PRODUCT DESCRIPTION
TMS7500/TMS75C00 – DATA ENCRYPTION DEVICE

1. INTRODUCTION

1.1 DESCRIPTION

The TMS7500 and TMS75C00 are inexpensive data encryption devices of the TMS7000 8-bit Microcomputer Family. These peripheral devices are designed to perform the National Bureau of Standards (NBS) Data Encryption Standard (DES) algorithm. The DES algorithm is specified in the Federal Information Processing Standard (FIPS) Publication 46.

The TMS7500 and TMS75C00 Data Encryption Devices (DED)* are firmware products derived from the TMS7020 and TMS70C20. Because of the similarities between the TMS7020 and TMS70C20, the TMS7500 and TMS75C00 are pin-to-pin functionally identical in operation. The only difference is that the TMS7500 is built using NMOS technology while the TMS75C00 is built using CMOS technology. Because the TMS7500 and TMS75C00 are based on 8-bit single-chip microcomputers that are in high volume production, they can be a very cost effective solution for low cost data encryption requirements.

1.2 TYPICAL APPLICATIONS

For simplicity, the term TMS7500 will refer to both the TMS7500 and TMS75C00 devices unless otherwise stated.

The TMS7500 is particularly well suited for any system requiring the use of a low-cost, medium-speed data encryption device. It can easily keep up with the data rates required by most modems and terminals without sacrificing system performance. Some typical applications are:

- Computer-to-terminal communication links
- Home banking communication links
- Teller machines for banks
- Portable terminals
- Point of sale terminals
- Small business systems
- Trade market software protection
- Any system requiring a low-cost, medium-speed data encryption device

1.3 KEY FEATURES

A number of key features, most of which are user programmable, enables the TMS7500 to enhance the flexibility of any system using data encryption. The device can store two keys at one time and operate in two of the standard data encryption modes. Some of the key features are:

- Validated by the National Bureau of Standards (NBS)
- Can store both a master and an active 64-bit key for coding and decoding
- Active key can be encrypted or decrypted by the master key internally
- Two DES modes of operation: Electronic Codebook (ECB) and Cipher Feedback (CFB)
- Dual 8-bit data buses: one for uncoded data, the other for ciphered data (optional)
- A programmable command register and accessible status register
- Status register data is available on external pins and can be read from the data bus
- Internal or external clock source
- On-Chip clock uses crystal or ceramic resonator
- Maximum data rate of 3200 bits-per-second for ECB and 400 bits-per-second for 8-bit CFB with TMS7500
- Maximum data rate of 2304 bits-per-second for ECB and 288 bits-per-second for 8-bit CFB with TMS75C00
- Single-power source requirements
- TMS75C00 offers a low-power operating supply current requirement of 5.5 mA typical (3 MHz clock)

* The products covered by this document (TMS7500 and TMS75C00) are within the group of electronic products that are wholly or partly of U.S. origin or technology, the export of which is subject to export license control by the U.S. Government. Therefore, prior to exportation, you are obligated to obtain the required export license from the U.S. Department of State. (Refer to Title 22, Code of Federal Regulations.)

- Available in a 40-pin plastic package with either a 100-mil or 70-mil pin spacing.
- I/O pins are TTL compatible for TMS7500, CMOS compatible for TMS75C00.

1.4 DEVICE INFORMATION

Both TMS7500 and TMS75C00 devices can be ordered from Texas Instruments in either a standard 600-mil, 40-pin plastic package with 100-mil pin-to-pin spacings or a shrink 600-mil, 40-pin plastic package with 70-mil pin-to-pin spacing.

The divide-by-2 (/2) or the divide-by-4 (/4) clock options are available for the TMS7500 while only the divide-by-2 (/2) clock option is available for the TMS75C00. See the TMS7500/75C00 DATA ENCRYPTION DEVICE DATA MANUAL (Part Number SPNS004) for a complete explanation of the available clock options.

The TMS7500 requires a single 5-volt power supply and all I/O pins are TTL compatible. The TMS75C00 requires a single 3 to 6 volt power supply and features a low current requirement of 5.5 mA typical (at a 3 MHz external clock rate and V_{DD} = 5 V).

