



8294 DATA ENCRYPTION UNIT

- Certified by National Bureau of Standards
- 80 Byte/Sec Data Conversion Rate
- 64-Bit Data Encryption Using 56-Bit Key
- DMA Interface
- 3 Interrupt Outputs to Aid in Loading and Unloading Data
- 7-Bit User Output Port
- Single 5V \pm 10% Power Supply
- Peripheral to MCS-86™, MCS-85™, MCS-80™ and MCS-48™ Processors
- Implements Federal Information Processing Data Encryption Standard
- Encrypt and Decrypt Modes Available

The Intel® 8294 Data Encryption Unit (DEU) is a microprocessor peripheral device designed to encrypt and decrypt 64-bit blocks of data using the algorithm specified in the Federal Information Processing Data Encryption Standard. The DEU operates on 64-bit text words using a 56-bit user-specified key to produce 64-bit cipher words. The operation is reversible: if the cipher word is operated upon, the original text word is produced. The algorithm itself is permanently contained in the 8294; however, the 56-bit key is user-defined and may be changed at any time.

The 56-bit key and 64-bit message data are transferred to and from the 8294 in 8-bit bytes by way of the system data bus. A DMA interface and three interrupt outputs are available to minimize software overhead associated with data transfer. Also, by using the DMA interface two or more DEUs may be operated in parallel to achieve effective system conversion rates which are virtually any multiple of 80 bytes/second. The 8294 also has a 7-bit TTL compatible output port for user-specified functions.

Because the 8294 implements the NBS encryption algorithm it can be used in a variety of Electronic Funds Transfer applications as well as other electronic banking and data handling applications where data must be encrypted.

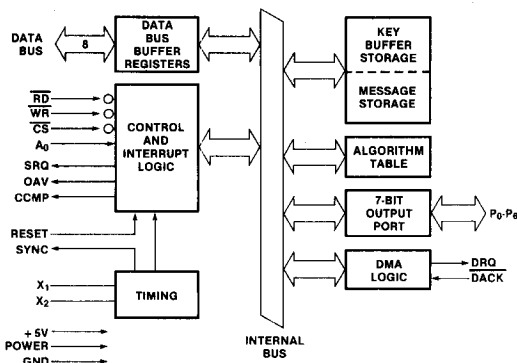


Figure 1. Block Diagram

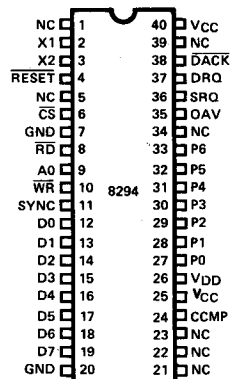


Figure 2. Pin Configuration

Table 1. Pin Description

Symbol	Pin No.	Type	Name and Function
NC	1		No Connection.
X1 X2	2 3	I	Crystal: Inputs for crystal, L-C or external timing signal to determine internal oscillator frequency.
RESET	4	I	Reset: A low signal to this pin resets the 8294.
NC	5		No Connection: No connection or tied high.
\overline{CS}	6	I	Chip Select: A low signal to this pin enables reading and writing to the 8294.
GND	7		Ground: This pin must be tied to ground.
\overline{RD}	8	I	Read: An active low read strobe at this pin enables the CPU to read data and status from the internal DEU registers.
A_0	9	I	Address: Address input used by the CPU to select DEU registers during read and write operations.
\overline{WR}	10	I	Write: An active low write strobe at this pin enables the CPU to send data and commands to the DEU.
SYNC	11	O	Sync: High frequency (Clock \div 15) output. Can be used as a strobe for external circuitry.
D ₀ D ₁ D ₂ D ₃ D ₄ D ₅ D ₆ D ₇	12 13 14 15 16 17 18 19	I/O	Data Bus: Three-state, bi-directional data bus lines used to transfer data between the CPU and the 8294.
GND	20		Ground: This pin must be tied to ground.
V _{CC}	40		Power: +5 volt power input: +5V \pm 10%.

Symbol	Pin No.	Type	Name and Function
NC	39		No Connection.
DACK	38	I	DMA Acknowledge: Input signal from the 8257 DMA Controller acknowledging that the requested DMA cycle has been granted.
DRQ	37	O	DMA Request: Output signal to the 8257 DMA Controller requesting a DMA cycle.
SRQ	38	O	Service Request: Interrupt to the CPU indicating that the 8294 is awaiting data or commands at the input buffer. SRQ=1 implies IBF=0.
OAV	35	O	Output Available: Interrupt to the CPU indicating that the 8294 has data or status available in its output buffer. OAV=1 implies OBF=1.
NC	34		No Connection.
P6 P5 P4 P3 P2 P1 P0	33 32 31 30 29 28 27	O	Output Port: User output port lines. Output lines available to the user via a CPU command which can assert selected port lines. These lines have nothing to do with the encryption function. At power-on, each line is in a 1 state.
V _{DD}	26		Power: +5V power input. (+5V \pm 10%) Low power standby pin.
V _{CC}	25		Power: Tied high.
CCMP	24	O	Conversion Complete: Interrupt to the CPU indicating that the encryption/decryption of an 8-byte block is complete.
NC	23		No Connection.
NC	22		No Connection.
NC	21		No Connection.

FUNCTIONAL DESCRIPTION

OPERATION

The data conversion sequence is as follows:

1. A Set Mode command is given, enabling the desired interrupt outputs.
2. An Enter New Key command is issued, followed by 8 data inputs which are retained by the DEU for encryption/decryption. Each byte must have odd parity.
3. An Encrypt Data or Decrypt Data command sets the DEU in the desired mode.

