

[54] CRYPTOGRAPHIC COMMUNICATION
SECURITY FOR SINGLE DOMAIN
NETWORKS

[75] Inventors: William F. Ehrsam, Kingston; Robert C. Elander, Saugerties; Stephen M. Matyas, Poughkeepsie; Carl H. W. Meyer, Kingston; Robert L. Powers, West Hurley; Paul N. Prentice, Hyde Park; John L. Smith; Walter L. Tuchman, both of Woodstock, all of N.Y.

[73] Assignee: International Business Machines Corporation, Armonk, N.Y.

[21] Appl. No.: 857,532

[22] Filed: Dec. 5, 1977

[51] Int. Cl.³ H04L 9/00

[52] U.S. Cl. 375/2; 340/149 R;
364/200

[58] Field of Search 340/149 A, 149 R, 150 R;
178/22; 375/2

[56] References Cited

U.S. PATENT DOCUMENTS

3,938,091	2/1976	Atalla et al.	340/152 R
3,956,615	5/1976	Anderson et al.	340/152 R
3,958,081	5/1976	Ehrsam et al.	178/22
3,985,998	10/1976	Crafton	340/149 A
4,004,089	1/1977	Richard et al.	340/149 A
4,025,760	5/1977	Trenkamp	340/149 A
4,120,030	10/1978	Johnstone	178/22

OTHER PUBLICATIONS

"Instructions for Cryptography Feature for Data Security", IBM Technical Disclosure Bulletin, vol. 19, No. 7, Dec. 1976, pp. 2644-2645, Author: Guyette.

"Conference Record, 11th Asilomar Conference on Circuits, Systems and Computers", Nov. 1977, IEEE

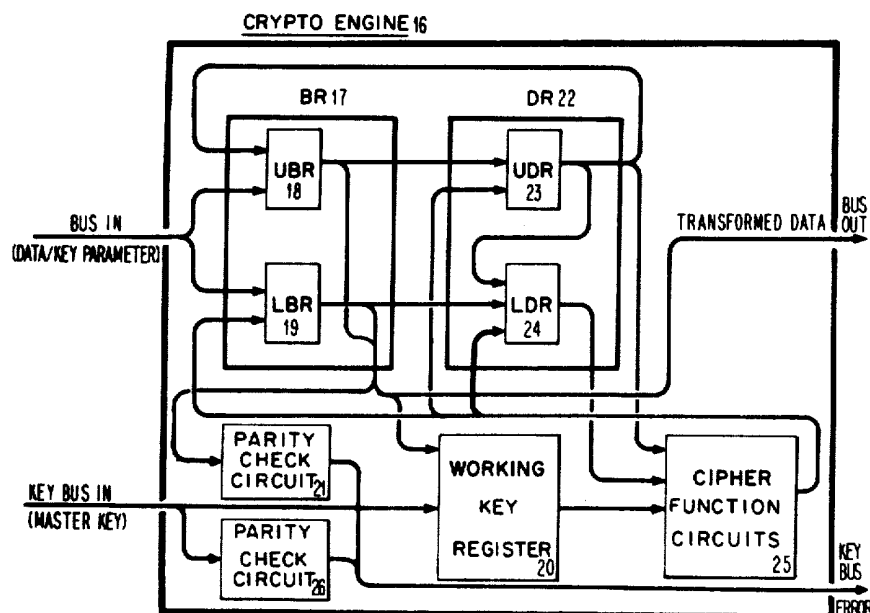
Computer Society, *Cryptographic Protection of Information in Communication Networks*, Hellman, pp. 204-207.

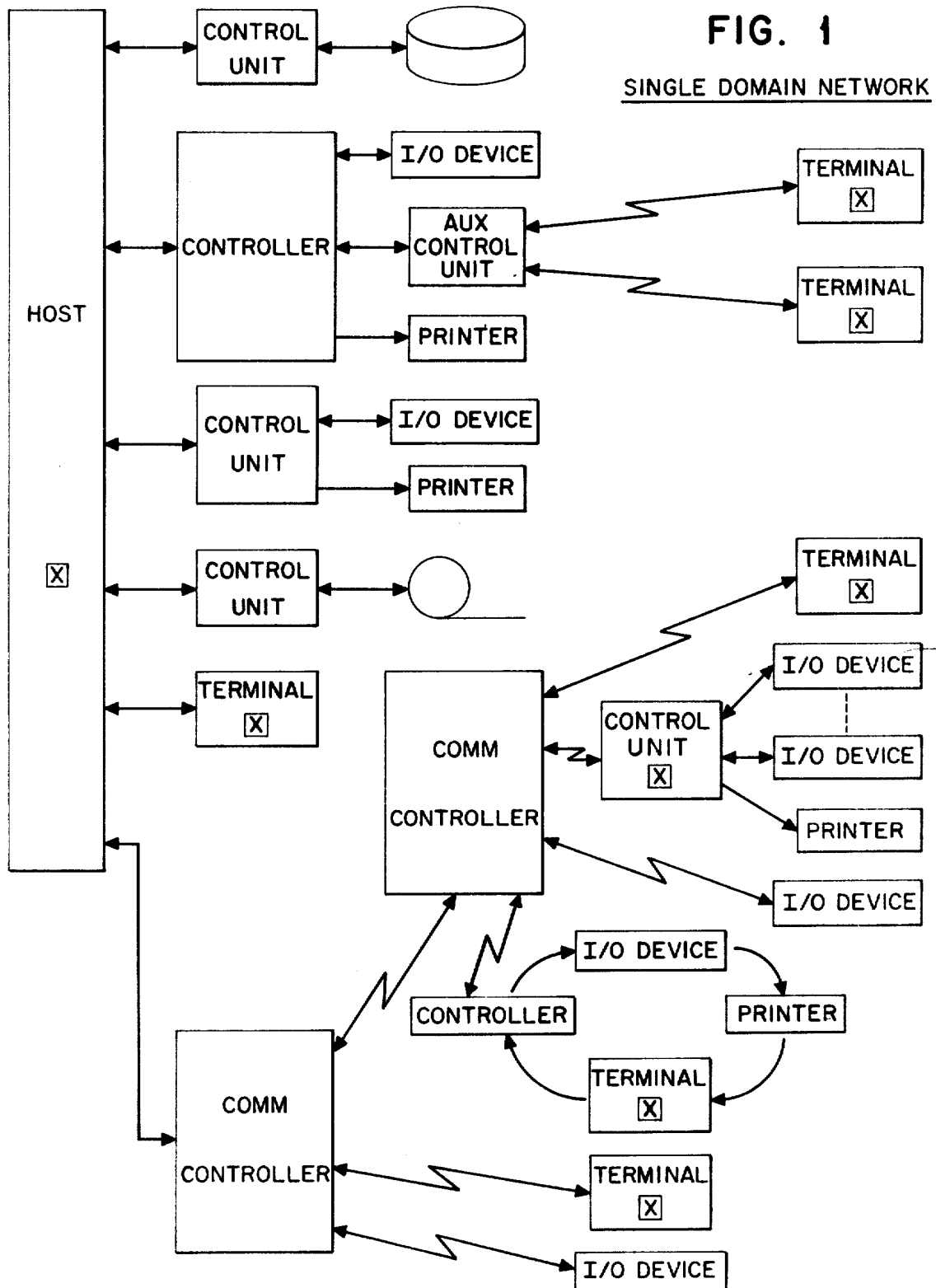
Primary Examiner—Howard A. Birmiel
Attorney, Agent, or Firm—Edwin Lester

[57] ABSTRACT

A communication security system for data transmissions between remote terminals and a host system. The remote terminals and the host system include data security devices capable of performing a variety of cryptographic operations. At initialization time, a host master key is written into the host data security device and the host system generates a series of terminal master keys for the remote terminals. Protection is provided for the terminal master keys by enciphering them under a variant of the host master key. The terminal master keys are then written into the data security devices of the respective remote terminals to permit cryptographic operations to be performed. When a communication session is to be established between a designated remote terminal and the host system, a random number is generated and defined as an operational key enciphered under the host master key which permits the operational key to be used at the host system for enciphering or deciphering data operations. The host data security device, using the enciphered master key of the designated remote terminal, transforms the enciphered operational key under control of the host master key into a form in which the operational key is enciphered under the terminal master key of the designated remote terminal. The operational key enciphered under the terminal master key of the designated remote terminal is transmitted to the remote terminal to permit the enciphered operational key to be used at the remote terminal for enciphering or deciphering data operations.

