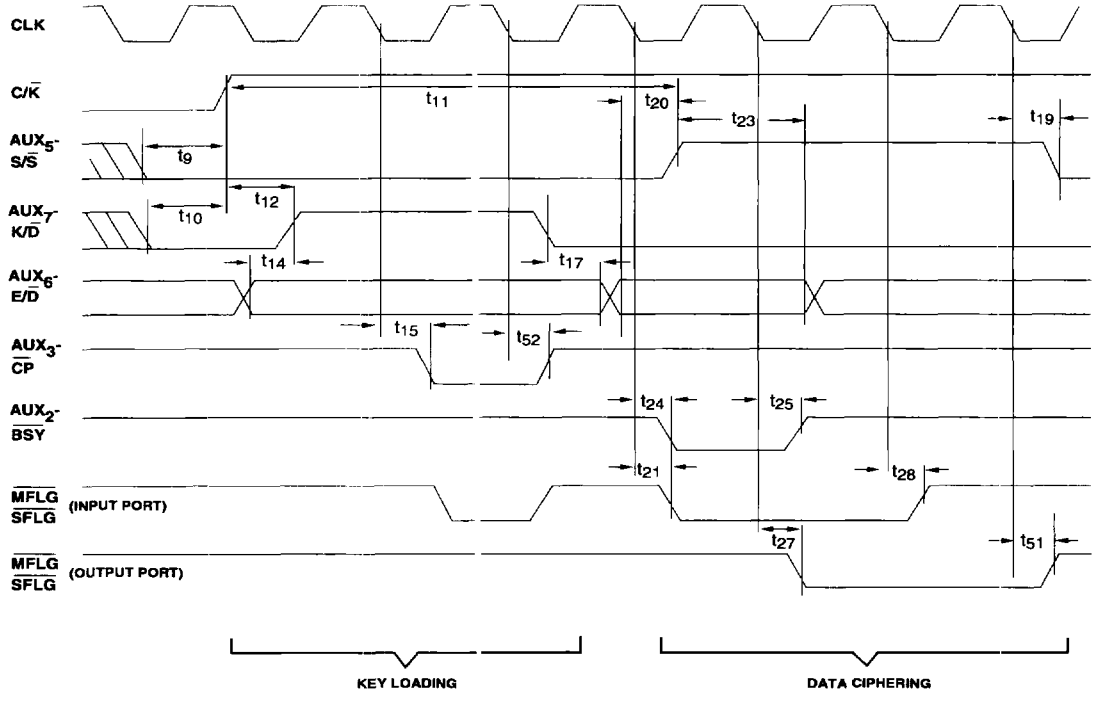


Figure 9 : CA95C68/18 Control and Status Signals Timing (Direct Control Mode)

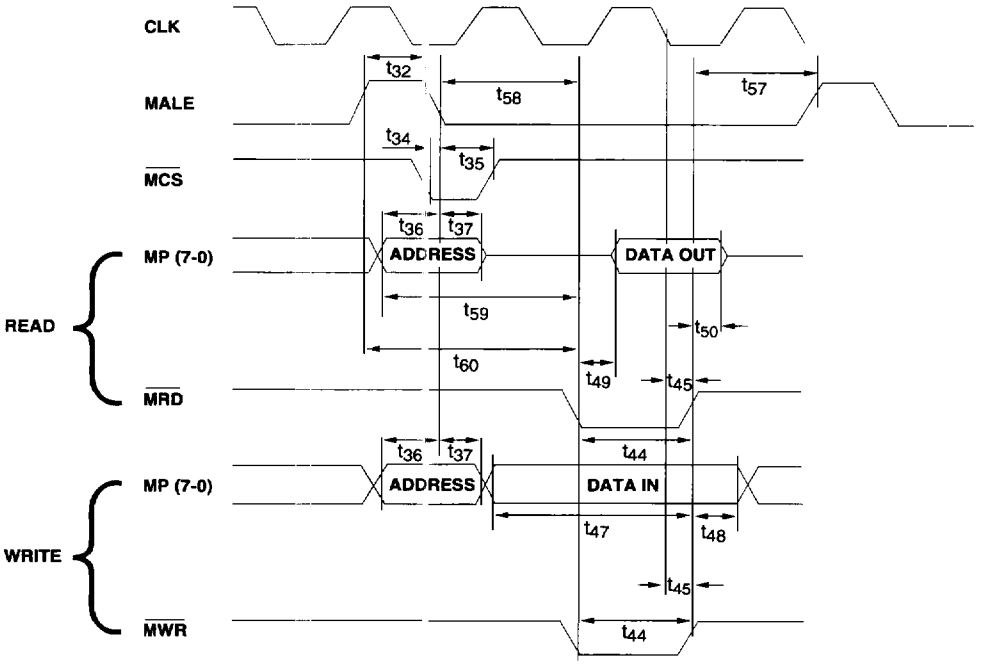
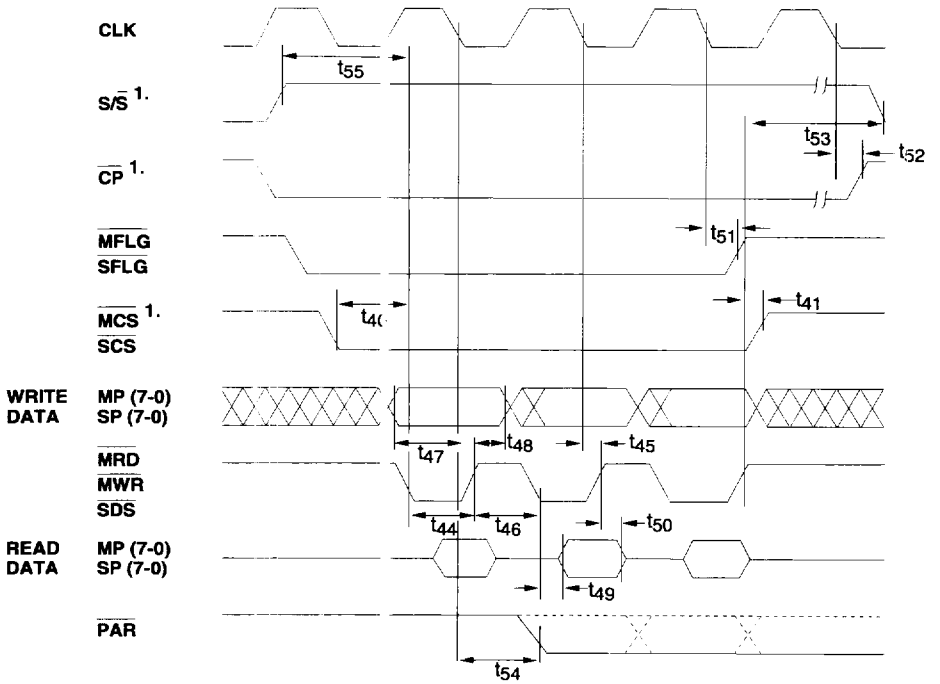


Figure 10 : CA95C68 Master Port, Multiplexed Control Mode Read/Write



1. These signals are only used for Read/Write Timing in Direct Control Mode of Operation.

Figure 11 : CA95C68 Master (Slave) Port Read/Write Timing

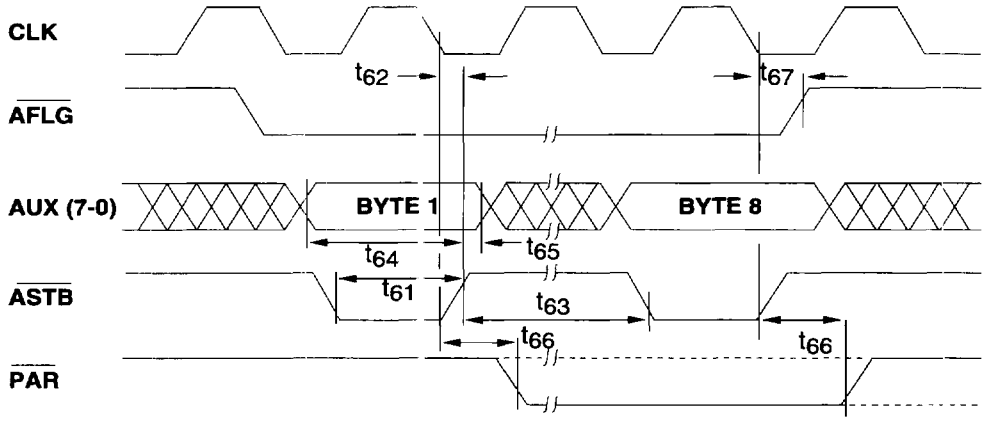


Figure 11 : CA95C68/18 Auxiliary - Port Key Entry Timing

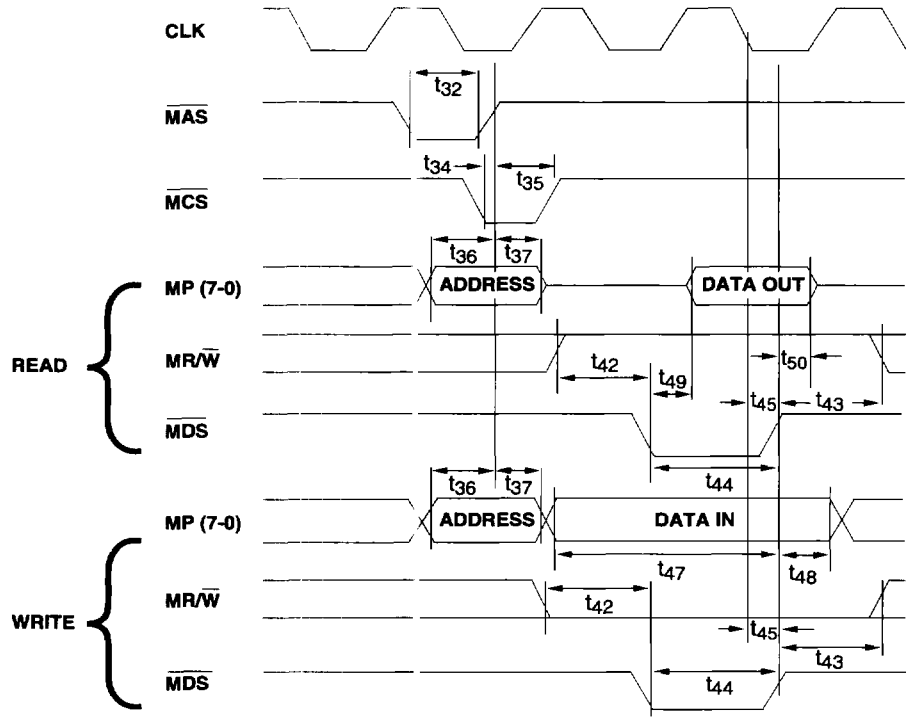
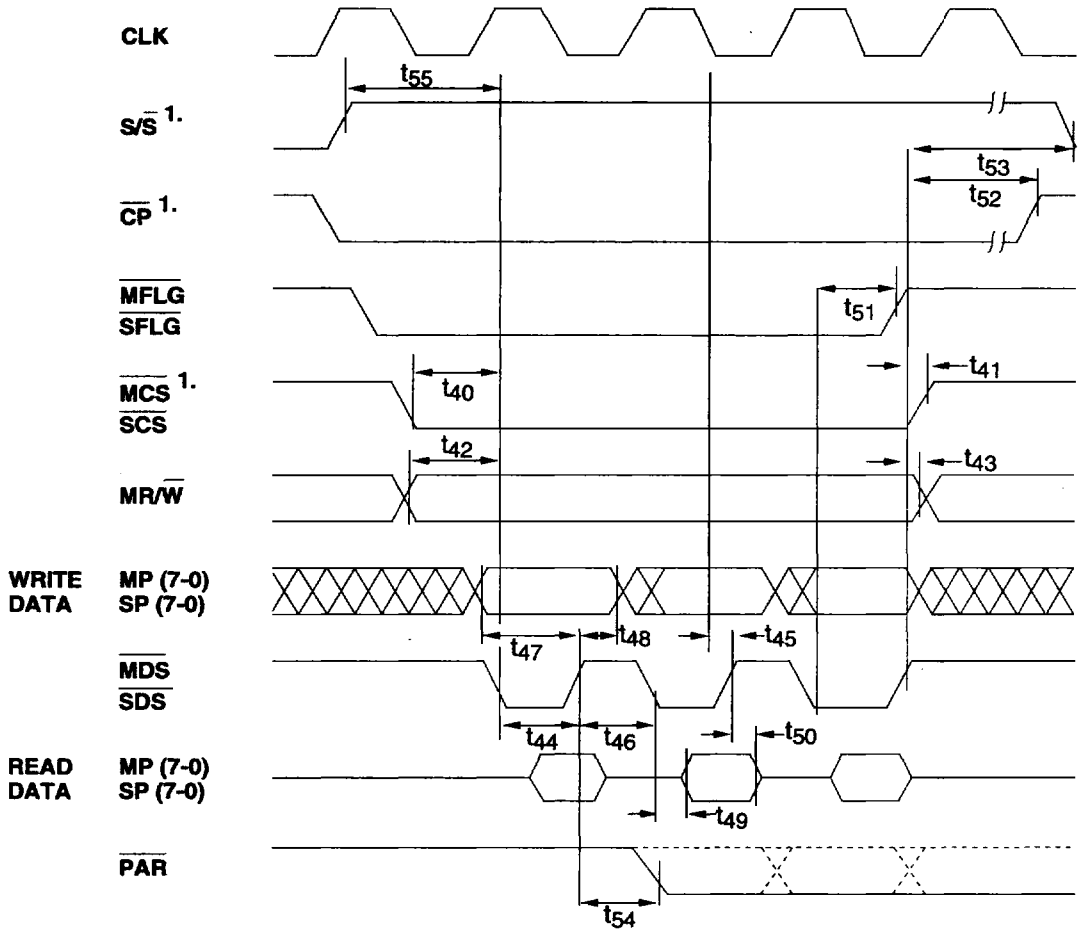