After this, data conversions are made by writing 8 data bytes and then reading back 8 converted data bytes. Any of the above commands may be issued between data conversions to change the basic operation of the DEU; e.g., a Decrypt Data command could be issued to change the DEU from encrypt mode to decrypt mode without changing either the key or the interrupt outputs enabled.

INTERNAL DEU REGISTERS

Four internal registers are addressable by the master processor: 2 for input, and 2 for output. The following table describes how these registers are accessed.

RD	WR	CS	A ₀	Register
1	0	0	0	Data input buffer
0	1	0	0	Data output buffer
1	0	0	1	Command input buffer
0	1	0	1	Status output buffer
X	X	1	X	Don't care

The functions of each of these registers are described below.

Data Input Buffer — Data written to this register is interpreted in one of three ways, depending on the preceding command sequence.

1. Part of a key.
2. Data to be encrypted or decrypted.
3. A DMA block count.

Data Output Buffer — Data read from this register is the output of the encryption/decryption operation.

Command Input Buffer — Commands to the DEU are written into this register. (See command summary below.)

Status Output Buffer — DEU status is available in this register at all times. It is used by the processor for poll-driven command and data transfer operations.

STATUS BIT:	7	6	5	4	3	2	1	0
FUNCTION:	X	X	X	KPE	CF	DEC	IBF	OBF

OBF Output Buffer Full; OBF = 1 indicates that output from the encryption/decryption function is available in the Data Output Buffer. It is reset when the data is read.

IBF Input Buffer Full; A write to the Data Input Buffer or to the Command Input Buffer sets IBF = 1. The DEU resets this flag when it has accepted the input byte. Nothing should be written when IBF = 1.

DEC Decrypt; indicates whether the DEU is in an encrypt or a decrypt mode. DEC = 1 implies the decrypt mode. DEC = 0 implies the encrypt mode.

CF Completion Flag; This flag may be used to indicate any or all of three events in the data transfer protocol.

1. It may be used in lieu of a counter in the processor routine to flag the end of an 8-byte transfer.
2. It must be used to indicate the validity of the KPE flag.
3. It may be used in lieu of the CCMP interrupt to indicate the completion of a DMA operation.

KPE Key Parity Error; After a new key has been entered, the DEU uses this flag in conjunction with the CF flag to indicate correct or incorrect parity.

COMMAND SUMMARY

1 — Enter New Key

OP CODE:	0	1	0	0	0	0	0	0
	MSB							LSB

This command is followed by 8 data byte inputs which are retained in the key buffer (RAM) to be used in encrypting and decrypting data. These data bytes must have odd parity represented by the LSB.

2 — Encrypt Data

OP CODE:	0	0	1	1	0	0	0	0
	MSB							LSB

This command puts the 8294 into the encrypt mode.

3 — Decrypt Data

OP CODE:	0	0	1	0	0	0	0	0
	MSB							LSB

This command puts the 8294 into the decrypt mode.

4 — Set Mode

OP CODE:	0	0	0	0	A	B	C	D
	MSB							LSB

where:

- A is the OAV (Output Available) interrupt enable
- B is the SRQ (Service Request) interrupt enable
- C is the DMA (Direct Memory Access) transfer enable
- D is the CCMP (Conversion Complete) interrupt enable

This command determines which interrupt outputs will be enabled. A "1" in bits A, B, or D will enable the OAV, SRQ, or CCMP interrupts respectively. A "1" in bit C will allow DMA transfers. When bit C is set the OAV and SRQ interrupts should also be enabled (bits A,B=1). Following the command in which bit C, the DMA bit, is set, the 8294 will expect one data byte to specify the number of 8-byte blocks to be converted using DMA.

5 — Write to Output Port

OP CODE:

1	P ₆	P ₅	P ₄	P ₃	P ₂	P ₁	P ₀
---	----------------	----------------	----------------	----------------	----------------	----------------	----------------

MSBLSB

This command causes the 7 least significant bits of the command byte to be latched as output data on the 8294 output port. The initial output data is 1111111. Use of this port is independent of the encryption/decryption function.

PROCESSOR/DEU INTERFACE PROTOCOL ENTERING A NEW KEY

The timing sequence for entering a new key is shown in Figure 3. A flowchart showing the CPU software to accommodate this sequence is given in Figure 4.

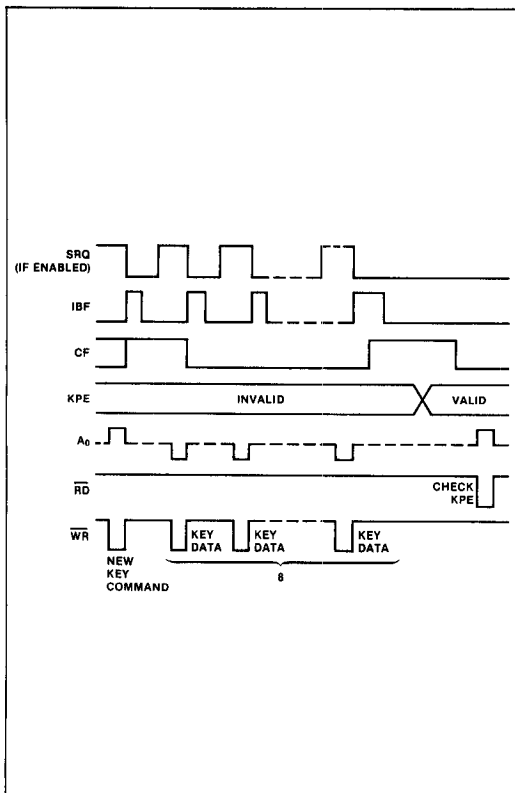


Figure 3. Entering a New Key

After the Enter New Key command is issued, 8 data bytes representing the new key are written to the data input buffer (most significant byte first). After the eighth byte is accepted by the DEU, CF goes true (CF = 1). The CF bit goes false again when KPE is valid. The CPU can then check the KPE flag. If KPE = 1, a parity error has been detected and the DEU has not accepted the key. Each byte is checked for odd parity, where the parity bit is the LSB of each byte.