49 Claims, 83 Drawing Figures





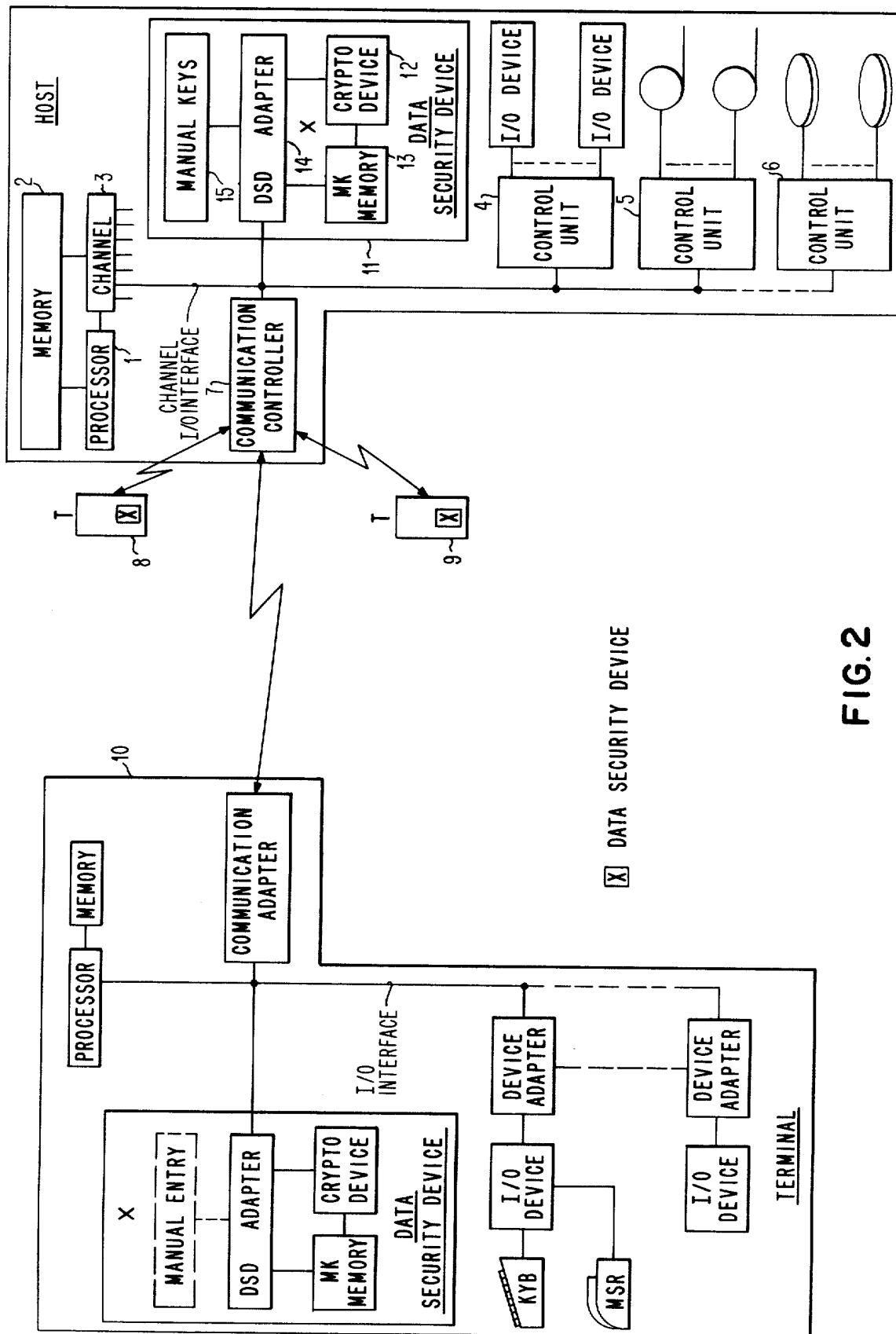


FIG. 2

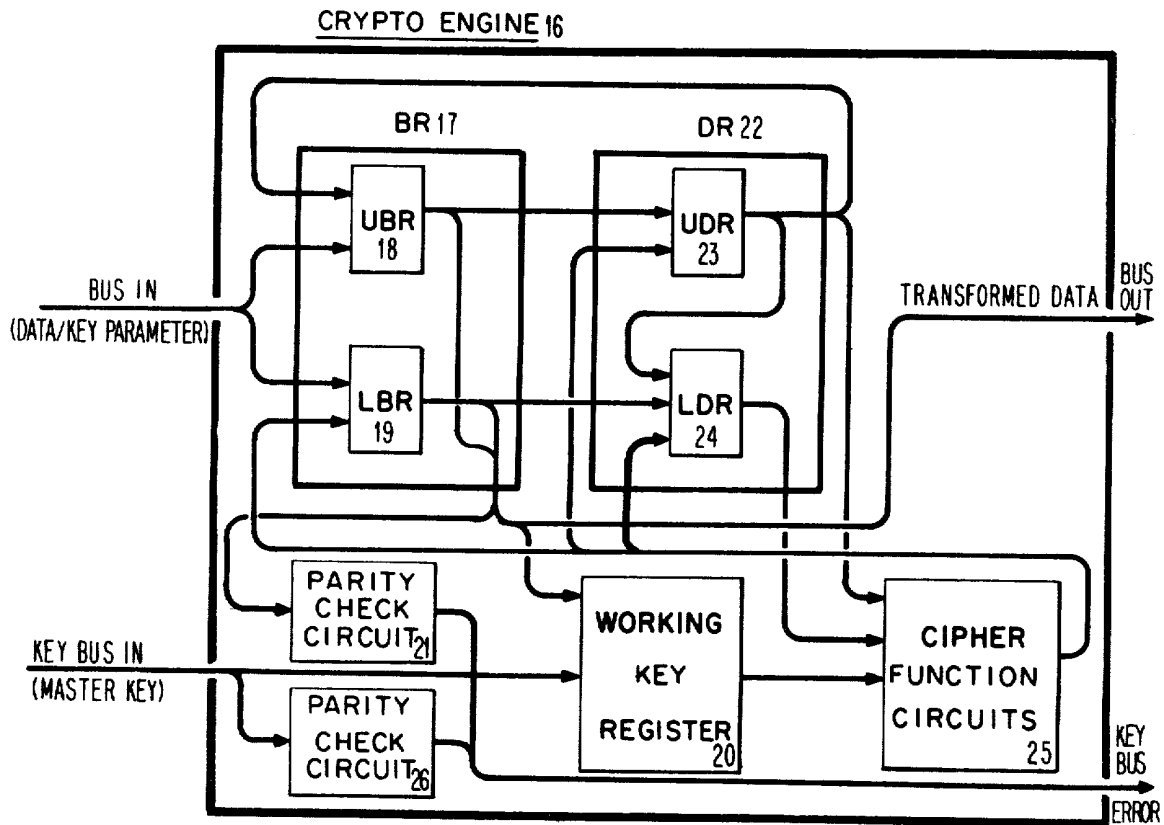


FIG. 3

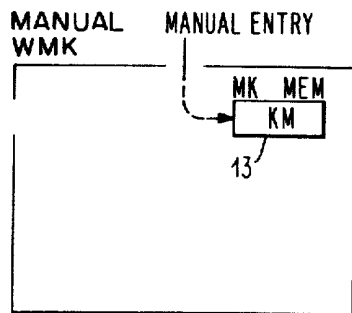


FIG. 4

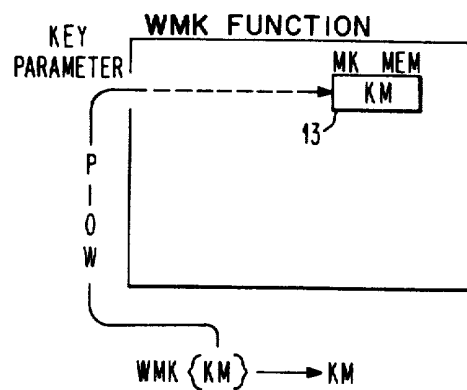
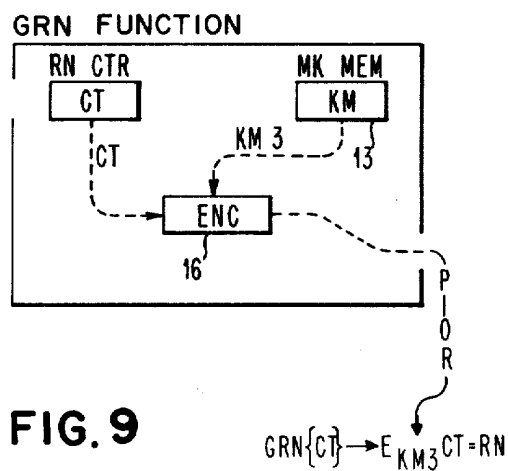
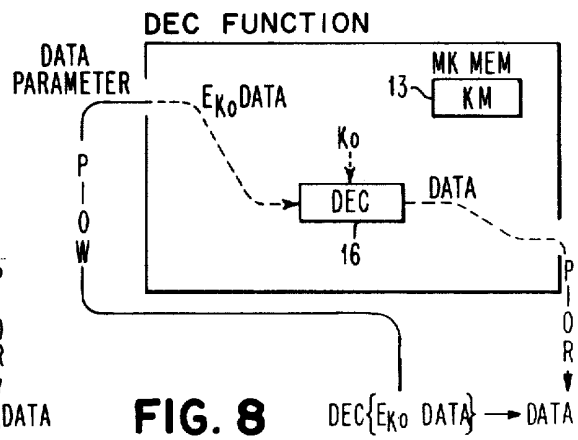
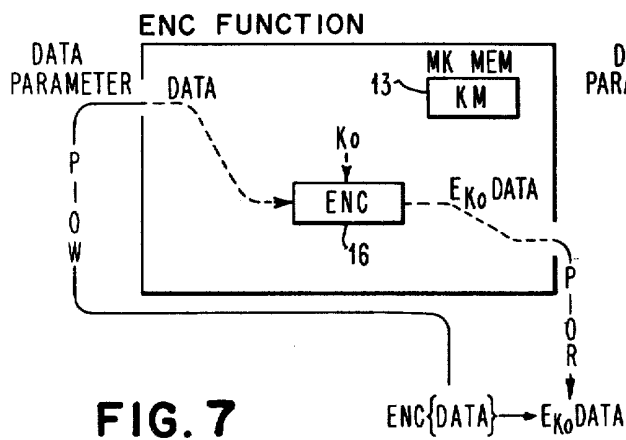
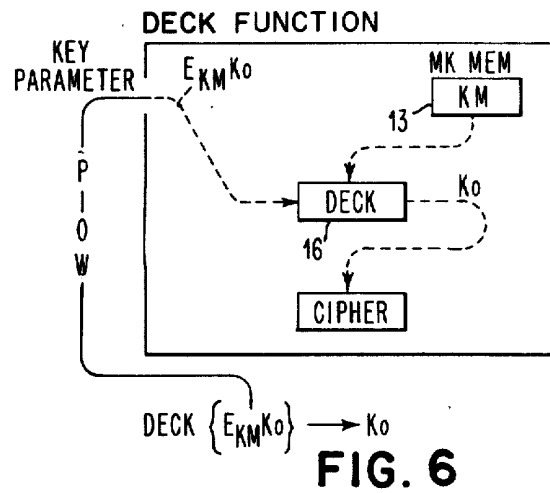