Figure 12 : CA95C18 Master Port, Multiplexed Control Mode, Read/Write Timing



1. These Signals are only used for Read/Write timing in Direct Control Mode of operation.

Figure 13 : CA95C18 Master (Slave) Port Read/Write Timing

Table 4 : DC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Test Conditions	Limits		Units
			Min	Max	
I_{IL}	Input leakage current	$0 V \le V_{IN} \le V_{DD}$	-1.0	+1.0	µA
I_{OZ}	Output leakage current	$0 V \le V_{IN} \le V_{DD}$	-10.0	+10.0	µA
I_{DDOP}	Operating supply current	–	–	3.0	mA/MHz
I_{DDSB}	Standby supply current	$V_{IN} = V_{DD}$ or V_{SS} V_{DD} = 5.50V, Outputs open	–	70.0	µA
V_{IL}	Input low voltage	Note 2	-0.5	0.8	V
V_{IH}	Input high voltage	Note 2	2.0	V_{DD}	V
V_{TL}	Schmitt trigger input low voltage	Note 1	-0.5	0.8	V
V_{TH}	Schmitt trigger input high voltage	Note 1	2.3	V_{DD}	V
V_{HY}	Schmitt trigger hysteresis	Note 1	0.4	–	V
V_{OL}	Output low voltage	I_{OL} = 4.0mA	–	0.4	V
V_{OH}	Output high voltage	I_{OH} = -4.0mA	2.4	–	V

Note:

1. Applies to the following inputs:
   For CA95C68: CLK, C/$\overline{K}$, $\overline{MCS}$, $\overline{MRD}$, $\overline{MWR}$, MALE, $\overline{SCS}$, $\overline{SDS}$, $\overline{ASTB}$.
   For CA95C18: CLK, C/$\overline{K}$, $\overline{MCS}$, $\overline{MAS}$, $\overline{MDS}$, MR/$\overline{W}$, $\overline{SCS}$, $\overline{SDS}$, $\overline{ASTB}$.
   For CA95C09: CLK, DCM, $\overline{MCS}$, $\overline{MRD}$ _ $\overline{MDS}$, MALE_$\overline{MAS}$, $\overline{MWR}$ _MR/$\overline{W}$, $\overline{SCS}$, $\overline{SDS}$, $\overline{ASTB}$, OPTION.
2. Applies to the following inputs: MP_{7-0}, SP_{7-0}, $AUX_{7\ 0}$.

Table 5 : Recommended Operating Conditions

DC Supply Voltage (V_{DD})	+4.5V to +5.5V
Power Dissipation (P_{DD}), (Note 1)	0.5 W
Ambient Operating Temperature (T_A Commercial)	0 to 70° C

Note:

1. The power dissipation figure is based on typical internal logic dissipation plus the worst case set of outputs simultaneously active with maximum rated loads.

Table 6 : Absolute Maximum Ratings

DC Supply Voltage (V_{DD})	-0.3 to +7.0V
Input Voltage (V_{IN})	-0.3 to +7.0V
DC Input Current (I_{IN})	-10 to +10 mA
Storage Temperature, plastic (T_{STG})	-65° to +150°C

Stresses beyond those listed above may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to maximum rating conditions for extended periods may affect device reliability.

FUNCTIONAL DESCRIPTION

The design of the DCP, as shown in Figure 1 is optimized for high data throughput. The cryptography key bytes can be written through both the Auxiliary and Master Ports. 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 each incoming key byte. Two 64-bit registers are provided for the initialization Vectors (IVE and IVD) required for chained (feedback) ciphering modes. Clear and cipher data bytes can be transferred through both the Master and Slave Ports to the Input Register; conversely, data can be transferred from the Output Register to either port. Four 8-bit registers (Mode, Command, Status and Mask) are accessible through the Master Port for interfacing to a host microprocessor.

Algorithm Processing

The DCP's Algorithm Processing Unit (see Figure 1) 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 FIPS PUB 46 (1-15-1977).

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 four ciphering methods: Electronic Code Book (ECB), Cipher Block Chaining (CBC), one (CFB-1) and eight bit Cipher Feedback (CFB-8). Electronic Code Block (ECB) is a straightforward implementation of the DES algorithm; 64 bits of clear data in, 64 bits of cipher text out, with no cryptographic dependence between blocks. Cipher Block Chaining (CBC) also operates on blocks of 64 bits, but includes a feedback step which chains consecutive blocks so that repetitive data in the plain text (such as ASCII blanks) does not yield identical cipher text. CBC also provides an error extension characteristic which protects against fraudulent data insertions and deletions. Cipher Feedback is an additive stream cipher method in which the DES generates a pseudo random binary stream which is then exclusive-OR'd with the clear text 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 both 1-bit and 8-bit cipher feedback which is useful for low speed bit and byte oriented serial communications.

Multiple Key Registers

The DCP provides the necessary registers to implement a multiple-key system. In such an arrangement, a single Master Key, stored in the DCP M Key Register, is used only to encrypt session keys for transmission to remote DES equipment, and to decrypt session keys received from such equipment. The M Key Register may only be loaded with plain text through the Auxiliary Port, using the Load Clear M Key command.

In addition to the Master 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 through the Master Port (Multiplexed Control Mode) into the Command Register, and then writing the eight bytes of key data to the port when the Command Pending bit = "1" in the Status Register (see Command Description Section).

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 internally connected to allow a host CPU to directly address six internal (Mode, Command, Status, Mask, Input, Output) registers and thereby control the device by writing and reading these registers. In Multiplexed Control Mode, the Auxiliary Port is also enabled for entering keys.

If the logic level of C/$\overline{K}$ is brought HIGH, the DCP enters Direct Control Mode, and the Auxiliary Port pins are converted into direct hardware control or status signals that are capable of instructing the DCP to perform a functionally complete subset of its cipher processing at very high throughputs. This operating mode is especially well suited for ciphering data for high-speed peripheral devices.

Initialization

The DCP can be reset in several ways:

1. By the "Software Reset" command,
2. By a hardware reset:

(**CA95C68**) Assertion of $\overline{MRD}$ and $\overline{MWR}$ LOW simultaneously for 1 clock cycle,

(**CA95C18**) Assertion of $\overline{MAS}$ and $\overline{MDS}$ LOW simultaneously for 1 clock cycle.

3. By writing to the Mode Register,
4. By aborting any command.

All these sequences are identical internally, except that loading the Mode Register doesn't subsequently reset the Mode Register. Once the reset process starts, the DCP is unable to respond to any further commands for approximately five clock cycles. If a power-up reset is used, the rising edge of the reset signal should not occur until approximately 1 ms after V_{DD} has reached the normal operating voltage. This delay time is required for internal nodes to stabilize.

Master Port Read/Write Timing

The DCP's Master Port is designed to operate with multiplexed address-data buses. The Master Port can be optimized to interface with either a Latched Address Enable (CA95C68) or a Strobed (CA95C18) microprocessor.

Several features of the CA95C68 interface should be stressed.

- The level on Master Port Chip Select ($\overline{MCS}$) is latched internally on the falling edge of Master Port Address Latch Enable (MALE) in Multiplexed Control Mode only. This relieves external address decode circuitry of the responsibility for latching chip select at address time.
- The levels on MP1, MP2 are also latched internally on the falling edge of MALE and are subsequently decoded to enable reading and writing of the DCP's internal registers (Mode, Command, Status, Mask, Input and Output). Again, this eliminates the need for external address latching and decoding. The Mask Register is only accessible when the DCP is programmed for one-bit CFB mode via the Mode Register's Cipher Type bits.
- Data transfers through the Master Port are controlled by the levels and transitions on the Master Port Read ($\overline{MRD}$) and Master Port Write ($\overline{MWR}$) pins. Master Port data transfers do not disturb either the chip-select or address latches, so that once the DCP and a particular register have been selected, unlimited writing and reading of that register can be done without intervening address cycles. Given the required transfer control external to the DCP, this feature could greatly speed up loading keys and data.

The CA95C18 interface is similar with the following exceptions:

- The level on $\overline{MCS}$ is latched internally on the rising edge of $\overline{MAS}$ in Multiplexed Control Mode only.
- The levels on MP1, MP2 are also latched internally on the rising edge of $\overline{MAS}$ and are then decoded to enable reading and writing of internal registers.
- Data transfers through the Master Port are controlled by Master Port Data Strobe ($\overline{MDS}$) and Master Port Read/Write (MR/$\overline{W}$). The chip-select and address latches aren't affected by data transfers. Any number of reads or writes to this selected register can be accomplished without intervening address cycles.

Loading Key and Initialization Vector (IV) Registers

The Key and Initialization Vector Registers are not directly addressable through any of the DCP's ports, therefore keys and vector data must be loaded through "command data sequences" (see Command Description Section). 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 bit in the Status Register; the user then either writes eight bytes of key or initial vector data through the Master or Auxiliary Port, as selected by the specific command, or reads eight bytes of initial 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 asserting the proper state on the AUX_6-E/$\overline{D}$ input (HIGH for E Key, LOW for D Key) and subsequently raising the AUX_7-K/$\overline{D}$ input, indicating that key loading is required. The command processor will assert the AUX_3-$\overline{CP}$ (Command Pending) signal, then the eight key bytes may be written through the Master Port to the appropriate register. In Multiplexed Control Mode, all Key and Initial Vector Registers, except the Master (M) Key, may be loaded with encrypted, as well as clear, data. Before loading an encrypted key or initial vector, the clear Master Key must first be loaded through the Auxiliary Port. If the operation is a Load Encrypted command, the subsequent data is written to either the Master or Auxiliary Port and is routed first to the Input Register and decrypted before being stored in the specified Key or Initial Vector Register. After loading the last byte of an encrypted key or initial vector, no reading or writing of internal registers is allowed for the subsequent 70 clock cycles.