Since the CF bit is used in this protocol to indicate the validity of the KPE flag, it may not be used to flag the end of the 8 byte key entry. CF = 1 only as long as KPE is invalid. Therefore, the CPU might not detect that CF = 1 and the key entry is complete before KPE becomes valid. Thus, a counter should be used, as in Figure 4, to flag the end of the new key entry. Then, CF is used to indicate a valid KPE flag.

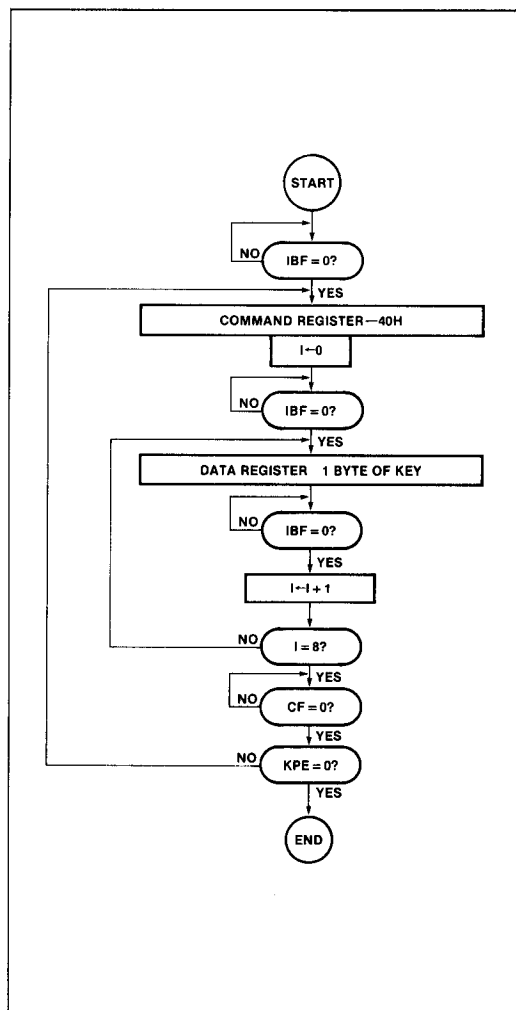


Figure 4. Flowchart for Entering a New Key

ENCRYPTING OR DECRYPTING DATA

Figure 5 shows the timing sequence for encrypting or decrypting data. The CPU writes 8 data bytes to the DEU's data input buffer for encryption/decryption. CF then goes true ($CF = 1$) to indicate that the DEU has accepted the 8-byte block. Thus, the CPU may test for $IBF = 0$ and $CF = 1$ to terminate the input mode, or it may use a software counter. When the encryption/decryption is complete, the CCMP and OAV interrupts are asserted and the OBF flag is set true ($OBF = 1$). OAV and OBF are set false again after each of the converted data bytes is read back by the CPU. The CCMP interrupt is set false, and remains false, after the first read. After 8 bytes have been read back by the CPU, CF goes false ($CF = 0$). Thus, the CPU may test for $CF = 0$ to terminate the read mode. Also, the CCMP interrupt may be used to initiate a service routine which performs the next series of 8 data reads and 8 data writes.

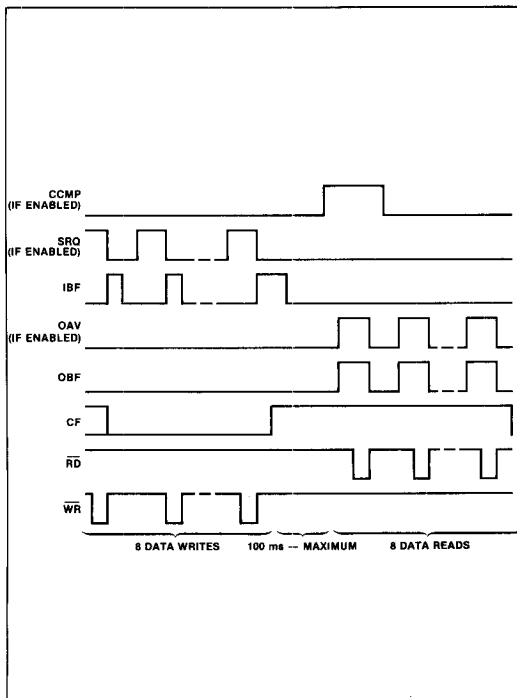


Figure 5. Encrypting/Decrypting Data

Figure 6 offers two flowcharts outlining the alternative means of implementing the data conversion protocol. Either the CF flag or a software counter may be used to end the read and write modes.

$SRQ = 1$ implies $IBF = 0$, $OAV = 1$ implies $OBF = 1$. This allows interrupt routines to do data transfers without checking status first. However, the OAV service routine must detect and flag the end of a data conversion.