FIG. 5



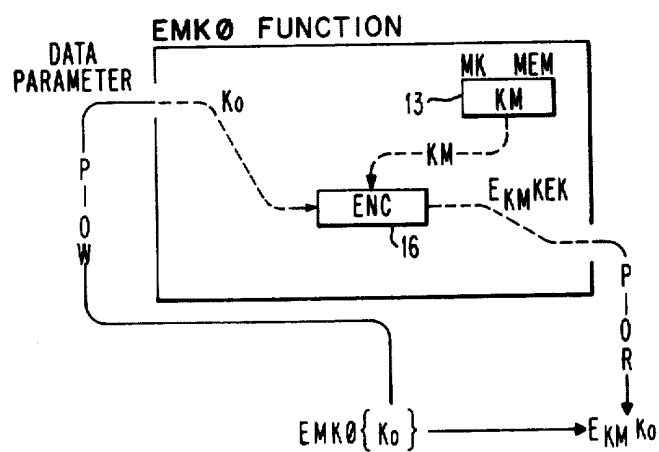


FIG. 10

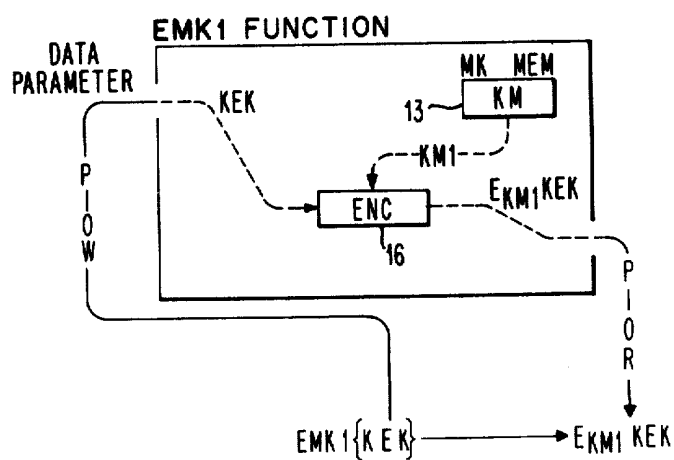


FIG. 11

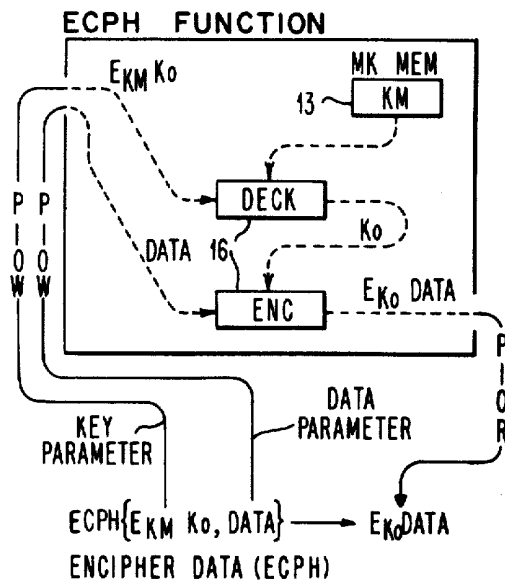


FIG. 12

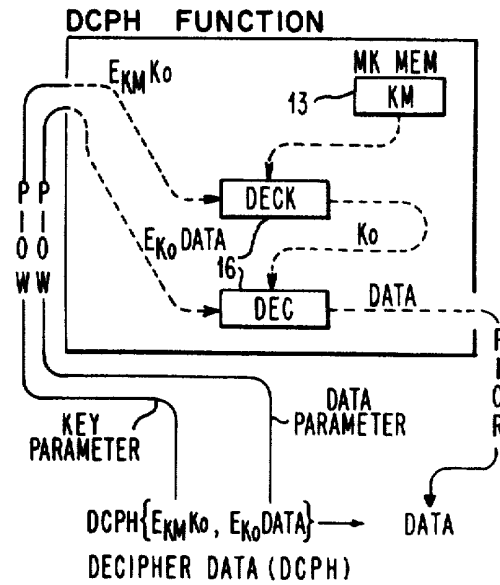


FIG. 13

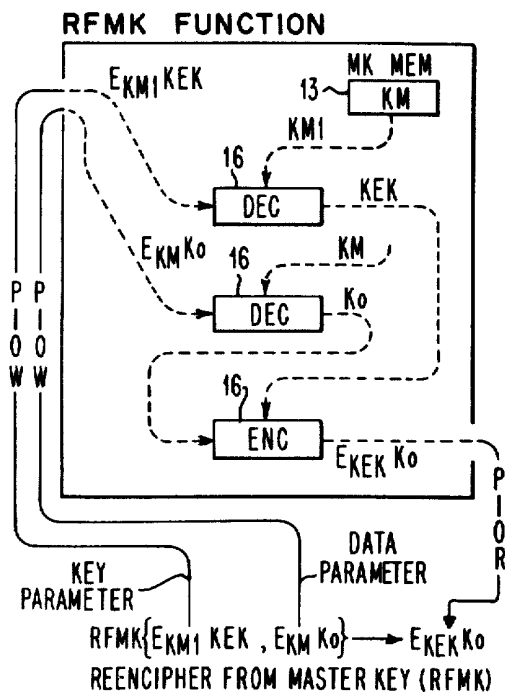


FIG. 14

SINGLE DOMAIN COMMUNICATION SECURITY

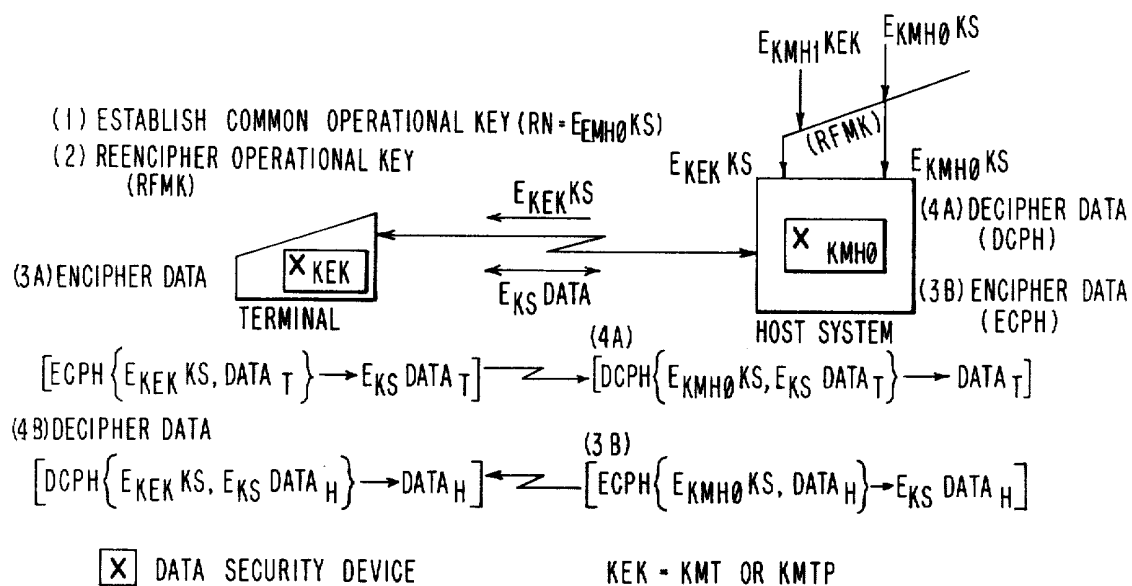


FIG. 15

SINGLE DOMAIN COMMUNICATION SECURITY—SYSTEM KEY