1.5 FUNCTIONAL BLOCK DIAGRAM

The functional block diagram of the TMS7500 Data Encryption Device in Figure 1 illustrates a firmware architecture organized around certain registers, buffers, and I/O buses which are all linked together through data selectors. All of the necessary data path sequences through these selectors are determined by a 5-bit command register and eight external control-handshake pins. The device status is stored in the status register and is also available on the status output pins. The 64-bit key values and encryption data are passed along the 8-bit main data bus and cipher data bus.

2. PROCESSOR INTERFACE

The TMS7500 incorporates two 8-bit data buses; the main data bus and the optional cipher data bus. All plain (uncoded) data is handled by the main data bus, whereas all encrypted (coded) data flows on the cipher data bus. This flow of data improves system security. For example, in the encryption process, plain data is written to the main data bus and encrypted data is read from the cipher bus. For deciphering, coded data is written to the cipher bus and plain data is read from the main bus.

Since both buses share the same handshake control lines used for data transfers, data can only pass to or from the TMS7500 one byte (8-bits) at a time on either bus.

The processor accesses the command and status registers, both master and active key registers and the 8-byte data buffer through the main data bus. Of course, the optional cipher data bus can be used to handle all encrypted data. The 7-bit read-only status register provides the host processor with current status information such as:

- Key entered
- Key parity error
- Active key register is being accessed
- Encrypt or decrypt mode
- Electronic codebook or cipher feedback mode
- Initialization Vector (IV) loaded (for cipher feedback mode)

The 5-bit write-only command register accepts several different commands from the processor, including the following commands:

- Reset the DED
- Enter an active key
- Enter active key and encrypt or decrypt under master key
- Encrypt or decrypt data
- Electronic codebook or cipher feedback operation

The master and active key registers are write-only registers. This prevents the key value from ever being discovered once it is entered into the device. Another unique feature is that a new active key, when entered into the DED,

can be encrypted or decrypted by the master key before it is stored into the active key register. This allows the user to send a new active key to the DED in encrypted or decrypted form for maximum security.

The 8-byte data buffer is used to handle all plain data and ciphered data sent to and read from the DED.