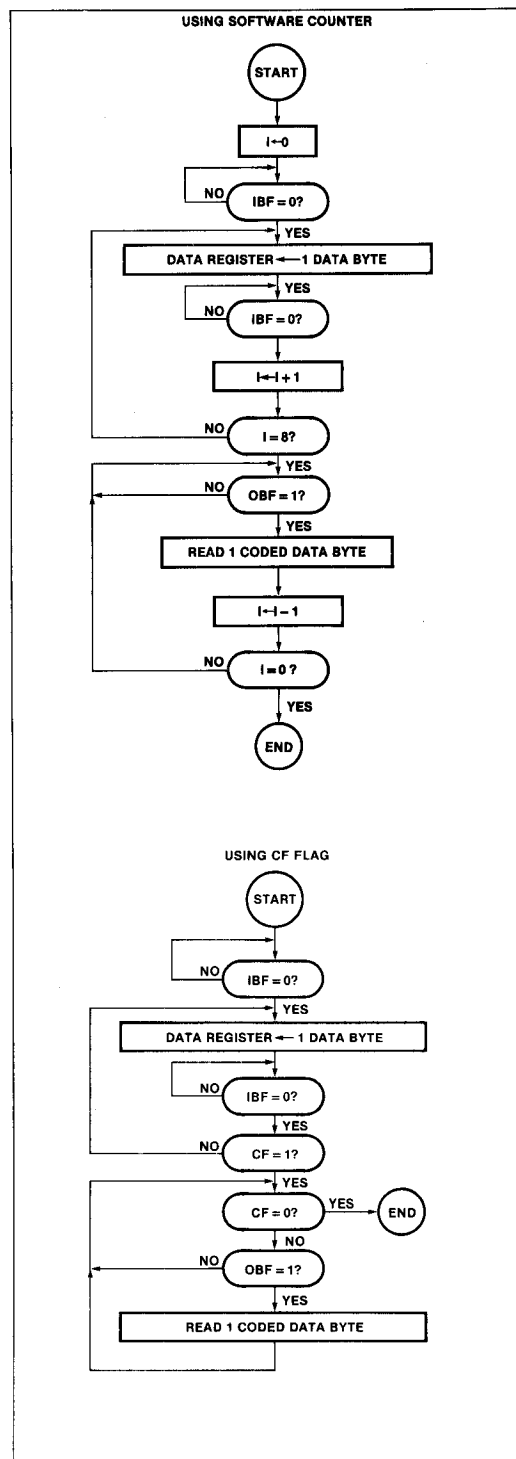


Figure 6. Data Conversion Flowcharts

CPU/DEU INTERFACES

Figures 12 through 15 illustrate four interface configurations used in the CPU/DEU data transfers. In all cases SRQ will be true (if enabled) and IBF will be false when the DEU is ready to accept data or commands.