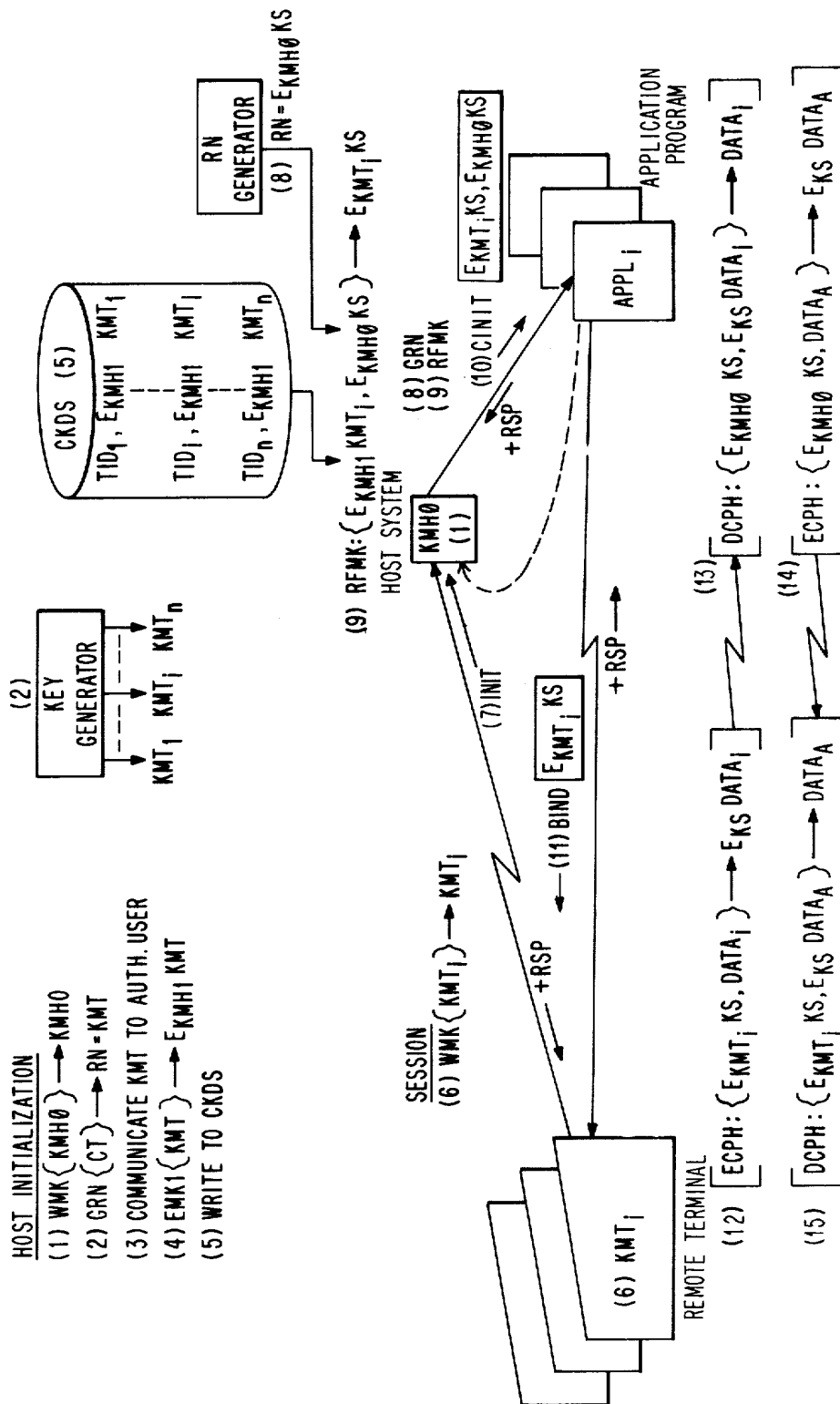


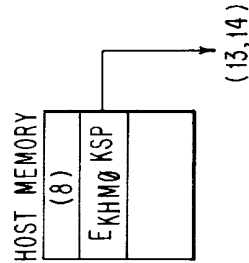
FIG. 16

SINGLE DOMAIN COMMUNICATION SECURITY - PRIVATE KEY

(PRIVATE PROTOCOL)

HOST INITIALIZATION

- (1) $WMK \{KMH0\} \rightarrow KMH0$
- (2) DEFINE KSP
- (3) LOAD KSP IN HOST
- (4) $EMK0 \{KSP\} \rightarrow EKMH0 KSP$
- (5) WRITE (2,4) TO OUTPUT DEVICE
- (6) STORE OUTPUT IN SECURE MANNER TILL SESSION REQ.