Parity Checking of Keys

Key bytes are considered to contain seven bits of key information and one Parity bit. By DES designation, the low-order bit is the Parity bit. The parity checking circuit is enabled whenever a byte is written to one of the three key registers. The output of the parity detection circuit is connected to the $\overline{PAR}$ pin, as well as the state of this pin being reflected by the Status Register PAR (S3) bit. Status Register bit PAR goes to "1" whenever a byte with even parity (an even number of "1"s) is detected. The Status Register also has a Latched Parity bit (LPAR, S4) which is set to "1" whenever the Status Register PAR bit goes to "1". Once it is set to "1", the LPAR bit is not cleared until a reset occurs or a new Load Key command is issued.

When an encrypted key has been loaded, the parity detect logic operates only after the decrypted key is available. The encrypted data is not checked for parity. The $\overline{PAR}$ signal will

reflect 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 appropriate key register. Therefore, the time $\overline{PAR}$ 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 will indicate if any byte contained errors.

Data Flow

The Mode Register contains two bits, M2 and M3, which control the flow of data into and out of the DCP through the Master and Slave Ports. Three basic configurations are provided: single port, and two dual port configurations.

Single Port Configuration

The simplest configuration occurs when the Mode Register Data Flow Control bits are set to Master Port only. Data to be encrypted/decrypted (depending on the value loaded into the Encrypt/Decrypt bit (M4) of the Mode Register) is written to the Input Register through the Master Port. To facilitate monitoring of the Input Register status, the $\overline{MFLG}$ signal goes LOW when the Input Register is not full. Clear or cipher data is ready to be read by the host CPU through the Master Port Output Register address when $\overline{SFLG}$ goes LOW. Therefore, $\overline{MFLG}$ is redefined as Master Input Flag and $\overline{SFLG}$ is redefined as Master Output Flag.

Dual Port, Master Port Clear Configuration

In the dual port configurations, entering and removing data is accomplished with both the Master and Slave Ports. In the Master Port Clear configuration, clear text for encryption or clear text resulting from decryption can pass only through the Master Port. Cipher text can be handled only through the Slave Port. The direction of data flow is controlled either by the Encrypt/Decrypt bit (M4) in the Mode Register, or by the Start Encryption or Start Decryption commands. For encryption, clear data is written through the Master Port to the Input Register, and cipher data can be read from the Output Register through the Slave Port at the appropriate time. If decryption is selected, the process is reversed, cipher data being written to the Input Register through the Slave Port, and the clear data being read from the Output Register through the Master Port.

Dual Port, Slave Port Clear Configuration

This configuration is identical to the Dual Port, Master Port Clear configuration described above, except that the direction of ciphering is reversed. That is, all data written, or read at the Master Port is cipher text, and all data at the Slave Port is clear text

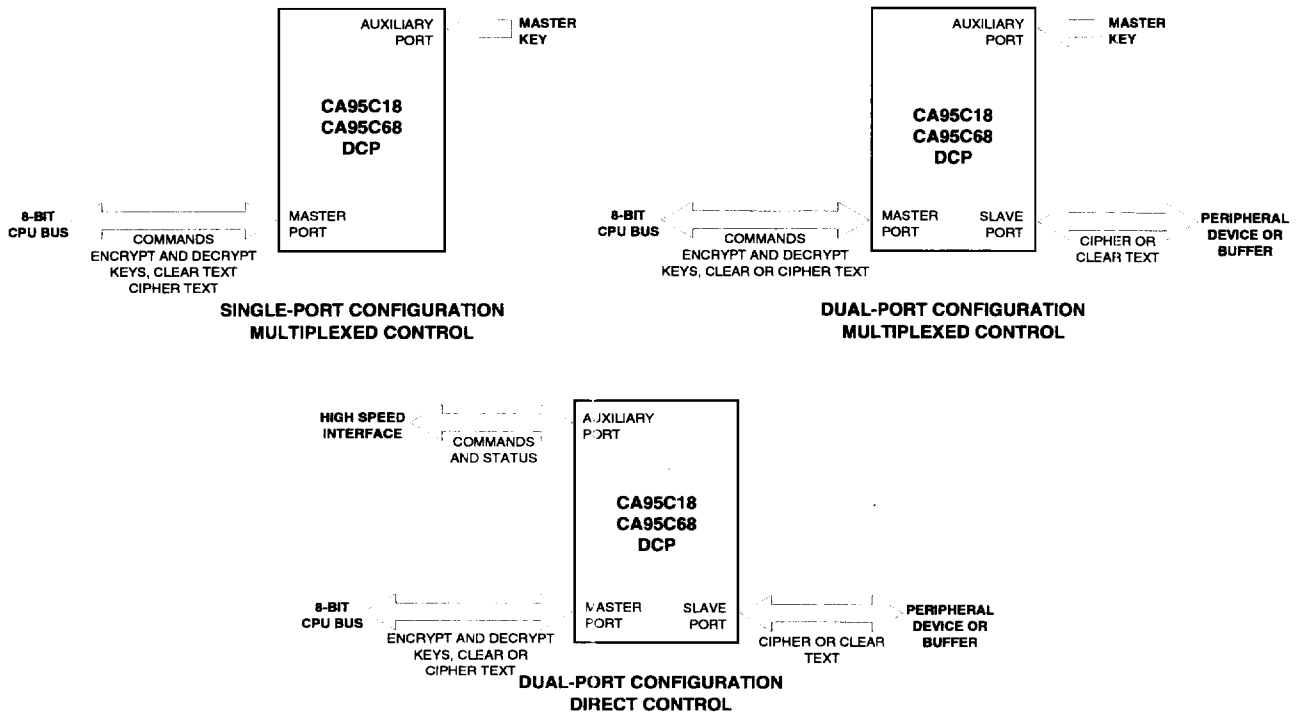


Figure 14 : CA95C68 and CA95C18 Data Flow Options

REGISTER DESCRIPTION

The registers in the DCP which can be directly addressed through the Master Port are shown with their addresses in Table 7. A brief description of these registers and others not directly accessible is given below.

Table 7 : Master Port Register Address

C/$\overline{K}$	Cipher Type	MP2	MP1	$\overline{MRD}$ 9568	$\overline{MWR}$ 9568	MR/$\overline{W}$ 9518	$\overline{MCS}$	Register Addressed
0	all	0	0	1	0	0	0	Input Register
0	all	0	0	0	1	1	0	Output Register
0	all	0	1	1	0	0	0	Command Register
0	all	0	1	0	1	1	0	Status Register
0	ECB/ CBC/ CFB-8	1	0	1	0	0	0	Input Register
0	ECB/ CBC/ CFB-8	1	0	0	1	1	0	Output Register
0	CFB-1	1	0	X	X	X	0	Mask Register
0	all	1	1	X	X	X	0	Mode Register
X	all	X	X	X	X	X	1	No Register Accessed
1	all	X	X	1	0	0	0	Input Register
1	all	X	X	0	1	1	0	Output Register

Mode Register

Figure 15 shows the bit assignments in this 7-bit read/write register. The Cipher Type bits (M1, M0) indicate to the DCP which ciphering algorithm is to be used. After a reset, the Cipher Type defaults to the Electronic Code Book.

Configuration bits (M3, M2) 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 (M3, M2=10), the Slave Port is disabled and no manipulation of Slave Port Chip Select ($\overline{SCS}$) or Slave Port Data Strobe ($\overline{SDS}$) can cause data movement through the Slave Port. All data transfers are accomplished through the Master Port, as described more fully in the Functional Description section. In this configuration, $\overline{MFLG}$ gives the status of the Input Register and $\overline{SFLG}$ the Output Register.

Both the Master and Slave Ports are available for input and output operations when the Configuration bits are set to one of the dual port configurations (M3,M2 = 00 or 01). When M3,M2 = 01 (the default configuration), the Master Port handles clear data while the Slave Port handles ciphered data. Configuration M3,M2 = 00 reverses this assignment. The data direction at any particular moment is controlled by the Encrypt/Decrypt bit (M4).

The Encrypt/Decrypt bit 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 the data flow direction within the DCP. For example, when the Encrypt/Decrypt bit is "1" (encrypt) and the Configuration bits are "01" (Dual Port, Master Clear, Slave Encrypted), clear data will enter the DCP through the Master Port and encrypted data will be removed from the Slave Port. When the Encrypt/Decrypt bit is set to "0" (decrypt), the direction of data flow reverses.

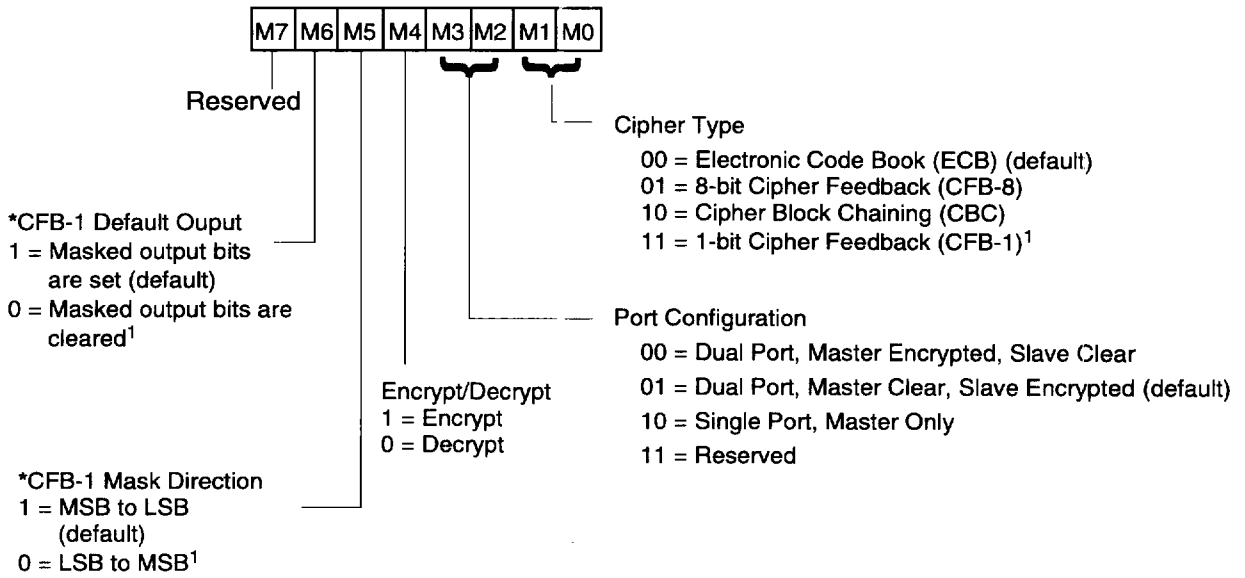
The CFB-1 Mask Direction bit (M5) determines the direction in which the Mask Register's bits and the input data are interpreted. When the CFB-1 Mask Direction bit is set to "1" the DCP will read the Mask Direction and data to be ciphered from most significant bit (MSB) to least significant bit (LSB). When the CFB-1 Mask Direction bit is set to "0" the DCP will read the Mask Register and data from LSB to MSB. The CFB-1 Mask Direction bit is only accessible when the DCP is set to 1-bit Cipher Feedback mode via the Mode Register.

The CFB-1 Default Output bit (M6) defines the sense of output bits which are masked off in the Mask Register. If the Default Output bit is set to "1" then output bits, which are masked (not used), will be set to "1". If the Default Output bit is cleared to "0" then output bits, which are masked (not used), will be cleared to "0".