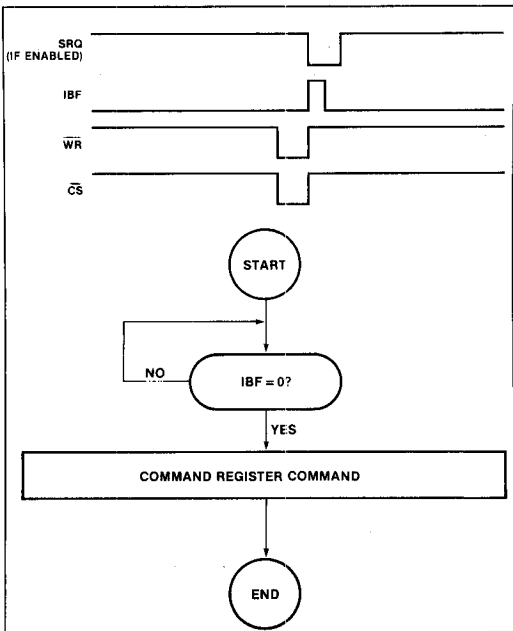


Figure 10. Single Byte Commands

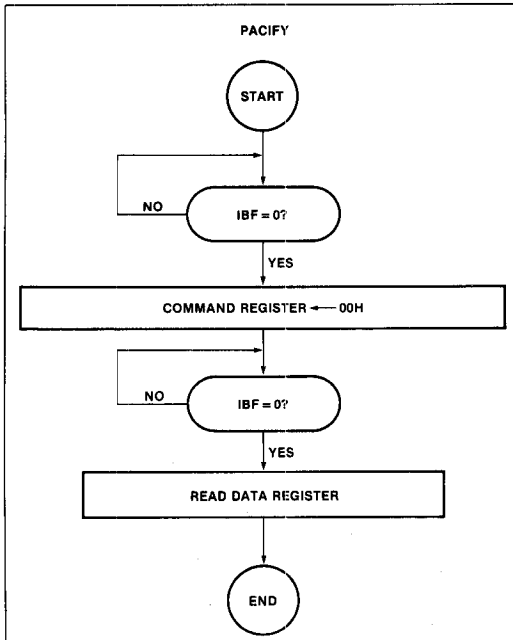


Figure 11. Pacify Protocol

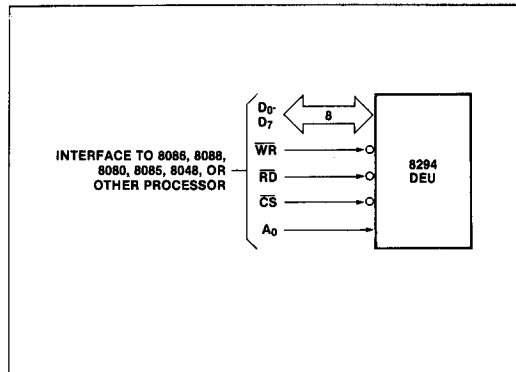


Figure 12. Polling Interface

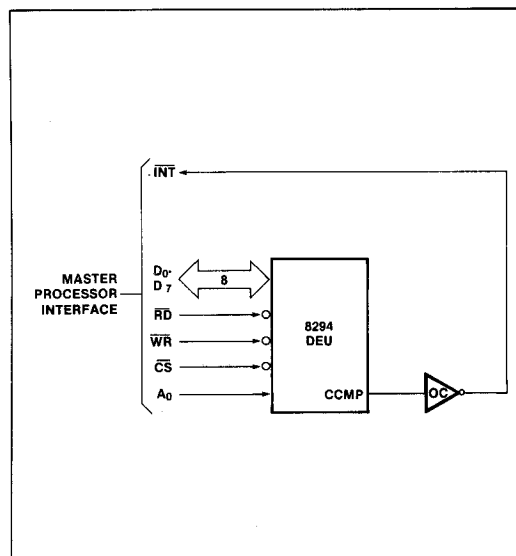


Figure 13. Single Interrupt Interface

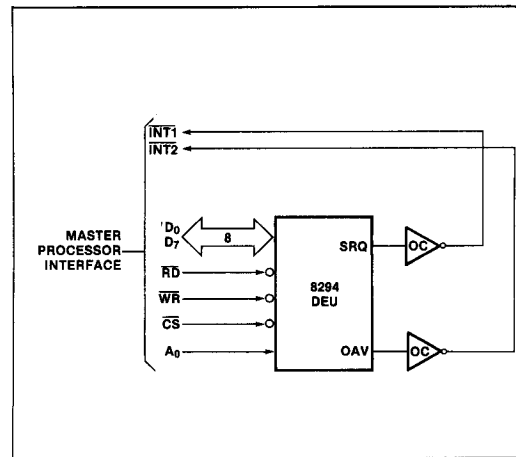


Figure 14. Dual Interrupt Interface

USING DMA

The timing sequence for data conversions using DMA is shown in Figure 7. This sequence can be better understood when considered in conjunction with the hardware DMA interface in Figure 8. Note that the use of the DMA feature requires 3 external AND gates and 2 DMA channels (one for input, one for output). Since the DEU has only one DMA request pin, the SRQ and OAV outputs are used in conjunction with two of the AND gates to create separate DMA request outputs for the 2 DMA channels. The third AND gate combines the two active-low DACK inputs.

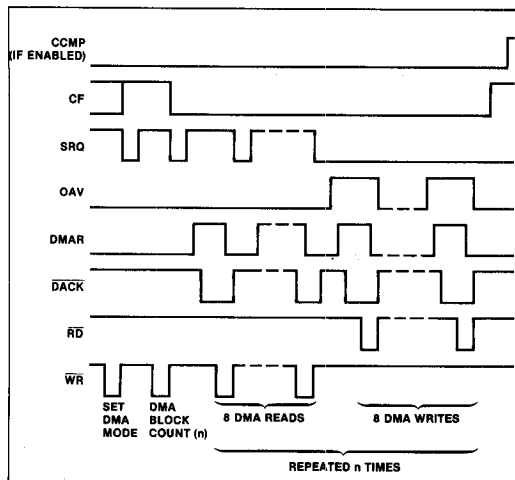


Figure 7. DMA Sequence

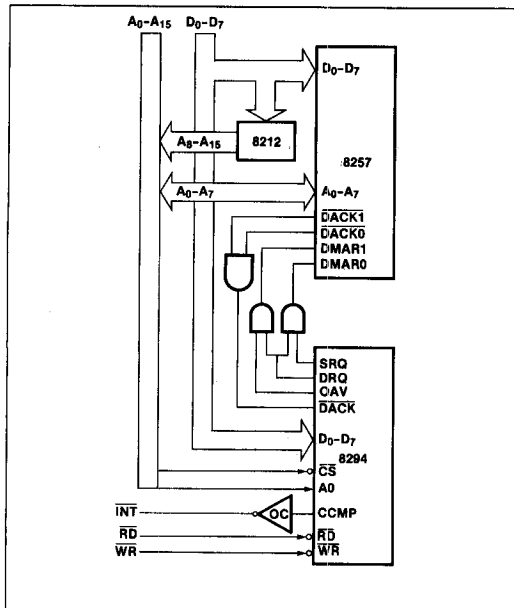


Figure 8. DMA Interface

To initiate a DMA transfer, the CPU must first initialize the two DMA channels as shown in the flowchart in Figure 9. It must then issue a Set Mode command to the DEU enabling the OAV, SRQ, and DMA outputs. The CCMP interrupt may be enabled or disabled, depending on whether that output is desired. Following the Set Mode command, there must be a data byte giving the number of 8-byte blocks of data ($n < 256$) to be converted. The DEU then generates the required number of DMA requests to the 2 DMA channels with no further CPU intervention. When the requested number of blocks has been converted, the DEU will set CF and assert the CCMP interrupt (if enabled). CCMP then goes false again with the next write to the DEU (command or data). Upon completion of the conversion, the DMA mode is disabled and the DEU returns to the encrypt/decrypt mode. The enabled interrupt outputs, however, will remain enabled until another Set Mode command is issued.