SESSION

TERMINAL

- (7) $LKD \{KSP\} \rightarrow K0 = KSP$

HOST

- (8) LOAD $EKMH0 KSP$

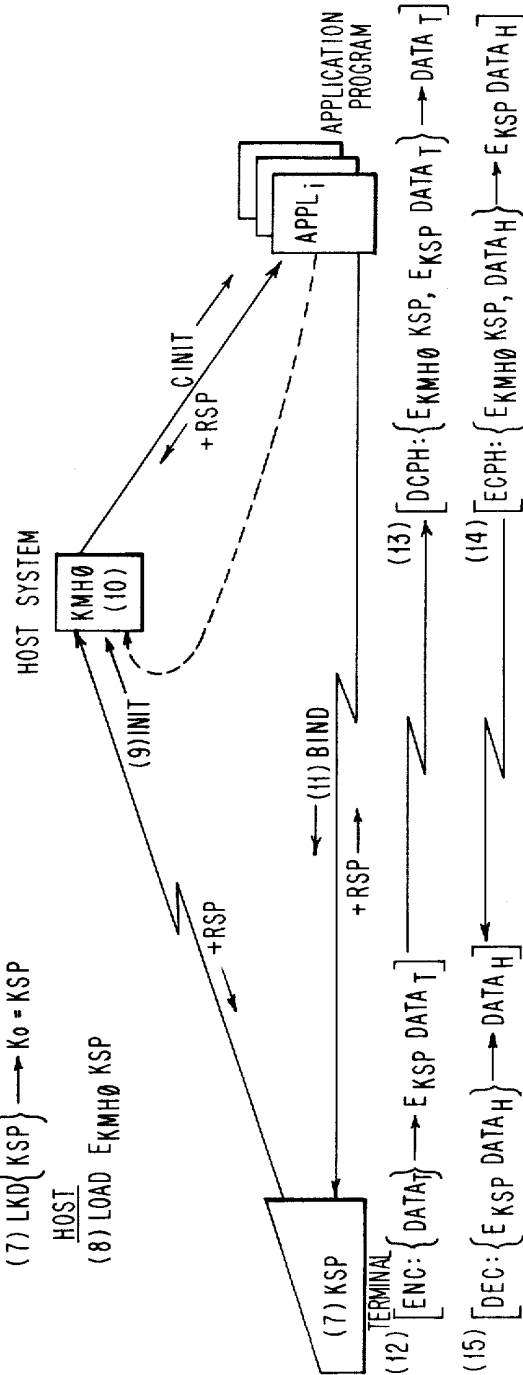


FIG. 19

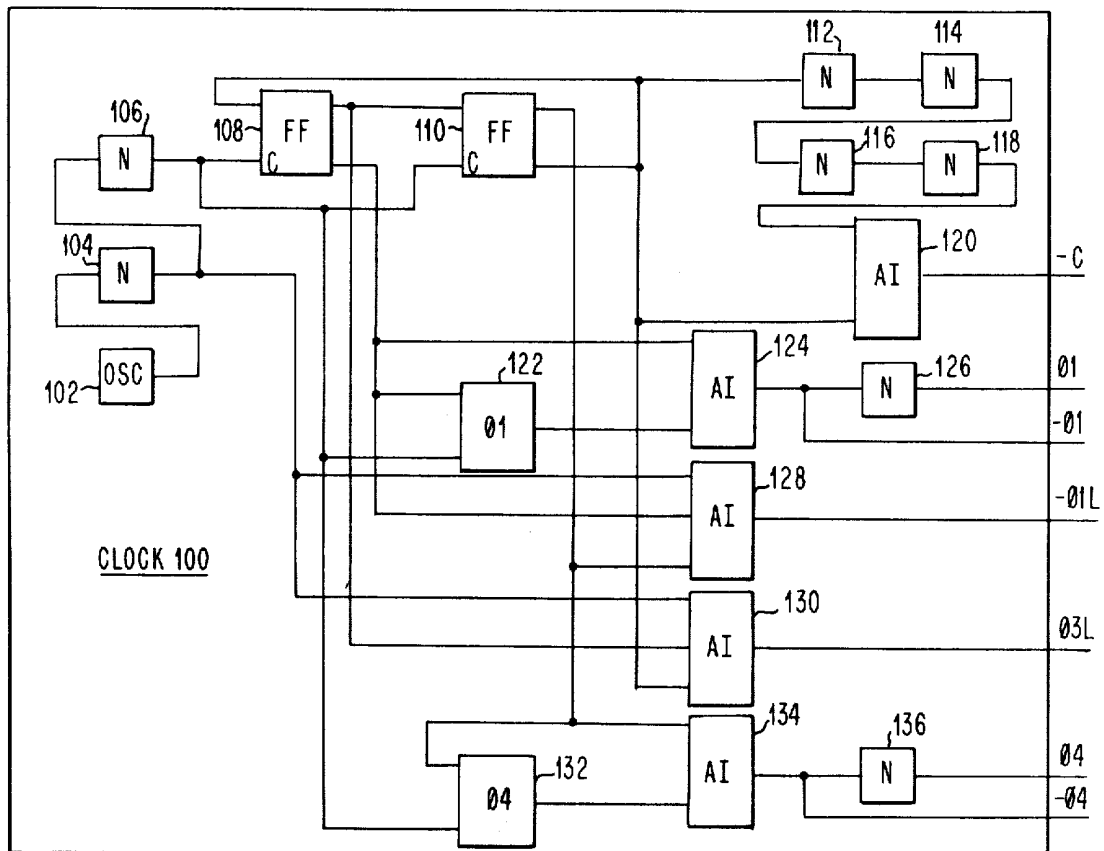


FIG. 20

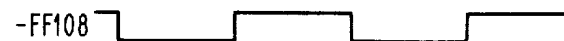
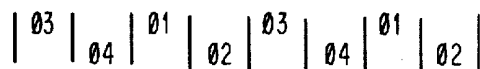
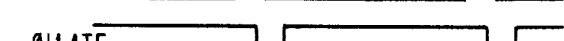


FIG. 21



CLOCK 100

FIG. 22

		Fig.22c1	Fig.22d1	Fig.22e1	Fig.22f1	Fig.22g1	Fig.22h1	
Fig.22a1	Fig.22b1	Fig.22c2	Fig.22d2	Fig.22e2	Fig.22f2	Fig.22g2	Fig.22h2	
Fig.22a2	Fig.22b2	Fig.22c3	Fig.22d3	Fig.22e3	Fig.22f3	Fig.22g3	Fig.22h3	Fig.22i1
	Fig.22b2'	Fig.22c3'	Fig.22d4	Fig.22e4	Fig.22f4	Fig.22g4	Fig.22h4	Fig.22i2
	FIG.22b3	FIG.22c4	FIG.22d5	FIG.22e5				