Mask Register

The 8-bit read/write Mask Register determines which Input and Output Register bits are significant during One-bit Cipher Feedback mode (CFB-1). If any Mask Register bit is set to "1" then the corresponding bit of the Input Register will be used as an input to the one-bit cipher feedback encryption/decryption process and its one bit result will likewise be placed in the corresponding bit of the Output Register. If any Mask Register bit is cleared to "0" then the corresponding bit of the Input Register will be ignored.

In one-bit cipher feedback mode, if a single byte is written to the Input Register (when requested by the DCP via the Input Flag) then the ciphering algorithm unit will remain busy until all bits in the Input Register, corresponding to set bits in the Mask Register, are processed. For example, if the Mask Register is set to "01101001" and the Mode Register's CFB-1 Mask Direction bit is set for MSB to LSB Mask interpretation, then the DCP will perform Encryption/Decryption on bit 6 of the Input Register, followed by bits 5, 3, and 1. The corresponding results will be placed in bits 6, 5, 3 and 1 of the Output Register. All other bits in the Input Register will be ignored and all other bits in the Output Register will be set to the state indicated by the Default Output bit (M6) of the Mode Register. The ciphering algorithm unit will remain busy until all four bits are ciphered. Zero to eight bits of the Mask Register may be set to "1". If zero bits are set to "1" then any subsequent writes to the Input Register will be ignored.



* The CFB-1 Mask Direction and Default Output bits are only accessible when the DCP is in CFB-1 mode, otherwise these bits are high.

1.) This mode is Newbridge Microsystems specific.

Figure 15 : Mode Register Bit Assignments

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 Command Description section, and the commands and their binary representations are summarized in Tables 8 and 9.

Table 8 : Command Codes in Multiplexed Control Mode

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 9 : Implicit Command Sequences in Direct Control Mode

$C/\overline{K}$	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 Clear D Key through Master Port
H	↑	H	L	Load Clear E Key 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

Status Register

The bit assignments for the read-only Status Register are shown in Figure 16. The PAR, AFLG, SFLG and MFLG bits indicate the status of the similarly named output pins, as do the Busy and Command Pending bits when the DCP is the 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, on the other hand, indicates whether any key byte with even parity has been encountered since the last Reset or Load Key command.

The Busy bit will be a "1" whenever the ciphering algorithm unit is actively encrypting or decrypting data. For example, the Busy bit is set in response to a Load Encrypted Key command (the Command Pending bit will go HIGH as well) or in the ciphering of regular text (indicated by the Start/Stop bit being a "1"). If the ciphered data cannot be transferred to the Output Register (due to the presence of data from a previous ciphering cycle), then the Busy bit will remain a "1". The Busy bit will be "0" at all other times, including if no ciphering is possible because no data has been loaded into the Input Register.

The Command Pending bit is set to "1" by any instruction which requires the transfer of data to or from a non-addressable internal register, such as when writing key bytes to the E Key Register or reading bytes from the IVE Register. Therefore, the Command Pending bit will be set following all commands except the three Start Commands, the Stop command and the software Reset command. The Command Pending bit will return to an inactive state ("0") after all eight bytes have been transferred following Load Clear, Read Clear or Read Encrypted commands. In addition the inactive state ("0") only returns after data has been entered, decrypted and placed into the desired register following Load Encrypted commands.

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

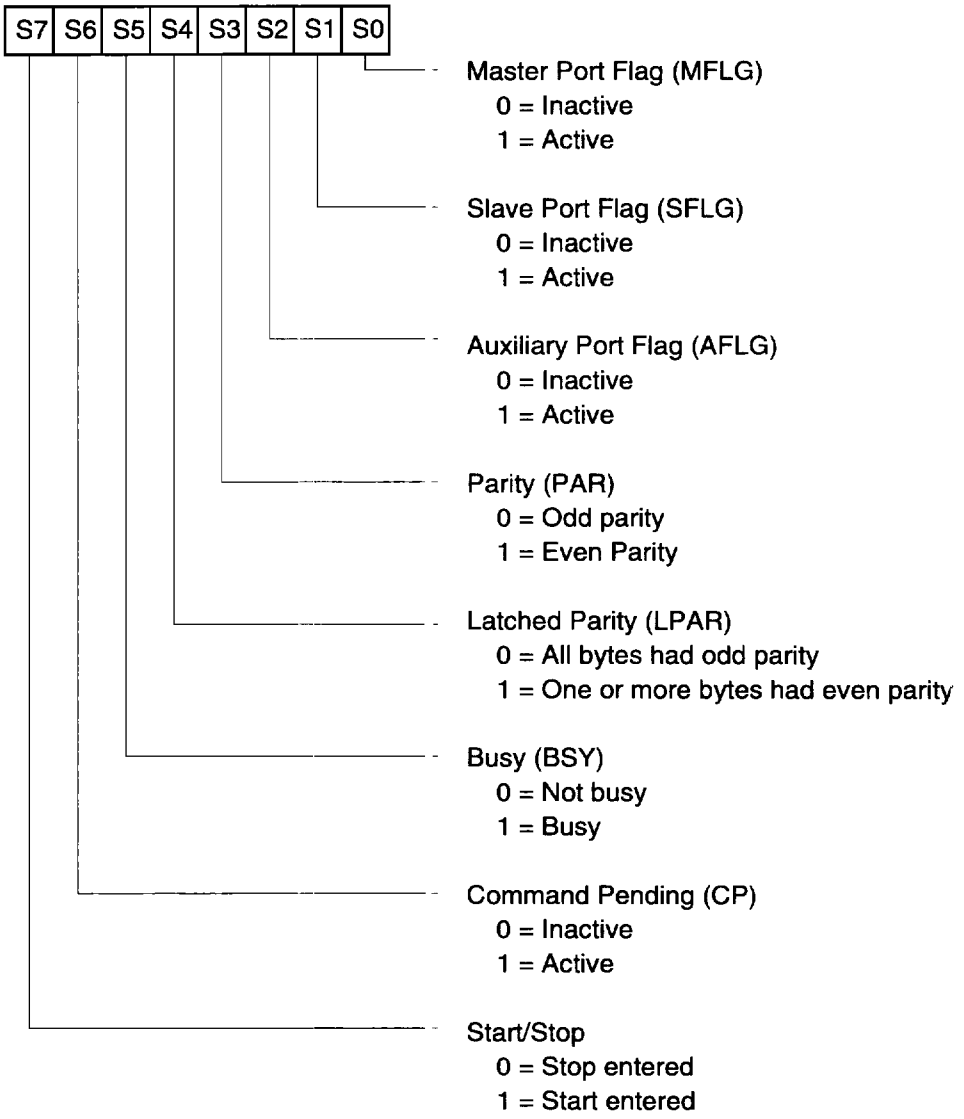


Figure 16 : Status Register Bit Assignments

Input Register

The 64-bit, write-only Input Register is organized to appear to the user as eight bytes of push-down storage. The number of bytes stored in the register is monitored by a status circuit. The register is considered full when eight bytes of data have been loaded with the ECB or CBC ciphering algorithm in use, or when one byte of data has been entered in either CFB mode. It is considered empty when the data stored in it has been or is being processed. The data in the register won't be destroyed if the user attempts to write data into the Input Register when it is full. Table 10 gives a summary of the port flag associated with this register depending on the mode of operation.

Output Register

The 64-bit, read-only Output Register is setup 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 out by the host CPU, and is considered full if it still contains one or more bytes of output data. If an attempt is made to read data from the Output Register when it is empty, the output buffers will remain in a tri-state condition.

Table 10 : Association of Master Port Flag ($\overline{\text{MFLG}}$) and Slave Port Flag ($\overline{\text{SFLG}}$) with Input and Output Registers

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

M,E,D Key Registers

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. These registers are not directly addressable, but can be loaded or read in response to a command (See Command Descriptions). The Master key can be loaded only with clear data through the Auxiliary Port. The Encrypt and Decrypt Keys can be loaded as either clear or cipher text through the Master or Auxiliary Port. If the key data is encrypted, it is first routed to the Input Register where it is decrypted using the M Key, and then written to the target key register from the Output Register.

Initialization Vector Registers

Two 64-bit registers are provided to store feedback from Cipher Feedback and Cipher Block Chaining modes of operation. One Initialization Vector (IVE) Register is used during encryption, the other (IVD) during decryption. Both registers can be loaded with either clear or encrypted data through the Master Port. If encrypted data is loaded, it is first decrypted before being written into the corresponding IV Register. Both registers may be read out through the Master Port as either clear or encrypted text (see Command Description Section).

PROGRAMMING INSTRUCTIONS FOR MULTIPLEXED CONTROL MODE

This section describes the registers that need programming prior to using the DCP in ECB, CBC, or CFB ciphering modes in Multiplexed Control Mode (MCM) of operation. The programming flow charts for each mode are implemented for a single 8 bit port interface (see the pipelining section for the dual port programming flow chart).

ECB Operation

Figure 17 illustrates the programming sequence for ECB.

1. A hardware or software reset must be implemented to bring the device to a known state. A reset clears all bits in the Status Register and programs the Mode Register to it's default setting.
2. Program the Mode Register (see Figure 15) with the cipher type and the port configuration. For further explanation see the Mode Register description.
3. The clear Encryption or Decryption Keys can be loaded through either the Master or Auxiliary Ports. The Command Pending bit in the Status Register will go active once a command has been entered in the Command Register. This bit will be active until all eight bytes of the key have been loaded into the Input Register of the DCP.

3A. An alternative method to Step 3 is to load a Master Key into the DCP through the Auxiliary Port. When this command is entered the AFLG bit in the Status Register will go active ($\overline{AFLG}$ output pin will be active low) until all 8 bytes have been entered. One key byte is loaded on each rising edge of the Auxiliary Strobe ($\overline{ASTB}$).

3B. A Load Encrypted Session Key command is then entered into the DCP. The Session Key is then decrypted by the Master Key before being stored in the corresponding register. This use of the Master Key allows you to enhance security by frequently changing the session keys over a communication link.

4. One of the three Start commands is then written to the Command Register to begin the ciphering session.
5. Once a Start command is entered, the DCP will indicate that it is ready for data input by activating the corresponding flag bit in the Status Register, as well as the associated input flag pin. Data can now be input through the assigned Input Port. The two flags, $\overline{MFLG}$ and $\overline{SFLG}$, which are associated with the Data Registers can be sensed by hardware or software to know when data is to be entered or removed from the DCP.
6. As soon as the Input flag is active, the DCP is ready to accept data (MSB first). This bit is deactivated once eight bytes of data have been entered.
7. The Output flag goes active whenever the DES algorithm is completed and data is ready to be removed from the Output Register.
8. Data is removed from the Output Port one byte at a time with the most significant byte first. The Output flag becomes inactive upon the removal of the eighth byte.
9. Loop through steps 5 through 9 until the ciphering session should be terminated.
10. The session can now be terminated by issuing the Stop command to the Command Register.

Upon termination, all remaining processed data is available in the Output Register until the DCP is reset. This allows you to enter the Stop command immediately upon entering the last input block. When all the data has been removed from the Output Register, all the flags will be inactive. If the DCP is restarted, any data that was not read out from the previous ciphering session will be lost.