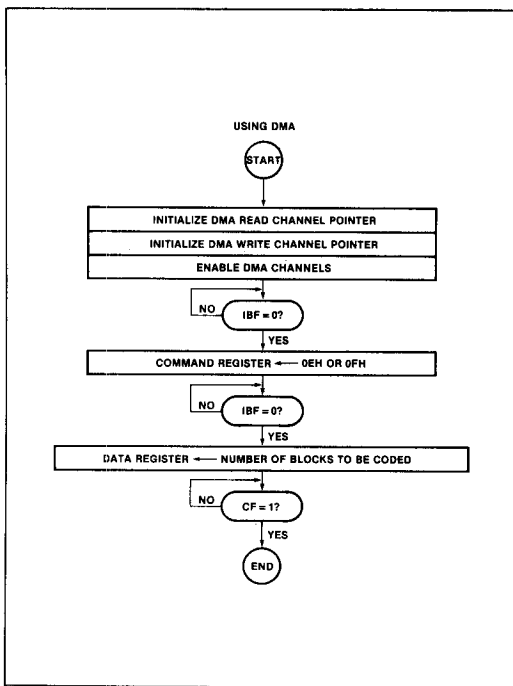


Figure 9. DMA Flowchart

SINGLE BYTE COMMANDS

Figure 10 shows the timing and protocol for single byte commands. Note that any of the commands is effective as a pacify command in that they may be entered at any time, except during a DMA conversion. The DEU is thus set to a known state. However, if a command is issued out of sequence, an additional protocol is required (Figure 11). The CPU must wait until the command is accepted ($IBF = 0$). A data read must then be issued to clear anything the preceding command sequence may have left in the Data Output Buffer.

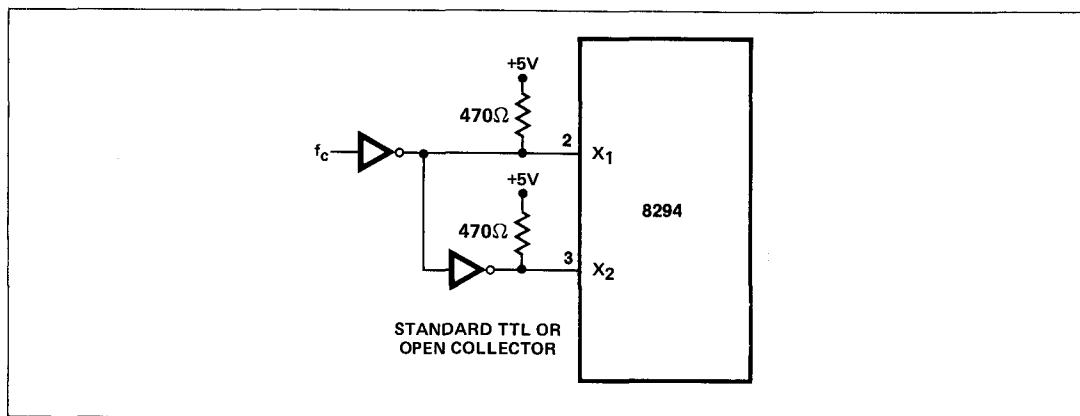


Figure 18. Recommended Connection for External Clock Signal

ABSOLUTE MAXIMUM RATINGS*

Ambient Temperature Under Bias 0°C to 70°C
 Storage Temperature -65°C to +150°C
 Voltage on Any Pin With
 Respect to Ground -0.5V to +7V
 Power Dissipation 1.5 Watt

**NOTICE: Stresses above those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.*

D.C. AND OPERATING CHARACTERISTICS (T_A = 0°C to 70°C, V_{CC} = +5V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Limits			Unit	Test Conditions
		Min.	Typ.	Max.		
V _{IL}	Input Low Voltage (All Except X ₁ , X ₂ , RESET)	-0.5		0.8	V	
V _{IL1}	Input Low Voltage (X ₁ , X ₂ , RESET)	-0.5		0.6	V	
V _{IH}	Input High Voltage (All Except X ₁ , X ₂ , RESET)	2.2		V _{CC}	V	
V _{IH1}	Input High Voltage (X ₁ , X ₂ , RESET)	3.8		V _{CC}	V	
V _{OL}	Output Low Voltage (D ₀ -D ₇)			0.45	V	I _{OL} = 2.0 mA
V _{OL1}	Output Low Voltage (All Other Outputs)			0.45	V	I _{OL} = 1.6 mA
V _{OH}	Output High Voltage (D ₀ -D ₇)	2.4			V	I _{OH} = -400 μA
V _{OH1}	Output High Voltage (All Other Outputs)	2.4			V	I _{OH} = -50 μA
I _{IL}	Input Leakage Current (RD, WR, CS, A ₀)			±10	μA	V _{SS} ≤ V _{IN} ≤ V _{CC}
I _{OZ}	Output Leakage Current (D ₀ -D ₇ , High Z State)			±10	μA	V _{SS} + 0.45 ≤ V _{OUT} ≤ V _{CC}
I _{DD}	V _{DD} Supply Current		5	15	mA	
I _{DD} + I _{CC}	Total Supply Current		60	125	mA	
I _{LI}	Low Input Load Current (Pins 24, 27-38)			0.5	mA	V _{IL} = 0.8V
I _{LI1}	Low Input Load Current (RESET)			0.2	mA	V _{IL} = 0.8V
I _{IH}	Input High Leakage Current (Pins 24, 27-38)			100	μA	V _{IN} = V _{CC}
C _{IN}	Input Capacitance			10	pF	
C _{I/O}	I/O Capacitance			20	pF	

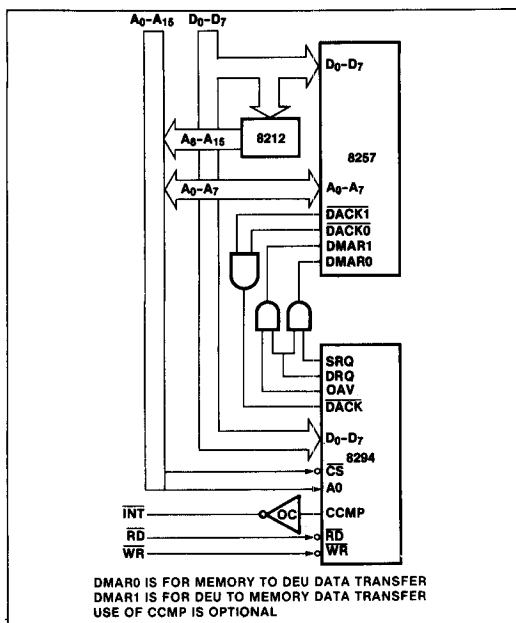


Figure 15. DMA Interface

OSCILLATOR AND TIMING CIRCUITS

The 8294's internal timing generation is controlled by a self-contained oscillator and timing circuit. A choice of crystal, L-C or external clock can be used to derive the basic oscillator frequency.