FIG. 22a1

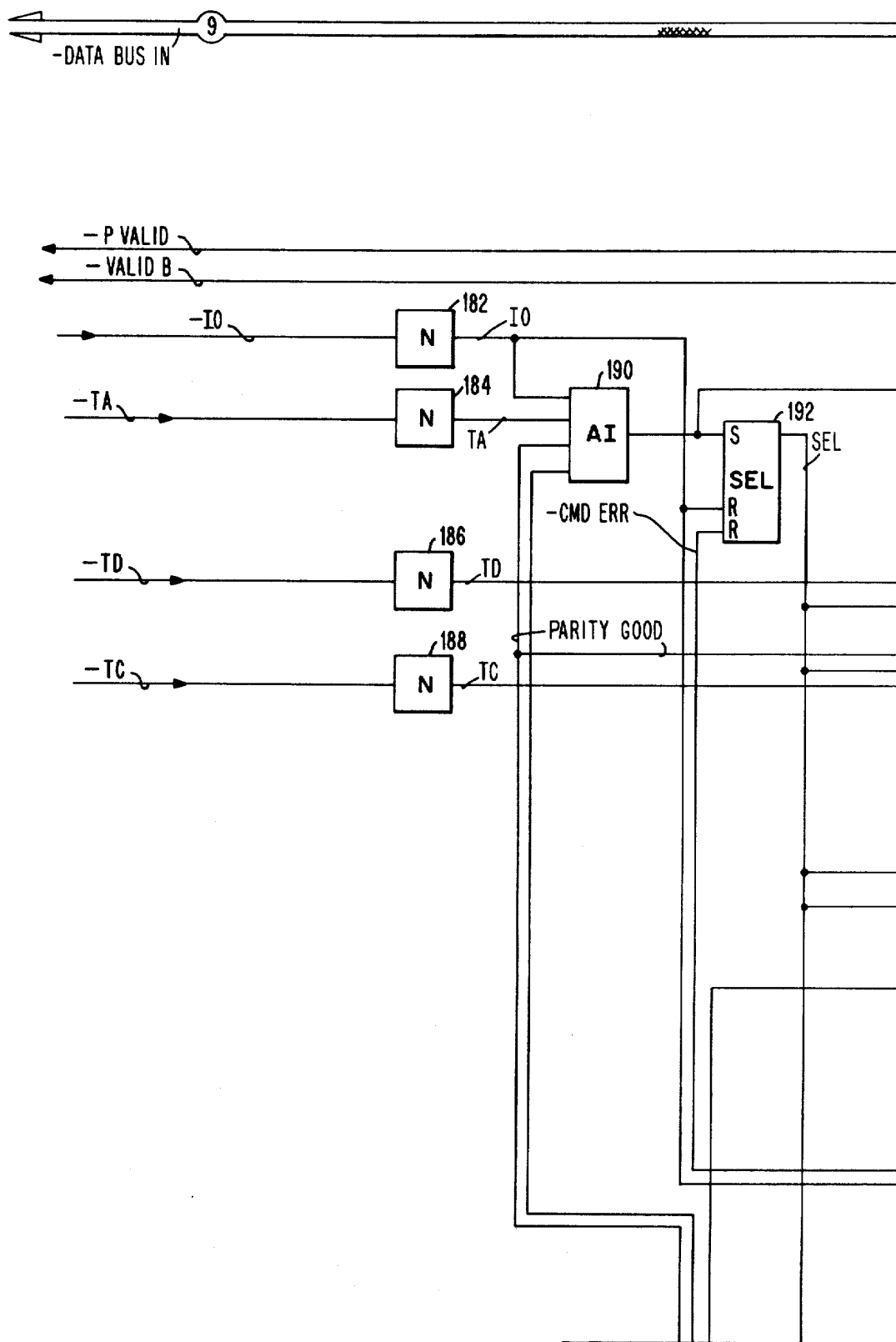


FIG. 22a2

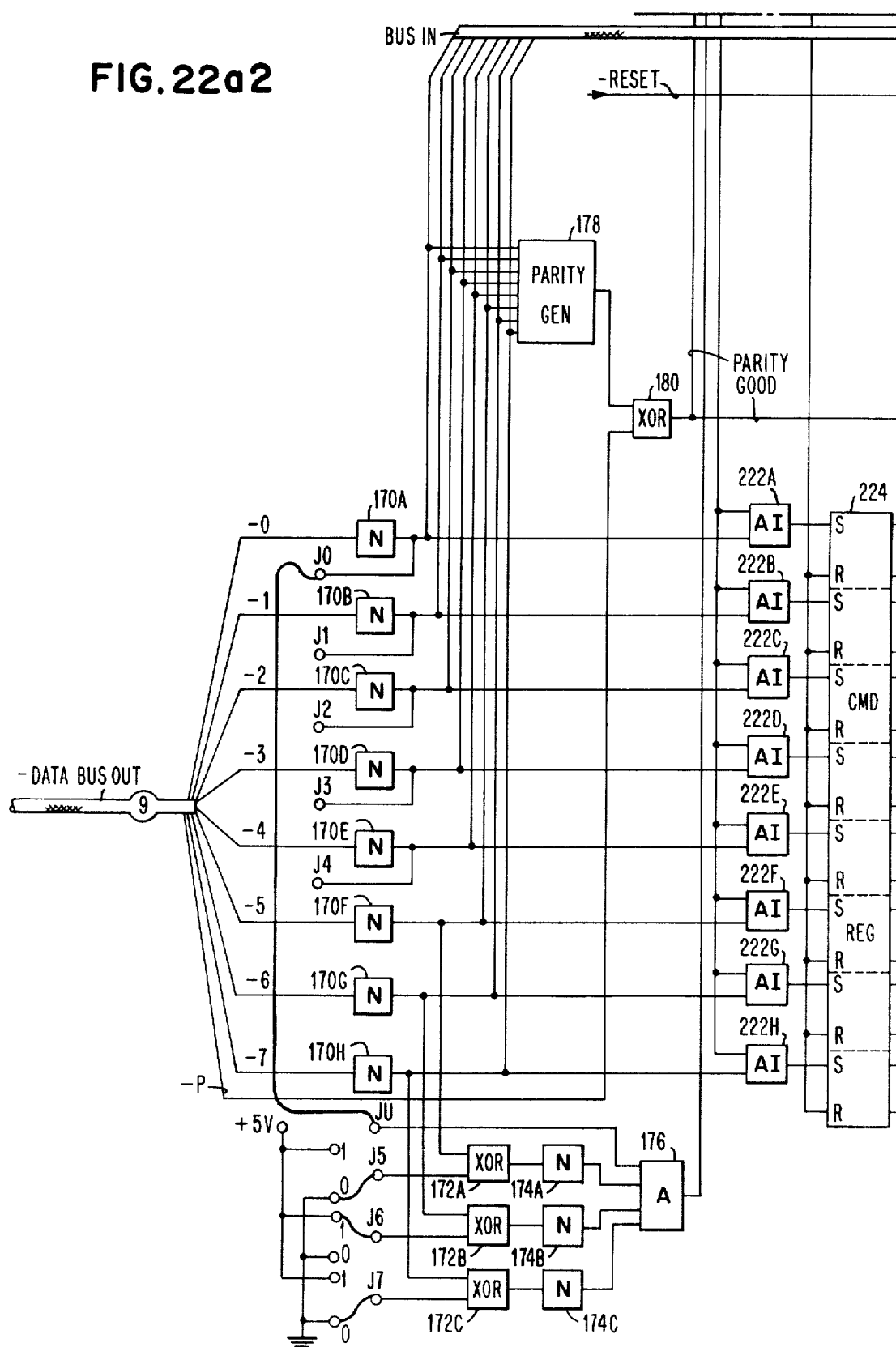