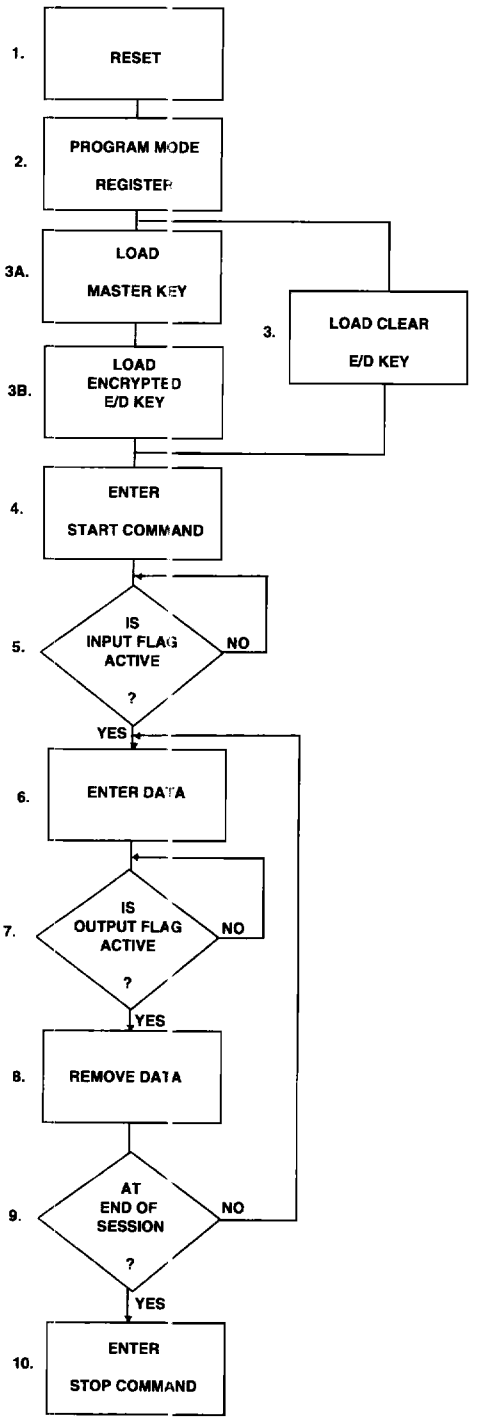


Figure 17 : Multiplexed Control Mode ECB Programming Flow Chart

CBC Operation

Figure 18 illustrates the DCP programming sequence for implementing the CBC method of ciphering. The programming sequence is identical to the ECB programming sequence except for an extra step included between steps 3 and 4. The Initialization Vectors (IVs) must be loaded before beginning to cipher data. These IVs can be loaded in either clear (step 3.1) or ciphered form (steps 3.1.A and 3.1.B).

3.1 Load in eight bytes (MSB first) of the Initialization Vector through the Master Port.

3.1.A(B) If the Initialization Vector is entered in encrypted form, it is decrypted using the Decrypt Session Key in ECB mode before being stored in the appropriate register. Load the D Key (if not already done) prior to executing an encrypted IV command. The eight IV bytes are then loaded into the Input Register and decrypted. The bits (Cipher Type and Encrypt/Decrypt bit) in the Mode Register are not affected by the decrypting of the IVs.

CFB Operation

The flow chart for the instruction sequence in CFB mode is very similar to CBC mode. The DCP can be programmed to execute in either 1-bit or 8-bit CFB mode. The Input and Output Registers hold between one and 8 bits depending on the cipher type and the setting of bits in the Mask Register. In both modes, the IV is first ciphered by the algorithm unit and the result is then XORed with the input byte or bit (see explanation of Mask Register for CFB-1 mode). The XOR result is then loaded into the Output Register to be read out by the CPU. This result is also shifted into the current IV Register to be used in the next cipher session. When operating in CFB mode, the Output Register must first be emptied before issuing a Stop command to the DCP. If you must stop in the middle of inputting a block of data while using ECB or CBC ciphering in Multiplexed Control Mode, follow this instruction sequence to avoid erroneous data:

1. Issue a Stop command.
2. Read all available data from the Output Register.
3. Reload the Mode Register.
4. Issue a Start command.
5. Wait for the input flag to go active and resume data input.

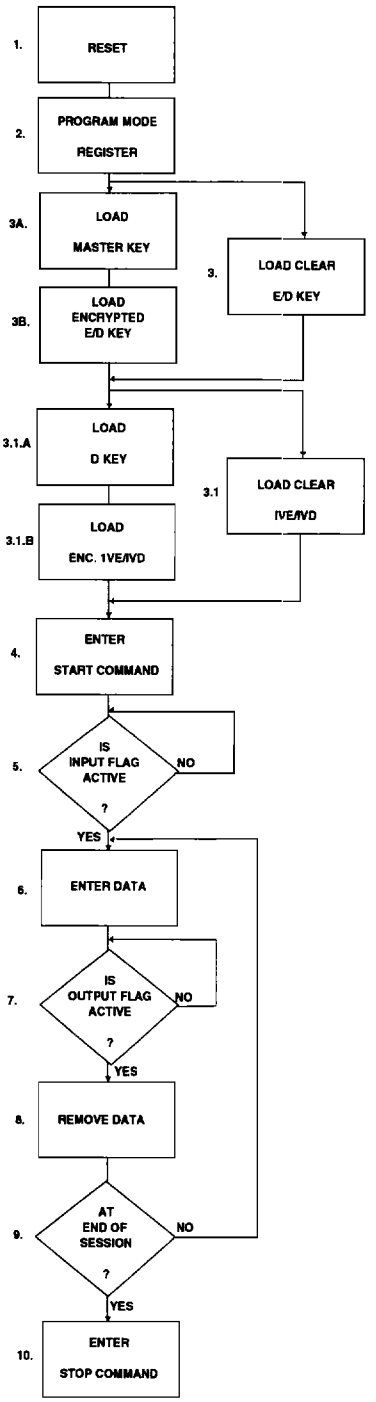


Figure 18 : Multiplexed Control Mode CBC Programming Flow Chart

PROGRAMMING INSTRUCTIONS FOR DIRECT CONTROL MODE

This section describes how the DCP functions in Direct Control Mode (DCM), (C/$\overline{K}$ pin is high). Only a subset of the commands that are available in Multiplexed Control Mode can be executed by controlling and monitoring the status of the Auxiliary Port pins. While in DCM, you are unable to access the Mode or Mask Register. The state of the E/$\overline{D}$ and K/$\overline{D}$ pins should be held constant throughout the entire key or data loading process. The state of the S/$\overline{S}$ pin must also be held constant during the entire data ciphering process.

ECB Operation

A flow chart of ECB operation in Direct Control Mode is illustrated in Figure 19. A detailed explanation of each step is described below:

In most DCM applications it is desirable to switch back and forth between MCM and DCM; therefore, C/$\overline{K}$ must be programmable. Before using the device, either a hardware or software reset should be performed to set the device to it's default state. If the default mode of operation and the Direct Control Mode instruction set is sufficient for your requirements, then C/$\overline{K}$ may be permanently tied high. If your application does not work in the default mode of operation, the Mode Register must be programmed while in Multiplexed Control Mode (which requires C/$\overline{K}$ to be low).

1. While in Multiplexed Control Mode, any key load commands can be executed before switching back to Direct Control Mode (DCM). Alternatively, the session keys may be loaded while in DCM. When operating in DCM, the DCP does not automatically latch the Input/Output Register's address. Before beginning to load any data into the Input Register, you must latch this address using the address latch enable strobe. Driving the K/$\overline{D}$ pin of the Auxiliary Port high sets up the DCP for key entry (the S/$\overline{S}$ pin must stay low for the entire key loading process). The level of the E/$\overline{D}$ pin determines whether the Encryption or Decryption Session Key will be loaded. As soon as the $\overline{CP}$ output pin goes low you may begin to strobe in the eight key bytes using the Master Port Write Strobe ($\overline{MCS}$ must be held low throughout the entire byte loading process).
2. Once the key loading process is complete, you may now enter a Start command by driving the S/$\overline{S}$ line high. The level on the E/$\overline{D}$ pin at this time will determine whether the data is encrypted or decrypted. The levels on the K/$\overline{D}$ and S/$\overline{S}$) pins must be low throughout the data ciphering process. The DCP responds to this command by lowering the Input Port flag (see Table 10).
3. Whenever the Input flag is active, data can be entered through the Master or the Slave Port, depending on the selected mode of operation. To achieve the highest throughput, the DCP must be configured to work in the pipeline mode of operation. When the DCP has processed the data, the Output flag will become active and the data may be removed from the Output Port.
4. Once all the data has been ciphered, the DCP should be returned to the inactive state by driving the S/$\overline{S}$ pin low.

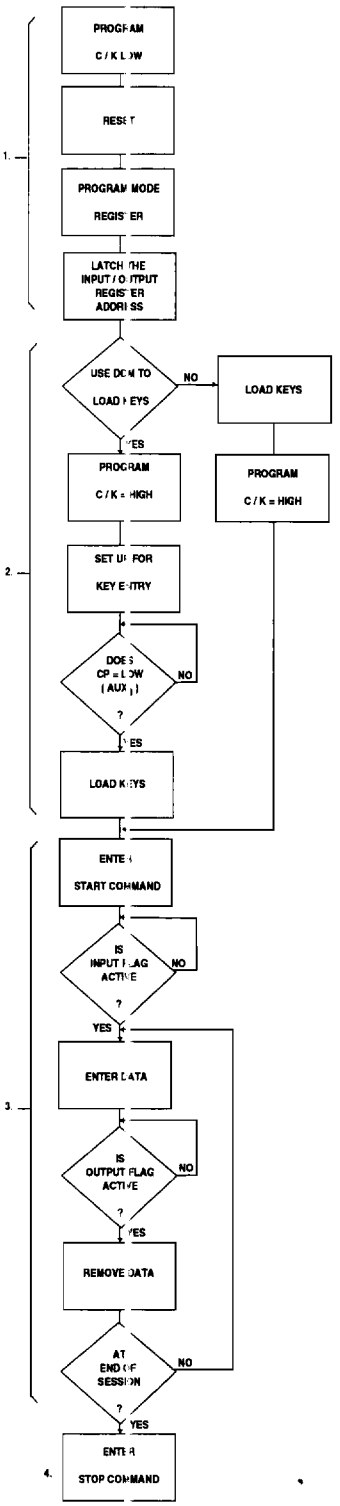


Figure 19 : Direct Control Mode ECB Programming Flow Chart

CBC and CFB Operation

The instruction sequence to perform CBC or CFB operation in Direct Control Mode (DCM) is similar to ECB mode of operation. When operating in these modes, the C/$\overline{K}$ pin must be programmable because the IV needed for CBC and CFB can only be loaded while in Multiplexed Control Mode. If you are using CFB-1 ciphering, the Mask Register must also be loaded before entering DCM. When operating in this mode you must ensure that a Stop command is not issued while the Command Pending or Busy pins are active or when there is data still remaining in the Output Register. (see Figure 20 for a programming flow chart).