The resident timing circuit consists of an oscillator, a state counter and a cycle counter as illustrated in Figure 16.

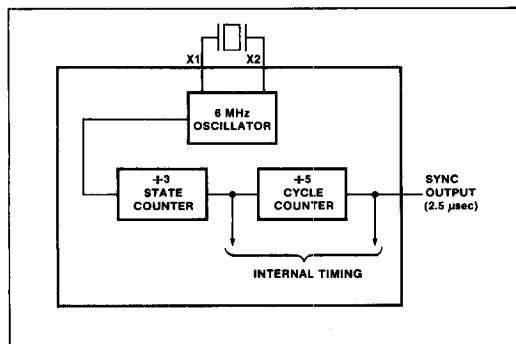


Figure 16. Oscillator Configuration

OSCILLATOR

The on-board oscillator is a series resonant circuit with a frequency range of 1 to 6 MHz. Pins X1 and X2 are input and output (respectively) of a high gain amplifier stage. A crystal or inductor and capacitor connected between X1 and X2 provide the feedback and proper phase shift for oscillation. Recommended connections for crystal or L-C are shown in Figure 17.

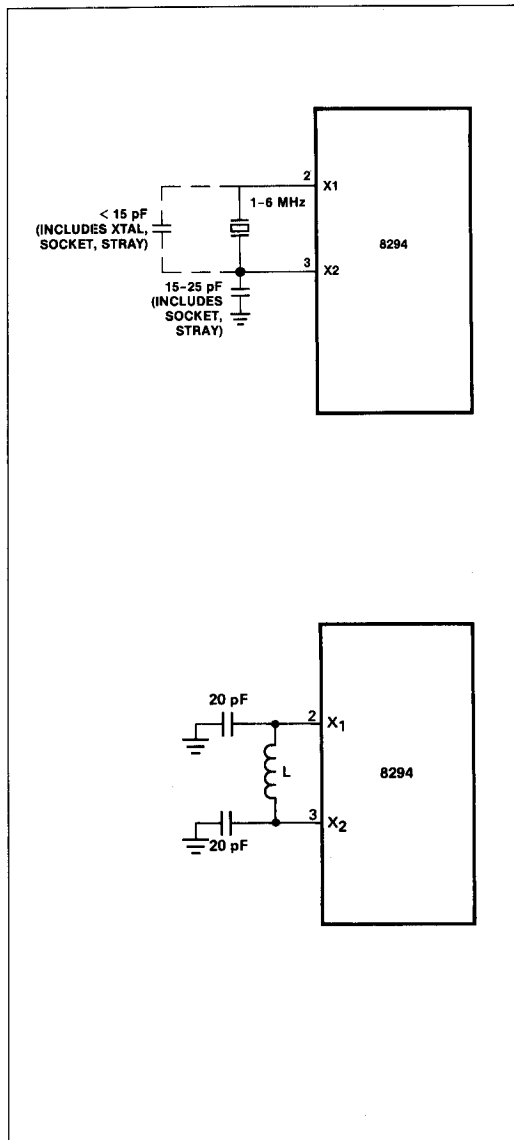


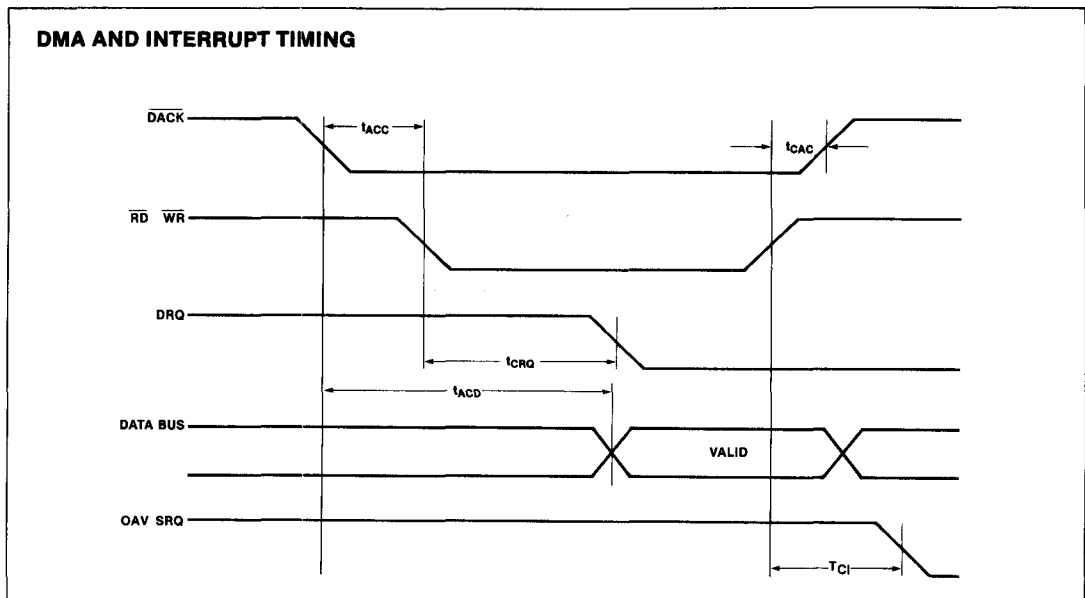
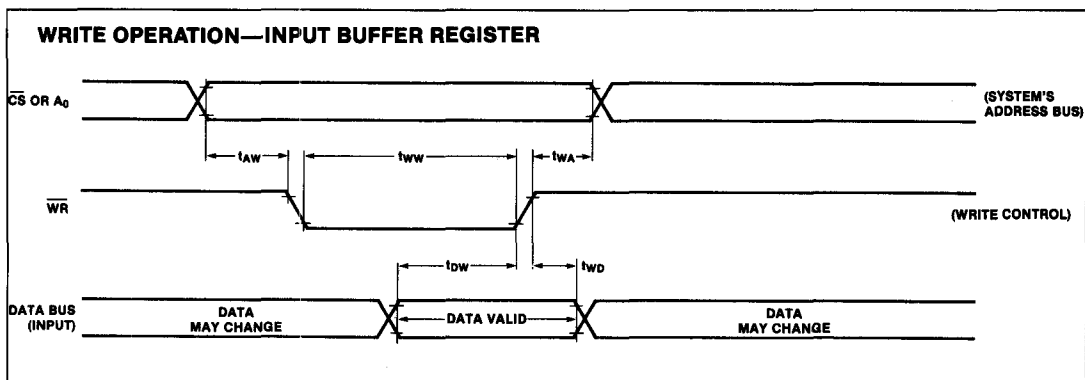
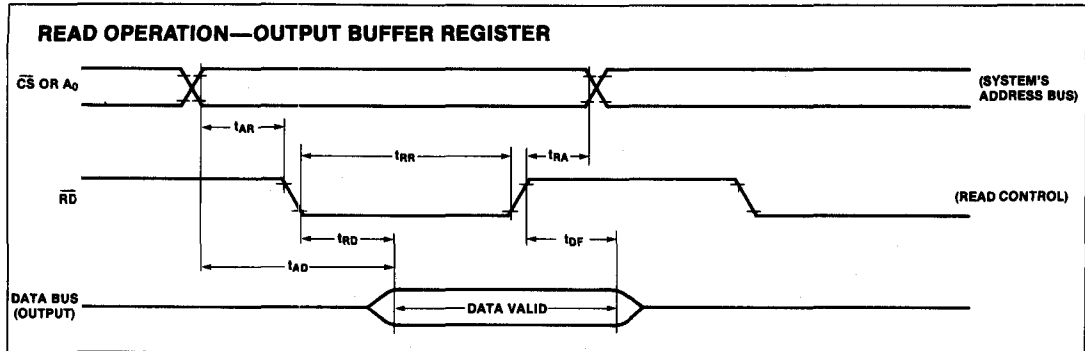
Figure 17. Recommended Crystal and L-C Connections

A recommended range of inductance and capacitance combinations is given below:

- L = 120 μ H corresponds to 3 MHz
- L = 45 μ H corresponds to 5 MHz

An external clock signal can also be used as a frequency reference to the 8294; however, the levels are *not* compatible. The signal must be in the 1 MHz-6 MHz frequency range and must be connected to pins X1 and X2 by buffers with a suitable pull-up resistor to guarantee that a logic "1" is above 3.8 volts. The recommended connection is shown in Figure 18.

WAVEFORMS