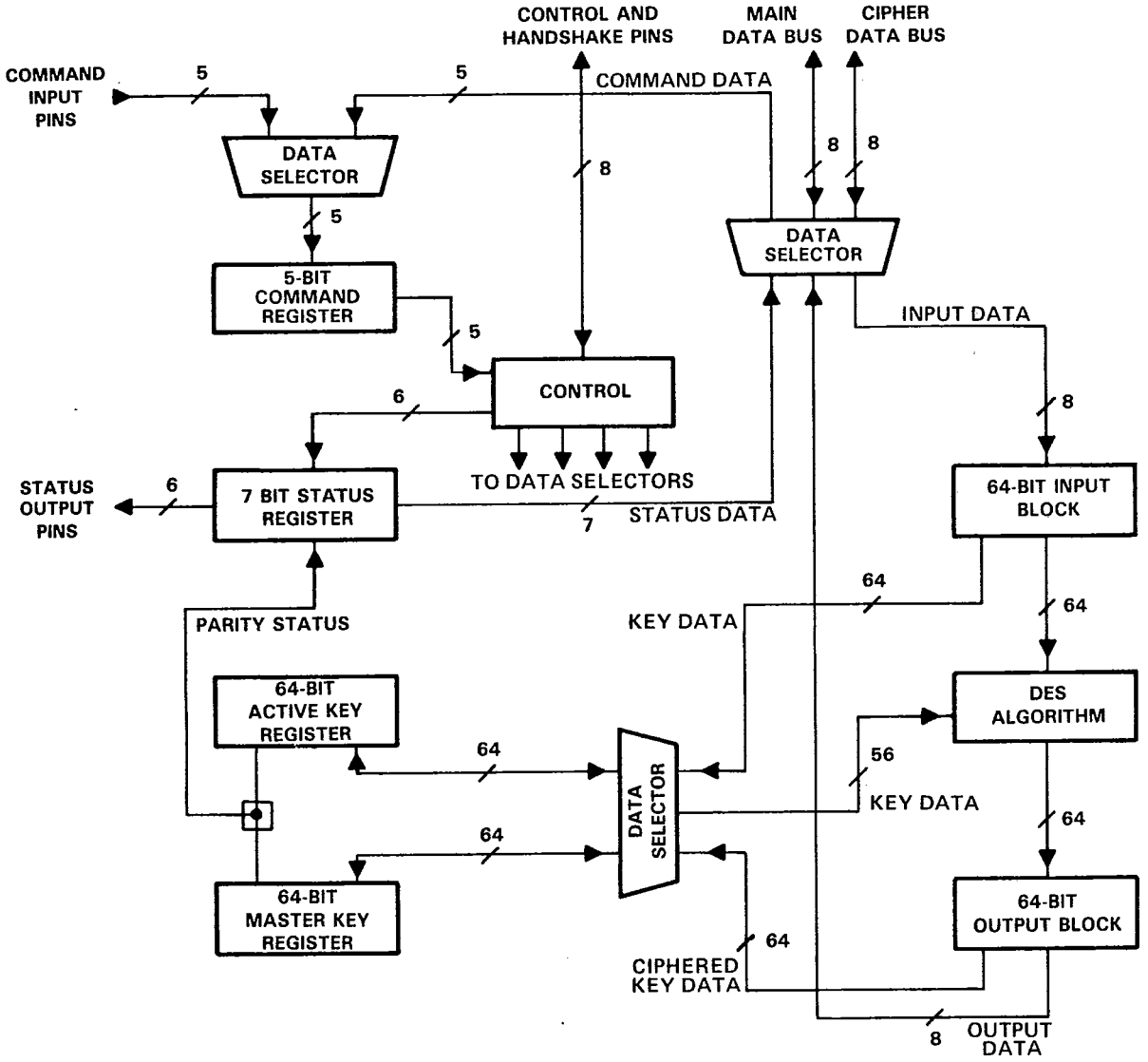

FIGURE 1 – TMS7500/TMS75C00 DED FUNCTIONAL BLOCK DIAGRAM

3. EXTERNAL COMMAND AND STATUS DATA

The TMS7500 has two separate internal registers for command and status data. All TMS7500 operations are controlled from the command register which is a write-only register. The command register can be loaded from five command input pins when the external command mode is enabled or from the main data bus.

Most of the status data can be accessed from external pins or from the main data bus. The status register contains the operational status of the TMS7500 at all times.

4. TMS7500 DATA ENCRYPTION DEVICE PIN-OUT

The TMS7500 pin-out is shown in Figure 2. The pins are arranged numerically, but the TMS7500 pins can also be grouped according to pin type and pin function. There are six groups and/or functions which are defined in the following paragraphs.

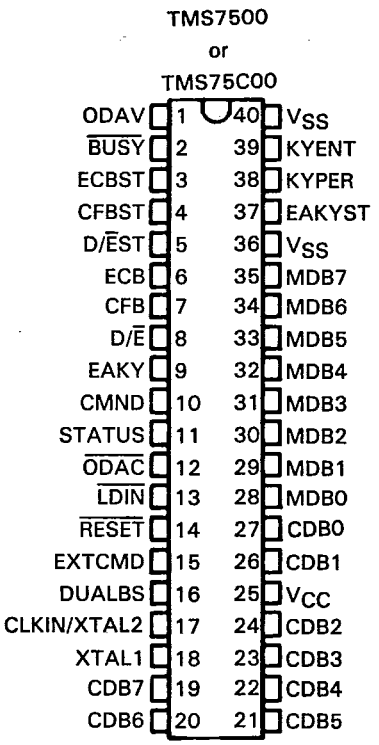

FIGURE 2 – TMS7500 DATA ENCRYPTION DEVICE PIN-OUT

HANDSHAKE PINS – these pins control I/O data flow from the TMS7500 chip to the host processor and vice versa. The handshake pins are shown in Table 1.