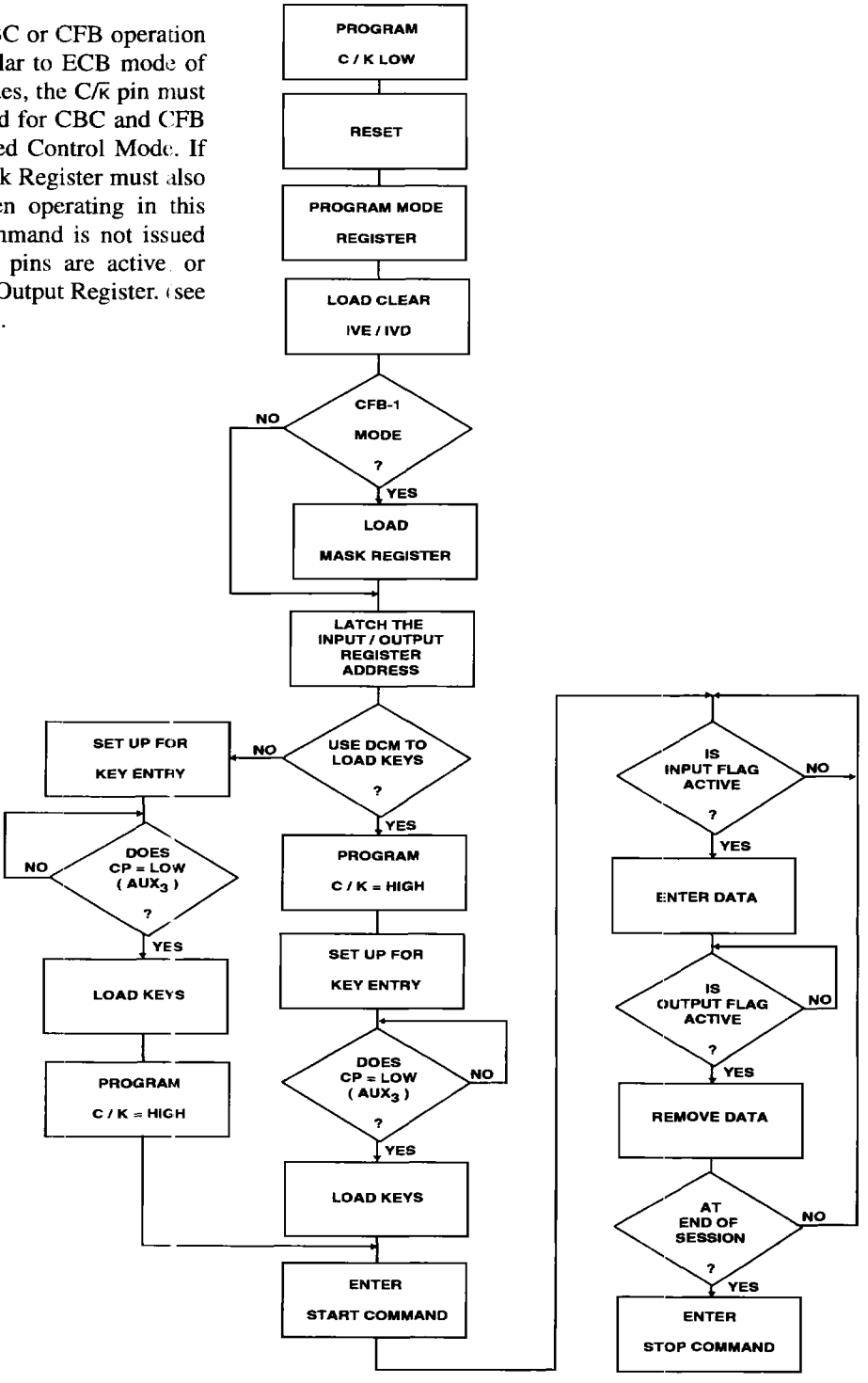
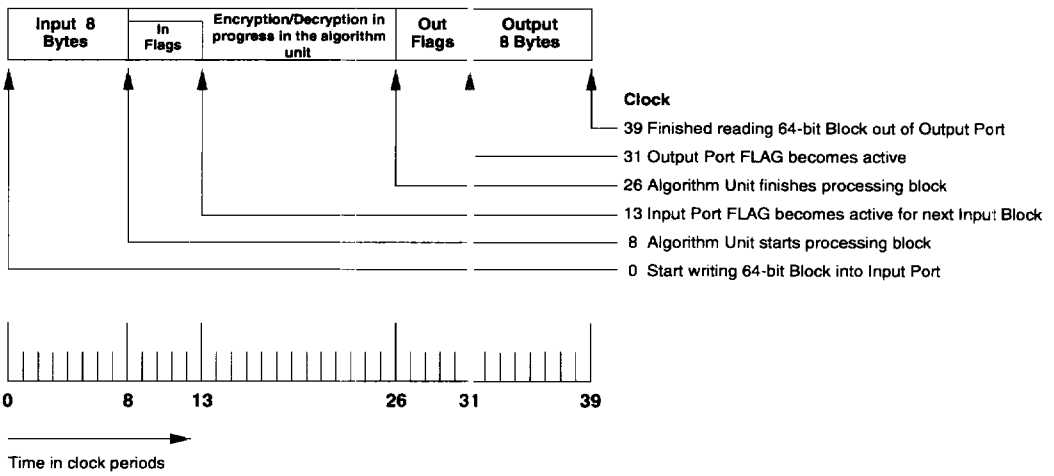


Figure 20 : Direct Control Mode CBC/CFB Programming Flow Chart

Maximum Throughput

The pipelined architecture of the DES DCPs allows simultaneous input, ciphering, and output operations. Maximum throughput is obtained when the device is configured for one of the dual port configurations. Figure 21 shows the timing for ciphering one block of 64 bits in either ECB or CBC modes of encryption. The inputting of the 64 bits of data takes 8 clock cycles to complete with one data strobe being issued per clock cycle. This data must then be transferred from the Input Register to the algorithm processing unit and the flags updated, which requires 5 additional clock cycles. The algorithm unit begins ciphering concurrently with the transfer and once the flags have been updated another 64 bit block may be entered. The ciphering of the first block is completed after 18 clock cycles have elapsed from the last byte having been written to the Input Register. Another 5 clock cycles are required to transfer the ciphered data to the Output Register and update flags. Transferring of data from the algorithm processing unit to the Output Register can be performed concurrently with loading new data into the DES algorithm unit. Removing the data from the Output Register involves 8 clock cycles with one data strobe per clock cycle. The whole procedure of ciphering one block takes 39 cycles but because the different operations can be overlapped, the DCP can process one block every 18 clock cycles once fully loaded.



Note: CA95C68 minimum clock period = 40 nanoseconds

Figure 21 : Detailed Timing of One Block

Pipelining

Once the device has been initialized for dual port configuration, two data blocks are loaded into the device to fill the Output Register and the DES algorithm processing unit. Now blocks of data can be strobed in and out concurrently. When the ciphering session is completed the DCP must be emptied by reading out the last two bytes.

Figure 22 illustrates a programming flow chart for programming the DCP for pipelined mode of operation.

Figure 23 shows the minimum timing configuration for maximum throughput for this device. The total time to transfer "n" blocks is (n+1)x18+3 clock cycles. The DCP can also be operated in pipelined mode when configured for signal port operation. Once initialized, one block of data is loaded into the device. Then, in a loop, one block of data is strobed in and one block is read out. The first block of data loaded before entering the loop is ciphered while the input of the second block is occurring.

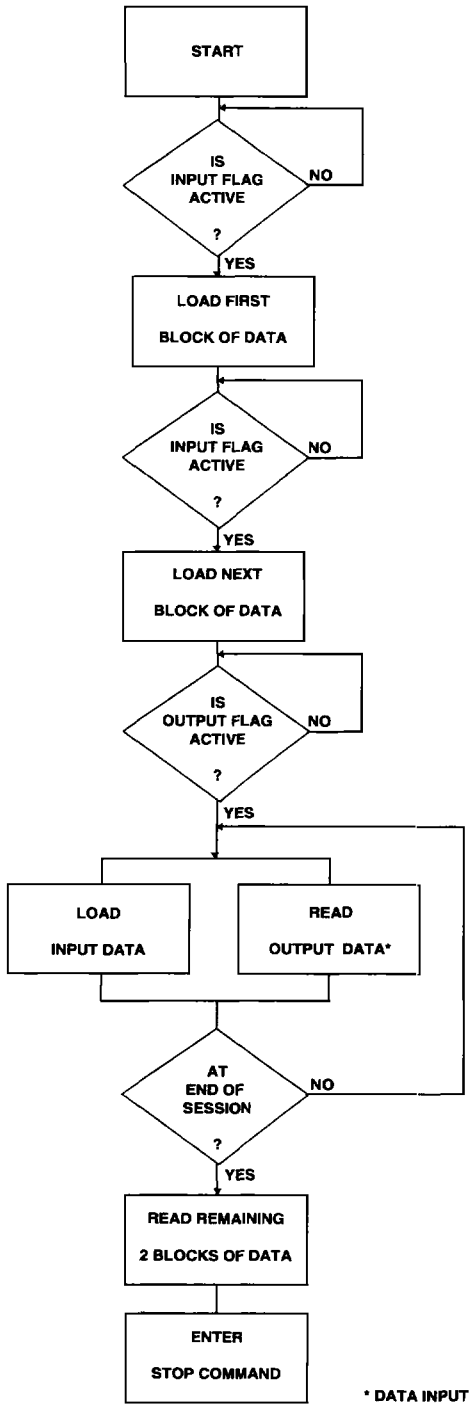


Figure 22 : Pipelining Operational Flow Chart

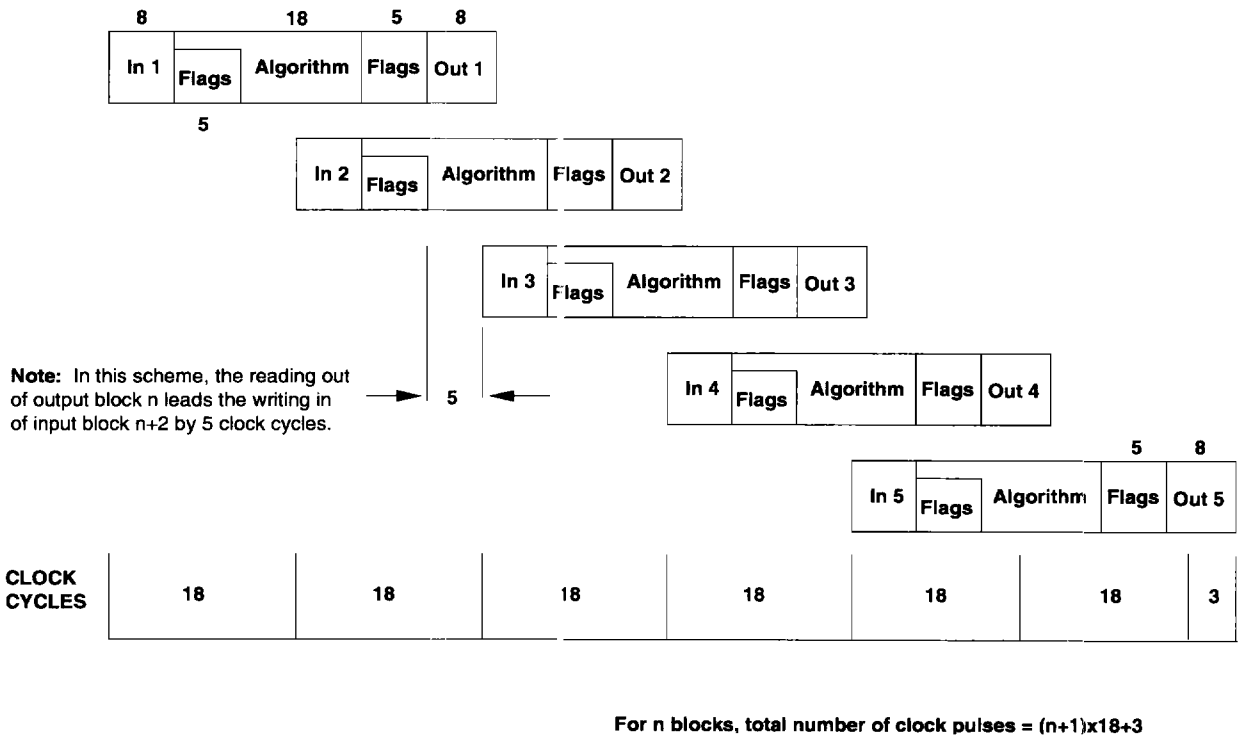


Figure 23 : Pipelined Minimum Timing Operation

COMMAND DESCRIPTION

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 8 shows all commands that may be given in Multiplexed Control Mode and Table 9 shows the subset executable in Direct Control Mode.