A.C. CHARACTERISTICS ($T_A = 0^\circ\text{C}$ to 70°C , $V_{CC} = V_{DD} = +5V \pm 10\%$, $V_{SS} = 0V$)

DBB READ

Symbol	Parameter	Min.	Max.	Unit	Test Conditions
t_{AR}	\overline{CS} , A_0 Setup to $\overline{RD} \downarrow$	0		ns	
t_{RA}	\overline{CS} , A_0 Hold After $\overline{RD} \uparrow$	0		ns	
t_{RR}	\overline{RD} Pulse Width	250		ns	
t_{AD}	\overline{CS} , A_0 to Data Out Delay		225	ns	$C_L = 150\text{ pF}$
t_{RD}	$\overline{RD} \downarrow$ to Data Out Delay		225	ns	$C_L = 150\text{ pF}$
t_{DF}	$\overline{RD} \uparrow$ to Data Float Delay		100	ns	
t_{CY}	Cycle Time	2.5	15	μs	6 MHz Crystal

DBB WRITE

Symbol	Parameter	Min.	Max.	Unit	Test Conditions
t_{AW}	\overline{CS} , A_0 Setup to $\overline{WR} \downarrow$	0		ns	
t_{WA}	\overline{CS} , A_0 Hold After $\overline{WR} \uparrow$	0		ns	
t_{WW}	\overline{WR} Pulse Width	250		ns	
t_{DW}	Data Setup to $\overline{WR} \uparrow$	150		ns	
t_{WD}	Data Hold to $\overline{WR} \uparrow$	0		ns	

DMA AND INTERRUPT TIMING

Symbol	Parameter	Min.	Max.	Unit	Test Conditions
t_{ACC}	\overline{DACK} Setup to Control	0		ns	
t_{CAC}	\overline{DACK} Hold After Control	0		ns	
t_{ACD}	\overline{DACK} to Data Valid		225	ns	$C_L = 150\text{ pF}$
t_{CRQ}	Control L.E. to \overline{DRQ} T.E.		200	ns	
t_{CI}	Control T.E. to Interrupt T.E.		$t_{CY} + 500$	ns	

A.C. TESTING INPUT, OUTPUT WAVEFORM