TABLE 1 – HANDSHAKE PINS

PIN NUMBER	PIN NAME	DESCRIPTION
1	ODAV	Output Data Available
2	$\overline{\text{BUSY}}$	Busy
12	$\overline{\text{ODAC}}$	Output Data Accepted
13	$\overline{\text{LDIN}}$	Load Data In

STATUS OUTPUT PINS – these pins will output the present status of the TMS7500 chip. The outputs will be the same state as the corresponding bit of the internal status register. The status output pins are shown in Table 2.

TABLE 2 – STATUS OUTPUT PINS

PIN NUMBER	PIN NAME	DESCRIPTION
3	ECBST	Electronic Codebook Status
4	CFBST	Cipher Feedback Status
5	D/$\overline{\text{E}}$ST	Decrypt/Encrypt Status
37	EAKYST	Enter Active Key Status
39	KYENT	Key Entered
38	KYPER	Key Parity Error

COMMAND INPUT PINS – these pins enable external loading at the command register. The command input pins increase system security and user convenience. The command input pins are shown in Table 3.

TABLE 3 – COMMAND INPUT PINS

PIN NUMBER	PIN NAME	DESCRIPTION
6	ECB	Electronic Codebook
7	CFB	Cipher Feedback
8	D/$\overline{E}$	Decrypt/Encrypt
9	EAKY	Enter Active Key
14	$\overline{RESET}$	Reset

MISCELLANEOUS PINS – each pin in this group has its own individual function which is needed to complete the TMS7500 configuration. For specific information on the miscellaneous pins see the TMS7500 AND TMS75C00 DATA ENCRYPTION DEVICE DATA MANUAL (SPNS004). The miscellaneous pins are shown in Table 4.

TABLE 4 – MISCELLANEOUS PINS

PIN NUMBER	PIN NAME	DESCRIPTION
10	CMND	Command Register Update
11	STATUS	Read Status
15	EXTCMD	External Command
16	DUALBS	Dual Data Bus
17	CLKIN/XTAL2	Crystal Input 2
18	XTAL1	Crystal Input 1
25	V_{CC}	Power Source
36	V_{SS}	Power Ground
40	V_{SS}	Power Ground

MAIN DATA BUS – most or all data is passed to or from the TMS7500 over the main data bus. The main data bus handles all uncoded data. The main data bus pins are shown in Table 5.

TABLE 5 – MAIN DATA BUS PINS

PIN NUMBER	PIN NAME	DESCRIPTION
28	MDB0	Main
29	MDB1	Data
30	MDB2	Bus
31	MDB3	0
32	MDB4	↓
33	MDB5	
34	MDB6	
35	MDB7	7

CIPHER DATA BUS – the optional cipher data bus is used for bi-directional encrypted data in place of the main data bus. Encrypted data transfers on this bus and increases system security. The cipher data bus pins are shown in Table 6.

TABLE 6 – CIPHER DATA BUS PINS

PIN NUMBER	PIN NAME	DESCRIPTION
19	CDB7	Cipher
20	CDB6	Data
21	CDB5	Bus
22	CDB4	7
23	CDB3	↓
24	CDB2	
26	CDB1	↓
27	CDB0	0

5. DEVICE APPLICATIONS

5.1 TYPICAL SYSTEM CONFIGURATION

A typical system configuration is shown in the block diagram in Figure 3. The TMS9995 microprocessor interfaces to the TMS7500 through a TMS9901 PSI (Programmable Systems Interface) to the main data bus. Since the TMS7500 handles the data encryption and decryption process, demands on the microprocessor's time are greatly reduced, including the time required to write the encryption and decryption software.