Load Clear M Key Through Auxiliary Port (90_H)

Load Clear E Key Through Auxiliary Port (91_H)

Load Clear D Key Through Auxiliary Port (92_H)

These commands override data flow specifications set in the Mode Register and cause the Master (M), Encrypt (E) or Decrypt (D) Key Register to be loaded with eight bytes written to the Auxiliary Port. Once the load command is written to the Command Register, the Auxiliary Port flag ($\overline{AFLG}$) pin will go active (LOW), as well as the Auxiliary Port Flag bit (S2) in the Status Register being set to "1", indicating that the device is able to accept key bytes at the Auxiliary Port bus. In addition, the Command Pending bit (S6) will go to "1" during the entire loading process.

When data has been setup on the Auxiliary Port pins, each byte is written by placing an active LOW signal on the Auxiliary Port Strobe ($\overline{ASTB}$). The actual write occurs on the rising edge of $\overline{ASTB}$. The Auxiliary Port Flag ($\overline{AFLG}$) will go inactive immediately after the eighth strobe goes active (LOW). However, the Command Pending bit (S6) will remain "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 (11_H)

Load Clear D Key Through Master Port (12_H)

These commands are available in both Multiplexed Control and Direct Control Modes. They override the data flow specifications set in the Mode Register and allow eight bytes of data to be written to the appropriate key register through the Master Port. In Multiplexed Control Mode, the command is initiated by writing the instruction 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/$\overline{S}$ input is LOW and the level on AUX_6-E/$\overline{D}$ determines which key register is loaded.

When the command has been recognized, the Command Pending bit (S6 in the Status Register) will go to "1" and in Direct Control Mode AUX_3-$\overline{CP}$ will go active (LOW), indicating that key loading may proceed. The host system then writes exactly eight bytes to the Input Register through the Master Port. When the Key Register has been loaded, the Command Pending bit will return to "0", and in Direct Control Mode the AUX_3-$\overline{CP}$ output will go inactive, indicating that the DCP can accept the next command.

Load Encrypted E Key Through Auxiliary Port ($B1_H$)

Load Encrypted D Key Through Auxiliary Port ($B2_H$)

These commands are only available in Multiplexed Control Mode. They are similar to the Load Clear E (or D) Key through Auxiliary Port commands, except that key bytes are initially decrypted using the Electronic Code Book algorithm and the Master (M) Key. The key bytes then pass through the parity checking logic and into the appropriate key register.

The Command Pending bit (S6) will be "1" during the entire decrypt-and-load operation. The Busy bit (S5) will be "1" during the actual decrypting of the key.

Load Encrypted E Key Through Master Port (31_H)

Load Encrypted D Key Through Master Port (32_H)

These commands (available in Multiplexed Control Mode only) are similar in effect to Load Clear E (or D) Key Through Master Port, except that key bytes are first decrypted using the Electronic Code Book algorithm and the Master (M) Key. The bytes are then loaded into the target key register, after having passed through the parity checking logic.

The Command Pending bit (S6) will be "1" during the entire decrypt-and-load operation. As well, the Busy bit (S5) will be "1" during the actual decryption process.

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

These commands (available in Multiplexed Control Mode only) are virtually identical to Load Clear E (or D) Key Through Master Port, except that the data written to the Input Register address is transferred to either the Initialization Vector for Encryption (IVE) or Decryption (IVD) Register instead of a Key Register and no parity checking takes place. The Command Pending bit (S6) is a "1" during the entire loading process.

Load Encrypted IVE Register Through Master Port ($A5_H$)
Load Encrypted IVD Register Through Master Port ($A4_H$)

These commands are similar to the Load Encrypted E (or D) Key Through Master Port commands. The data flow specification set in the Mode Register is overridden and the eight initial vector bytes are decrypted using the Decryption (D) Key and the Electronic Code Book algorithm. The resulting clear initial vector bytes are routed into the appropriate Initialization Vector Register, and no parity checking occurs. The Busy bit (S5) does not go to "1" during the decryption process, but Command Pending bit (S6) will be "1" during the entire decryption-and-load operation.

Read Clear IVE Register Through Master Port ($8D_H$)
Read Clear IVD Register Through Master Port ($8C_H$)

The effect of these commands (available in Multiplexed Control Mode only) is to override the data flow specifications set in the Mode Register and to allow the appropriate Initialization Vector Register to be read from the Output Register through the Master Port. When executing this instruction, each IV Register appears as eight bytes of FIFO storage. The first byte of data will be available six clocks after the loading of the Command Register. The Command Pending bit will be set to "1" and will remain a "1" until sometime after the eighth byte is read out. The host system has the responsibility to read out exactly eight bytes.

Read Encrypted IVE Register Through Master Port ($A9_H$)
Read Encrypted IVD Register Through Master Port ($A8_H$)

The effect of these commands (in Multiplexed Control Mode only) is to override the specifications set in the Mode Register and to encrypt the contents of the specified Initialization Vector Register using the Electronic Code Book algorithm and the Encrypt (E) Key. The resulting eight bytes of cipher text can be read from the Output Register through the Master Port. The Busy bit (S5) will be "1" during the encryption process, when it goes to "0, "the encrypted initial vector bytes are ready to be read out. The Command Pending bit (S6) will be "1" during the entire encryption-and-output process, and will go to "0" when the eighth byte is read out. The host system is responsible for reading out exactly eight bytes.

Encrypt with Master (M) Key (39_H)

This command (available in Multiplexed Control Mode only) overrides the data flow specifications set in the Mode Register and causes the DCP to write eight bytes of data to the Input Register via the Master Port. After the eighth byte has been received, the data is encrypted using the Master (M) Key and then routed to the Output Register, where it may be read out through the Master Port. The Command Pending (S6) and Busy (S5) bits are used to sense the three phases of this operation. Command Pending goes to "1" as soon as the Input Register can accept data. When exactly eight bytes have been entered, the Busy bit will got to "1" until the encryption process is complete. When Busy goes to "0", the encrypted data is available to be read out. Command Pending will return to "0" when the eighth byte has been read.

Start Encryption (41_H)

Start Decryption (40_H)

Start ($C0_H$)

The three "Start" commands begin normal data ciphering by setting the Start/Stop bit (S7) in the Status Register to "1." The Start Encryption and Start Decryption commands specify the ciphering direction by forcing the Encrypt/Decrypt bit (M4) in the Mode Register to "1" or "0", respectively. Whereas Start uses the current state of the Mode Register Encrypt/Decrypt bit, as specified in a previous Mode Register load. When any Start command has been entered, the port status flag (MFLG or SFLG) associated with the Input Register will become 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 of the AUX_5-S/$\overline{S}$ input. 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 ($E0_H$)

The Stop command sets the Start/Stop bit (S7) in the Status Register to "0." This causes the input flag ($\overline{MFLG}$ or $\overline{SFLG}$) to become inactive and inhibits the loading of any further data. Any ciphering in progress (Busy bit (S5) is "1" or AUX_2-$\overline{BSY}$ is active) will be completed and any data in the Output Register will remain accessible (except in CFB Mode). In either CFB Mode, the last byte of data must be read out before issuing the Stop command.

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.

Software Reset (00_H)

This command is similar to a hardware reset (CA95C68: $\overline{MRD}$ and $\overline{MWR}$ low, CA95C18: $\overline{MAS}$ and $\overline{MDS}$ low) in that it forces the DCP back to its default configuration, and all the processing flags go inactive. The default configuration for the Mode Register is: Electronic Code Book cipher type and dual port configuration with Master Port clear, Slave Port encrypted.

CA95C68/18/09 NOTES

This listing describes known operating variants between the CA95C68/18/09 devices and both the AMD AM9568/18 and VLSI VM009 devices. Also contained here are some CA95C68/18/09 operating idiosyncrasies.

1. **CA95C68/18/09 Reset**: The CA95C68/18/09 device does not operate in the default mode of operation until one of the reset operations are performed on it. Either a hardware reset, a software reset, or a write to the Mode Register must be performed before beginning to program the CA95C68/18/09 to ensure that the device is operating in the default mode.
2. **CA95C68/18/09 Direct Control Mode**: When the CA95C68/18/09 is programmed for Direct Control Mode (DCM) operation, the Input and Output Register address and $\overline{MCS}$ must be manually latched immediately before or immediately after DCM is entered. The device does not automatically address the Input and Output Registers (Address 0) when DCM is entered. This should be done before any operations are performed.
3. **CA95C68/18/09 Busy Bit in CFB-8 Cipher Mode**: When the CA95C68/18/09 is programmed for eight bit cipher feedback (CFB-8), ciphering in either Multiplexed Control or Direct Control Mode of operation, the Busy bit (bit 5 in the Status Register) and the $\overline{BSY}$ pin (AUX_2-$\overline{BSY}$ in DCM) go active before the Input Register is addressed. The Busy bit and the $\overline{BSY}$ pin go active immediately after the Mode Register is programmed for the CFB-8 cipher type. This bit (and pin in DCM) is not of great importance and should be ignored in this mode of operation.
4. **Synchronization for CA95C68/18/09 and VM009 Read/Write**: Compared to the VLSI VM009 device, the CA95C68/18/09 has a narrower window in which the read and write strobes must synchronize to the clock input. The CA95C68/18/09 AC parameter in question is t_{45} which is specified as a minimum of 3ns and a maximum of t_c-20ns. Therefore, the CA95C68/18/09 read and write strobes must be driven HIGH between 3 and 20ns after the falling edge of the clock if you are using the DCP strobes at 25MHz. With the VLSI device, the read and write synchronization occurs on the rising edge of the clock and there is only a 4ns region in which the strobes can not go HIGH for any clock frequency.
5. **Clock Frequency**: The clock input frequency for the various devices are:

AM9568	1.0 MHz to 4.0 MHz
AM9518	1.0 MHz to 3.1 MHz
CA95C68/18/09	0 MHz to 25MHz
VM009	0 MHz to 33 MHz

6. **One-Bit Cipher Feedback Mode**: This is a mode of encryption supported by the CA95C68/18/09 that the AMD and VLSI devices do not provide.

7. **Flag Output Assertion Timing Variant**: The AM9568/18 devices set and clear the flag output lines immediately after the corresponding event has occurred. The CA95C68/18/09 devices synchronize all internal events with respect to the falling edge of the clock input. Therefore, the flag output lines are set or cleared on the next falling clock edge after the corresponding event has occurred.
8. **IVE in Pipelined CBC Mode of Encryption**: The AM9568/18 presents the previous IVE instead of the current IVE during a read IVE operation after a series of CBC encryptions in which more than one round of data was in the encryption pipeline. In the CA95C68/18/09 devices, the correct IVE is presented for the pipelined CBC mode encryption scheme.
9. **Direct Control Mode, Mode Register Encrypt/Decrypt Bit Variant**: In Direct Control Mode (DCM), the AM9568/18 adjusts the sense of the Mode Register's Encrypt/Decrypt bit (M4) inconsistently; based on whether encryption or decryption is performed. The CA95C68/18/09 always sets the Encrypt/Decrypt bit to be the same sense as the AUX_6-E/$\overline{D}$ input line in this case.
10. **Key Parity in Direct Control Mode**: The AM9568/18 erroneously indicates a parity error during the loading of keys of correct parity in Direct Control Mode. The CA95C68/18/09 devices do not indicate a parity error in this scenario.
11. **Encrypted Key Load Parity Variant**: The AM9568/18 will clear a parity error regardless of whether the last byte of an encrypted key load has a parity error. The CA95C68/18/09 devices will indicate the parity of the last byte of an encrypted key load correctly, and if required, the parity error must be cleared by one of the specified methods.
12. **Mode Register's Encrypt/Decrypt Bit Status on a Command Abort Reset**: The AM9568/18 will not set the Encrypt/Decrypt bit high if that bit is low and a command is aborted. The CA95C68/18/09 devices will reset this bit high when the Mode Register is reset during a command abort sequence.