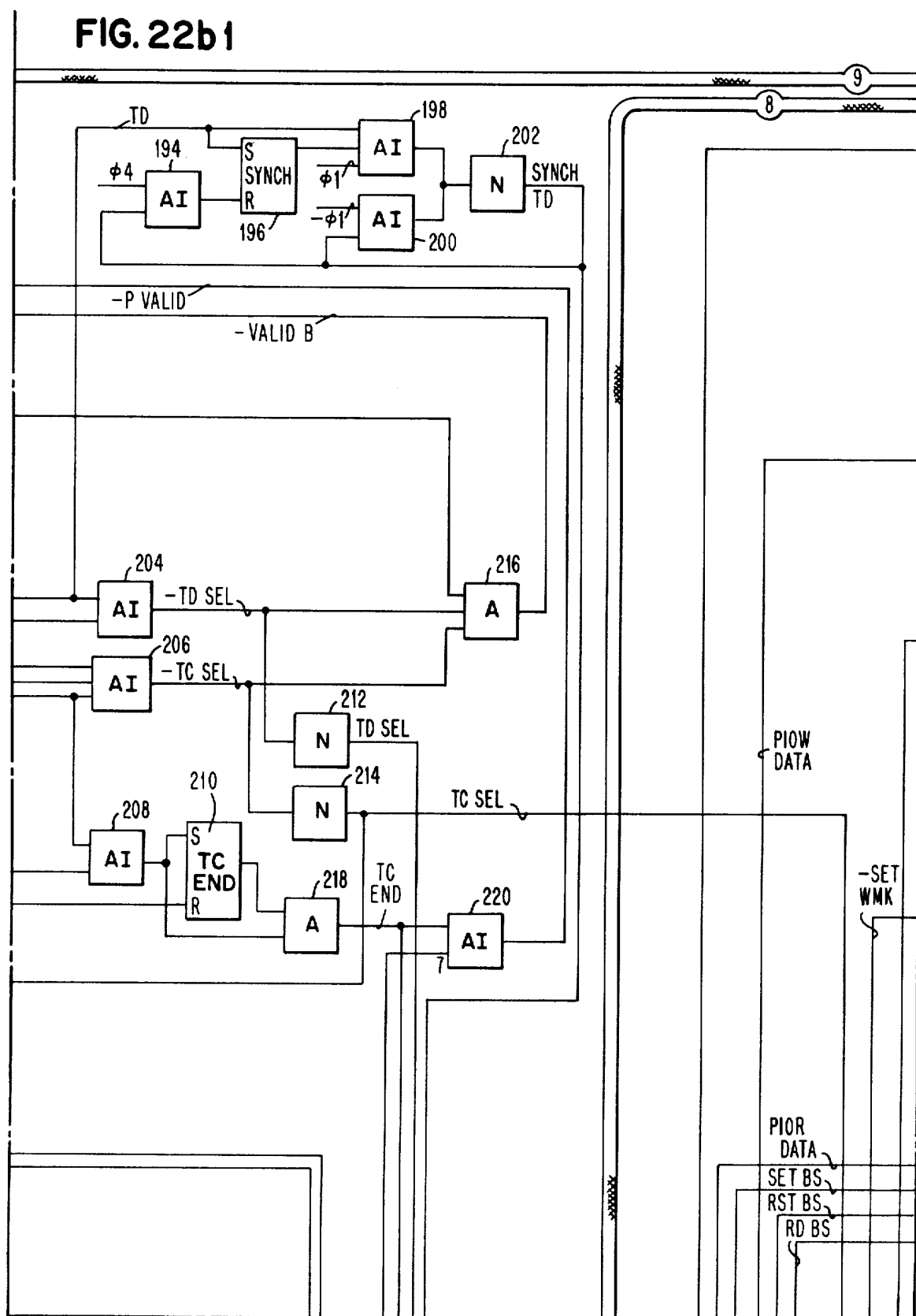
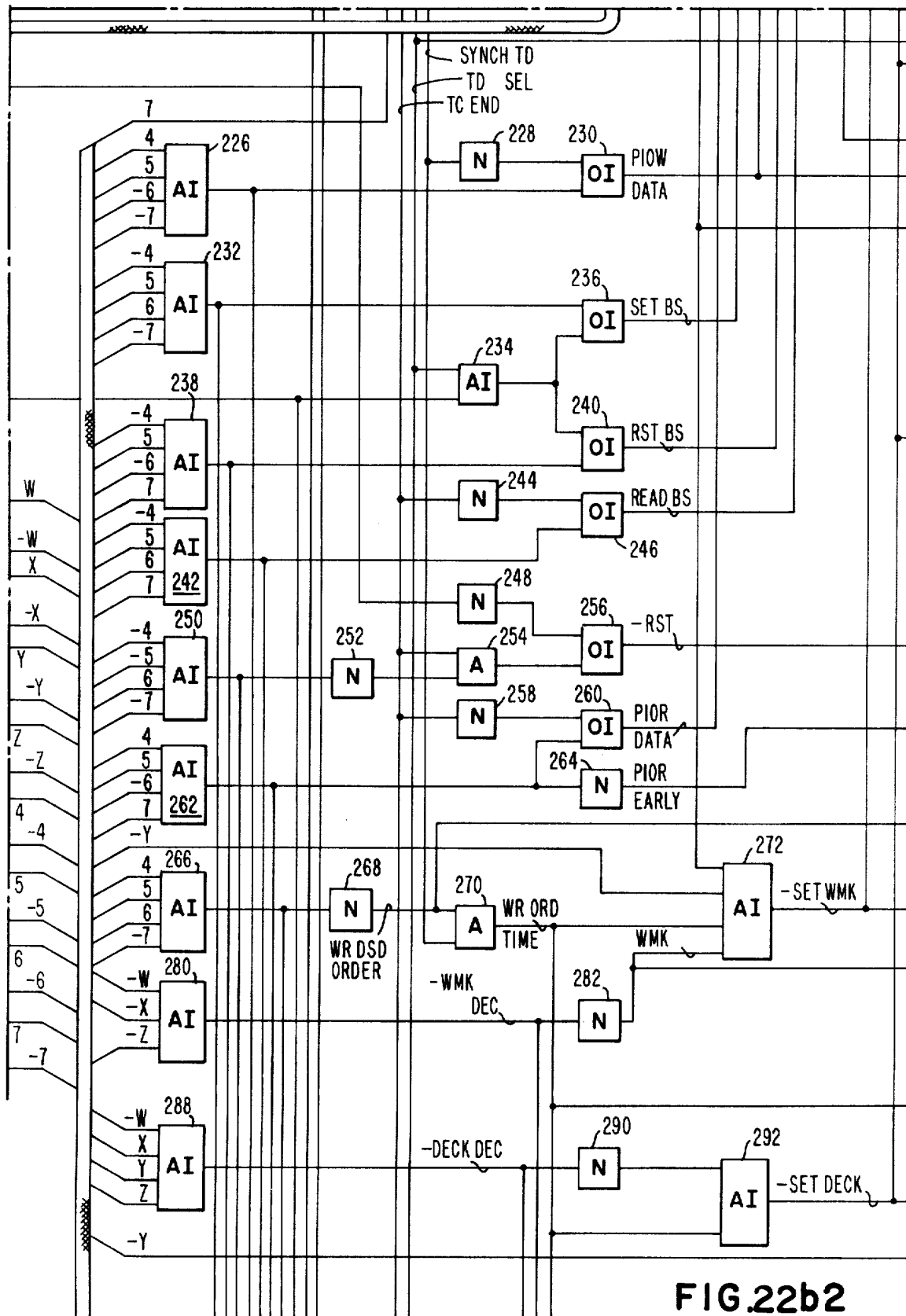
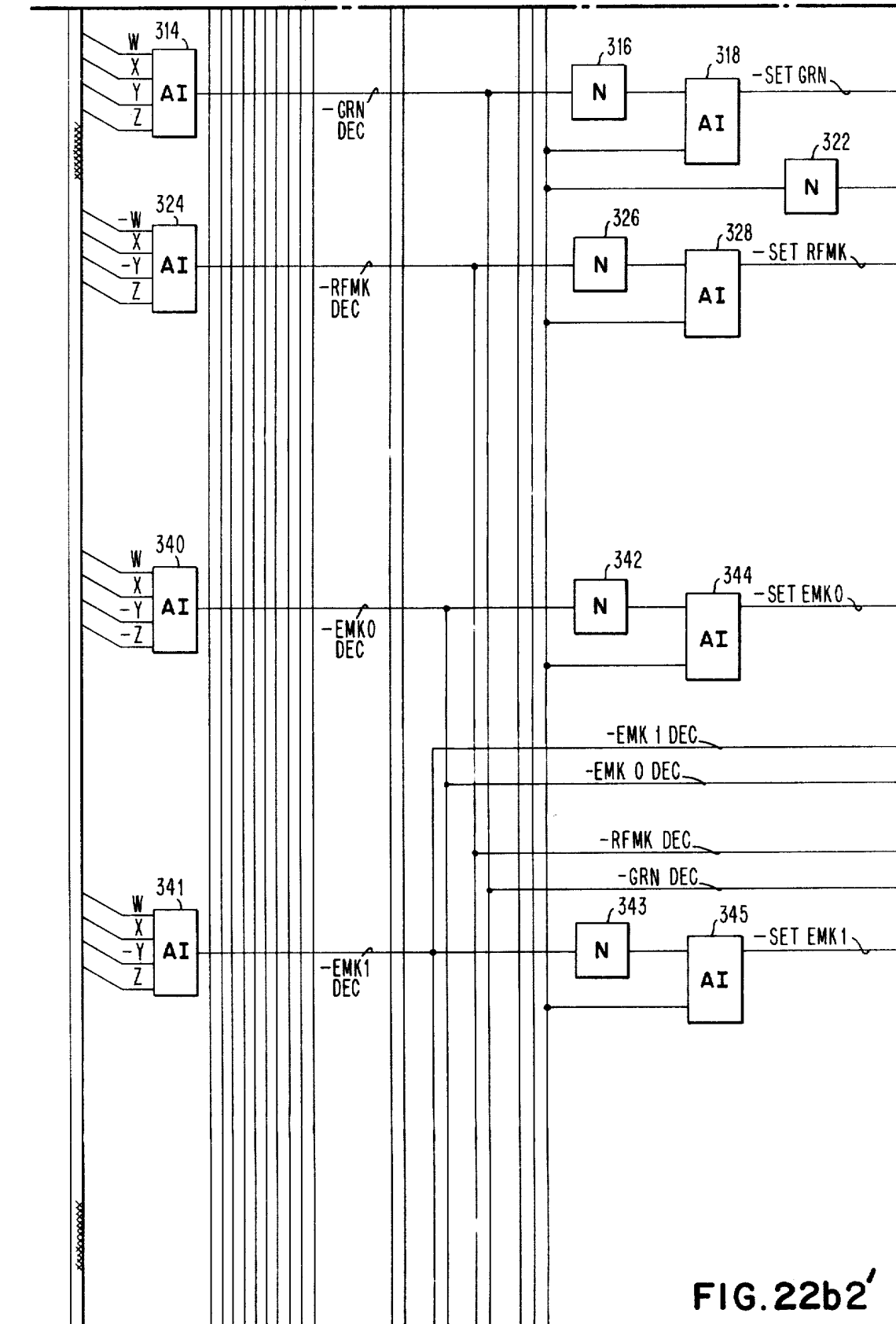