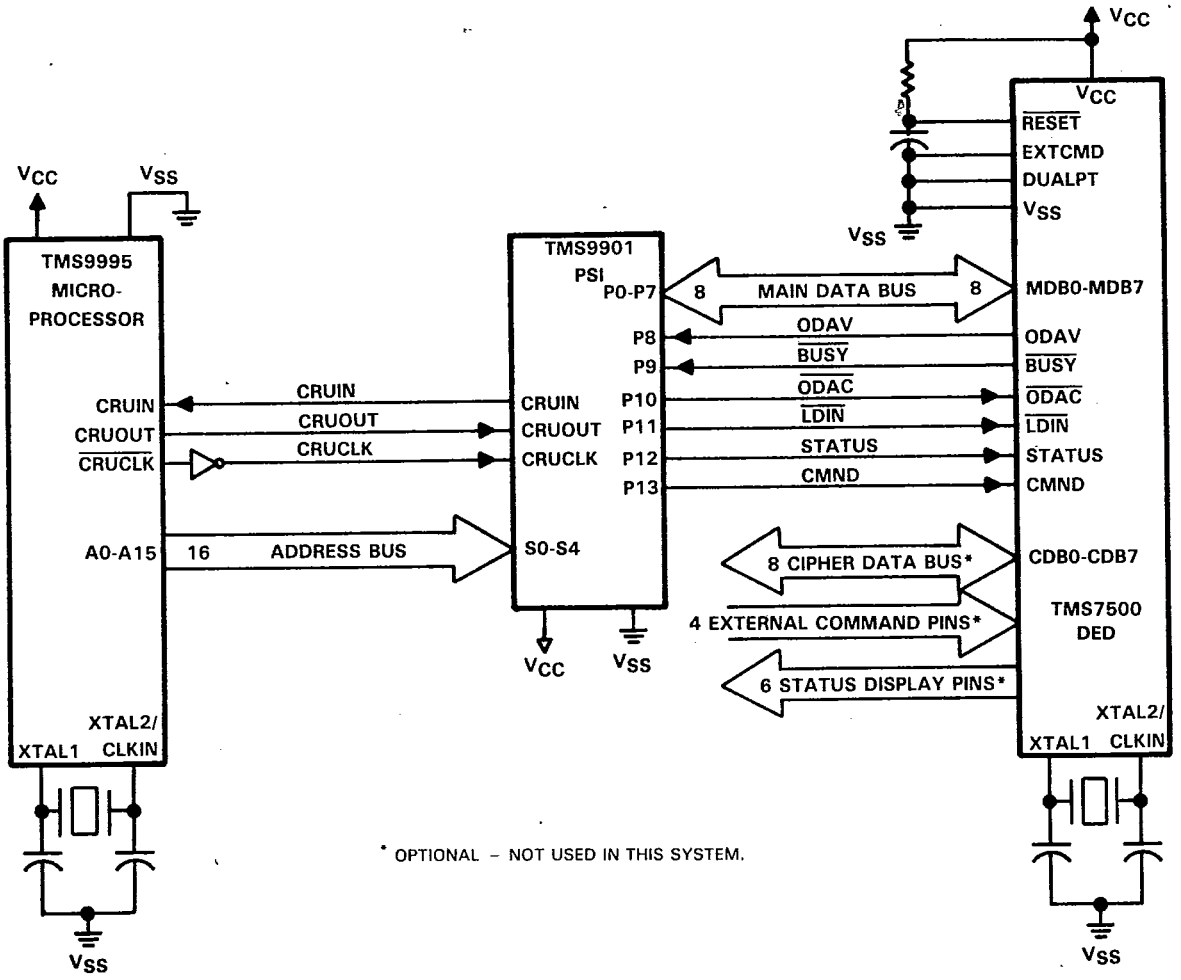

FIGURE 3 – TYPICAL SYSTEM CONFIGURATION

5.2 FULL I/O USAGE

All or part of the TMS7500 I/O capability may be utilized depending upon system requirements and user demands. An example using all the TMS7500 I/O options is shown in Figure 4. This configuration exhibits two data buses in use.