MECHANICALS

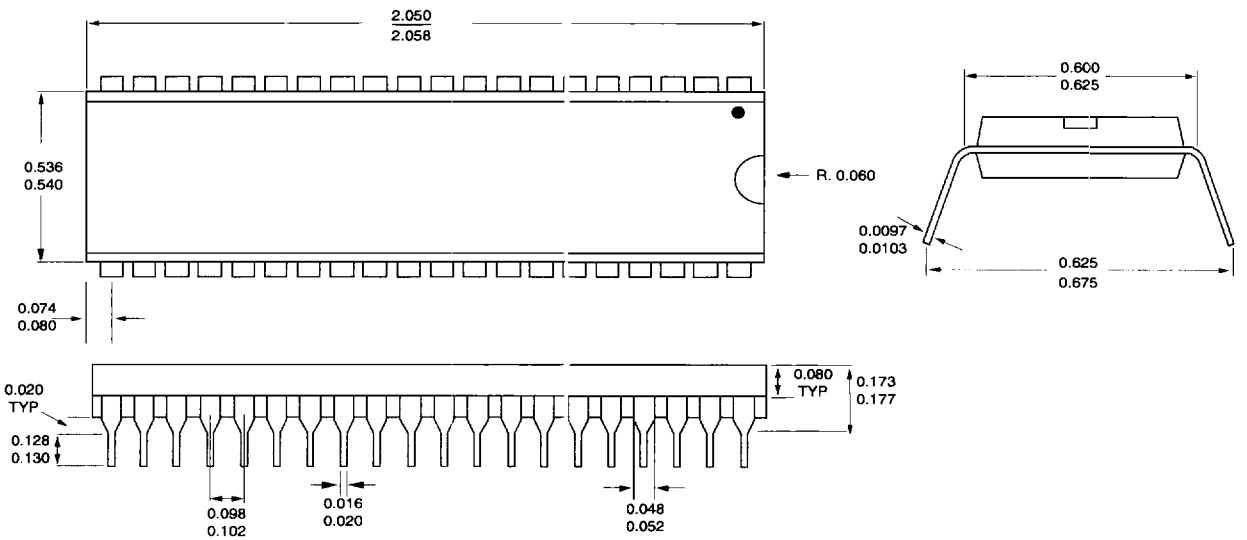


Figure 24 : 40-Pin PDIP Package

All dimensions in inches

MECHANICALS CONT'D

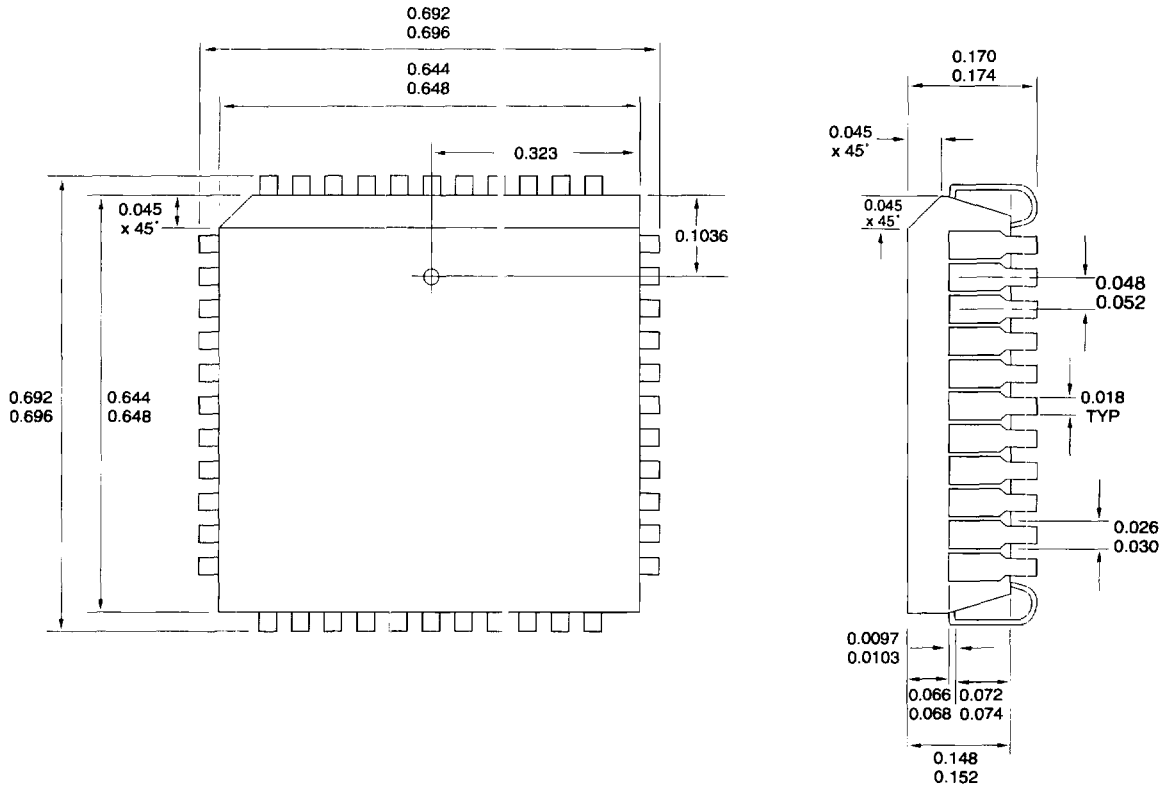
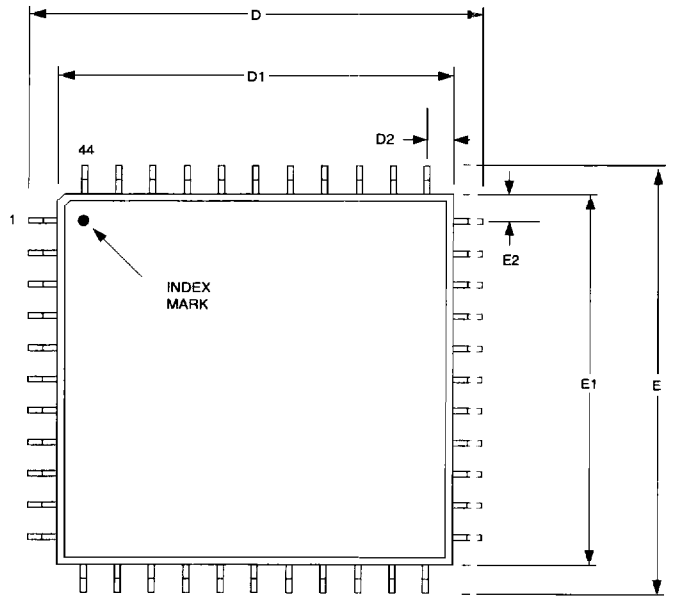


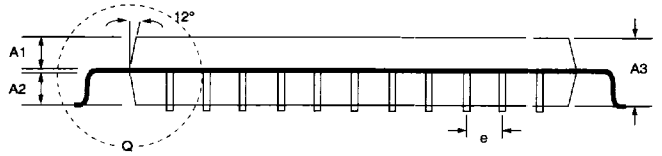
Figure 25 : 44-Pin PLCC Package

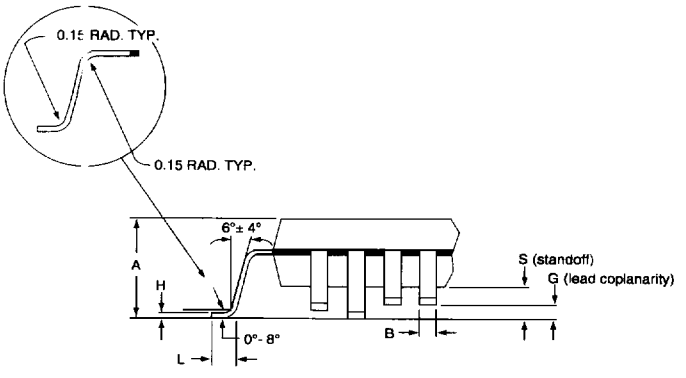
All dimensions in inches

MECHANICALS CONT'D



Dimensions	44 TQFP		
	MIN. (mm)	TYP. (mm)	MAX (mm)
A			1.60
A1		0.64	
A2		0.64	
A3	1.35	1.40	1.45
B	0.30	0.35	0.40
D	11.85	12.00	12.15
D1	9.95	10.00	10.05
D2		1.00	
e		0.80	
E	11.85	12.00	12.15
E1	9.95	10.00	10.05
E2		1.00	
G			0.08
H			0.17
L	0.50	0.60	0.75
S	0.05	0.10	0.15

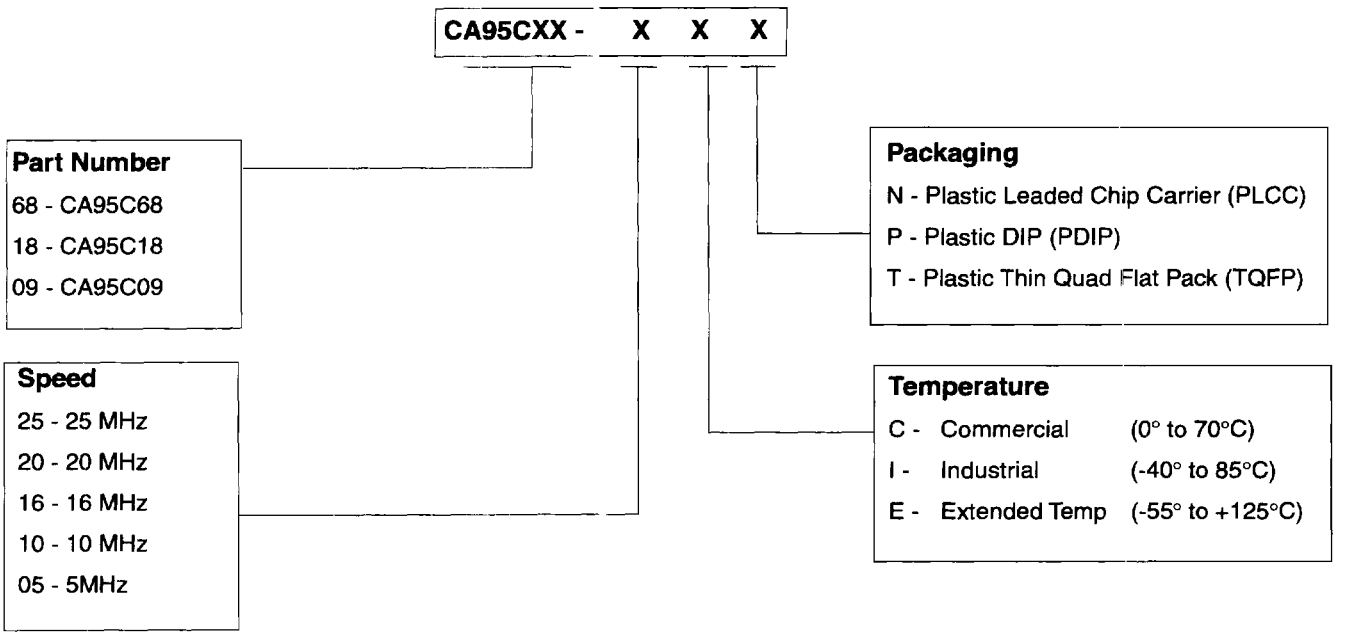




Detail Q

Figure 26 : 44-Pin TQFP Package

ORDERING INFORMATION and PRODUCT CODE



Newbridge Microsystems products are designated by a Product Code. When ordering, refer to products by their full code. For unusual, and/or specific packaging or processing requirements not covered by the standard product line, please contact our factory directly.

NEWBRIDGE MICROSYSTEMS
A Division of Newbridge Networks Corporation

695 High Glen Dr., San Jose, California 95133
Tel: (408) 258-3600 • Fax: (408) 258-3659

603 March Road, Kanata, Ontario Canada K2K 2M5
Tel: (613) 592-0714 or 1-800-267-7231 • Fax: (613) 592-1320