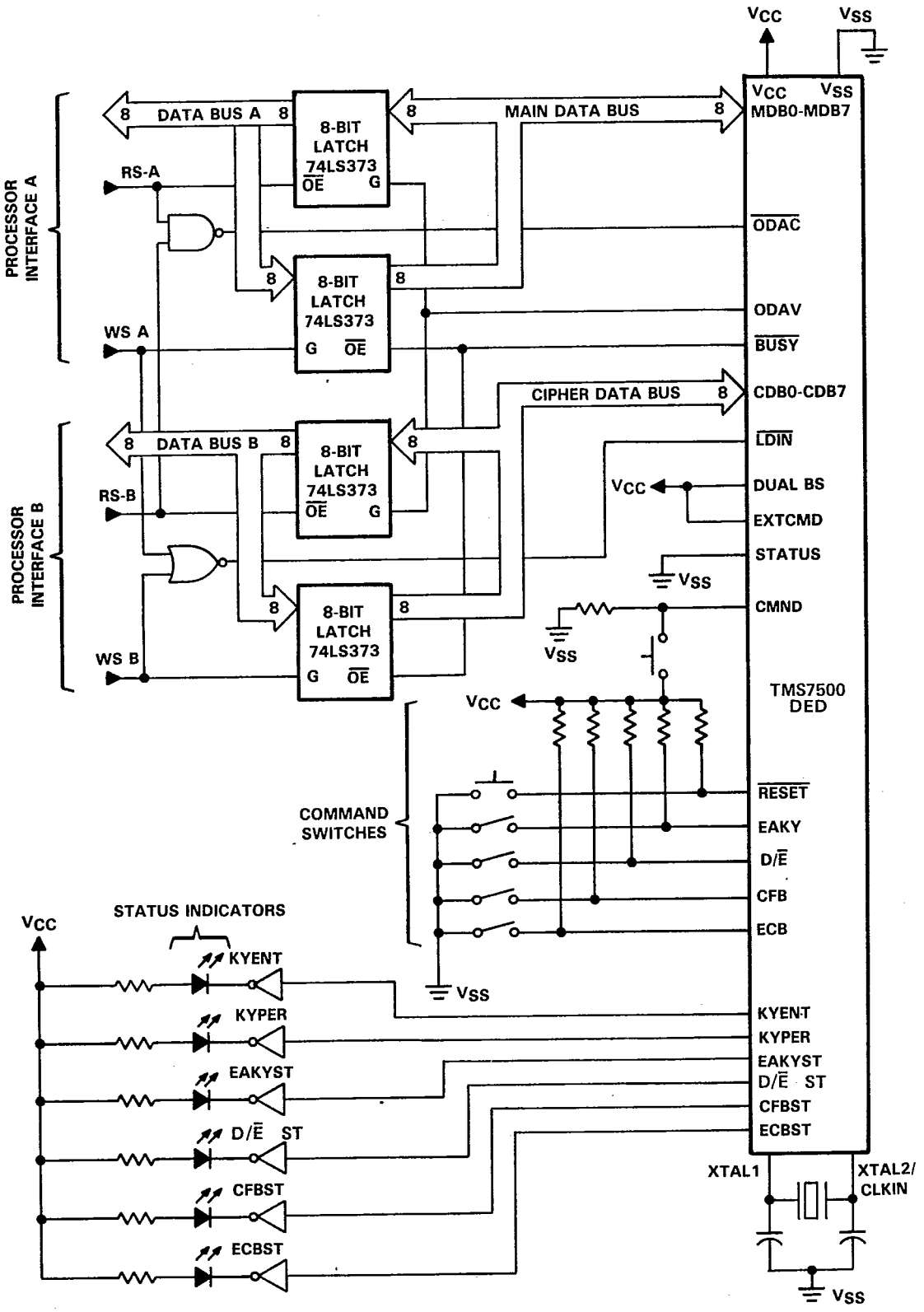

FIGURE 4 – EXAMPLE OF TMS7500 FULL I/O USAGE

The main data bus is used for clear data, master key, active key, and the initialization vector (IV) for the CFB mode. The cipher data bus is used for ciphered data if the DUALBS pin is connected to V_{CC}.

The main data bus and the cipher data bus can be hooked to two separate processors in a multiprocessor application. They may also be memory mapped in separate locations of a single host microprocessor for additional system security.

6. CONCLUSION

The TMS7500 and TMS75C00 Data Encryption Devices will protect private information of transmitted data without sacrificing system performance. These DEDs by Texas Instruments are low-cost chips which have many features that are found in higher-priced data encryption devices. They are ideally suited for low-cost, medium speed telecommunications equipment.