FIG. 22b1







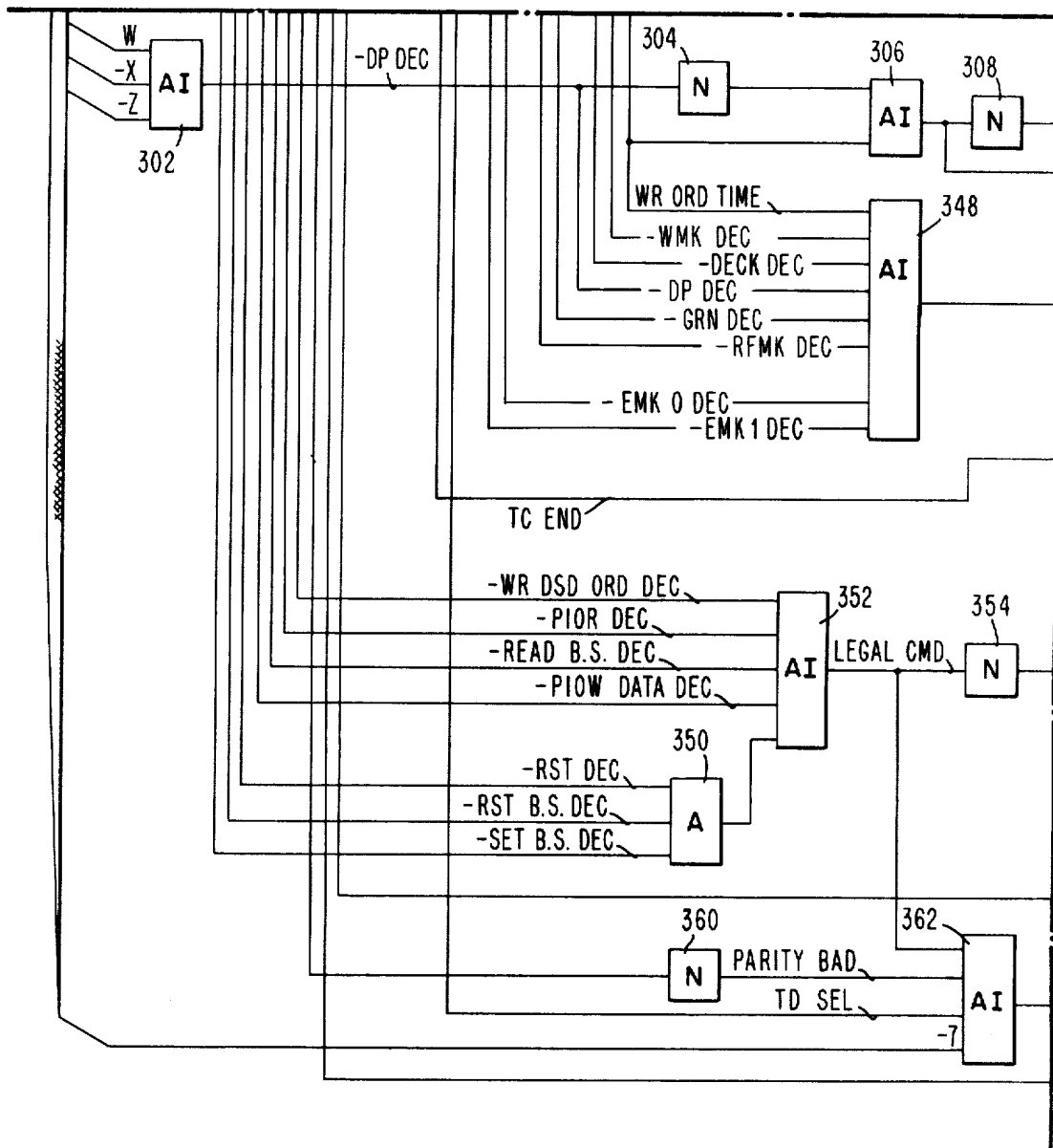
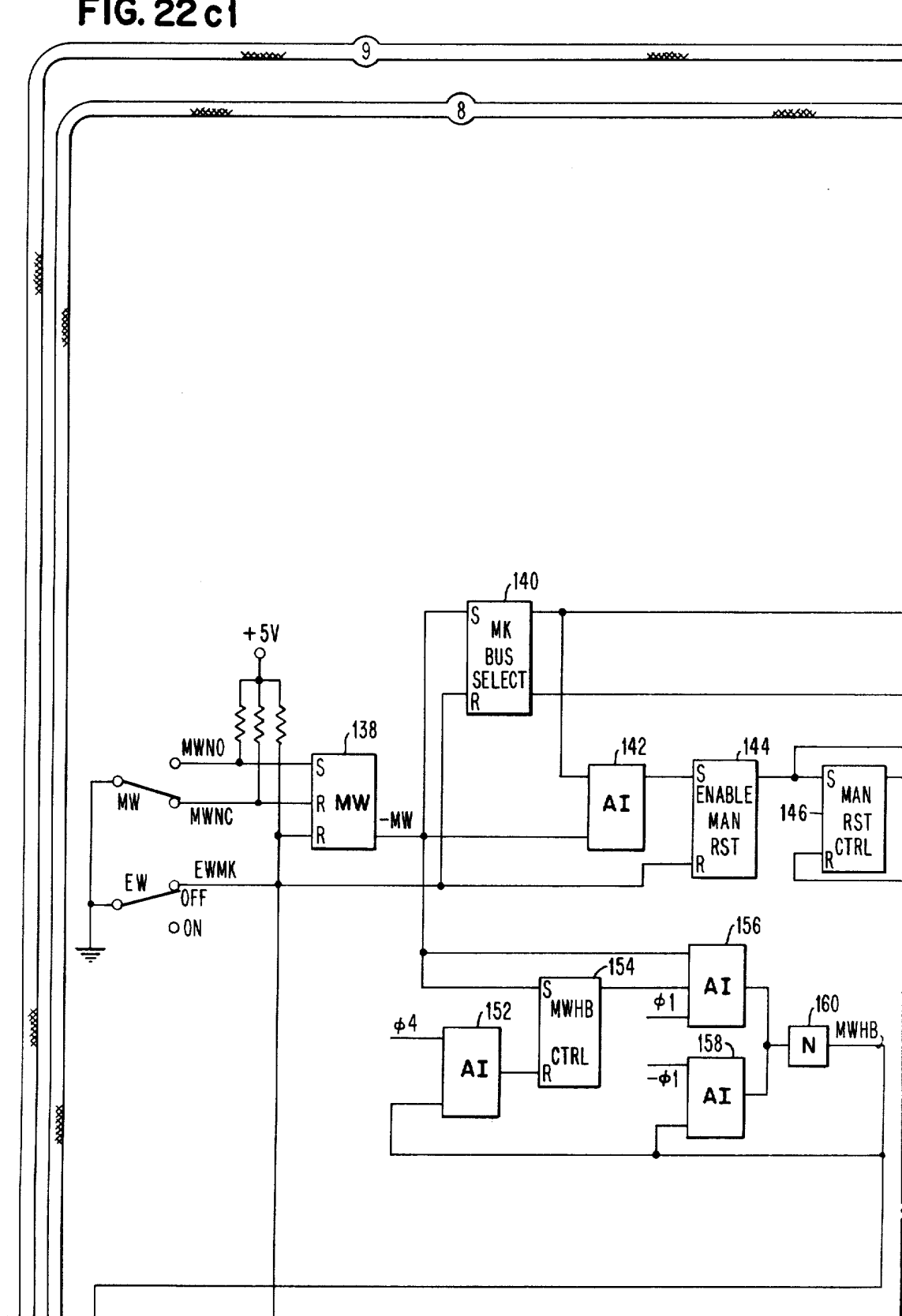
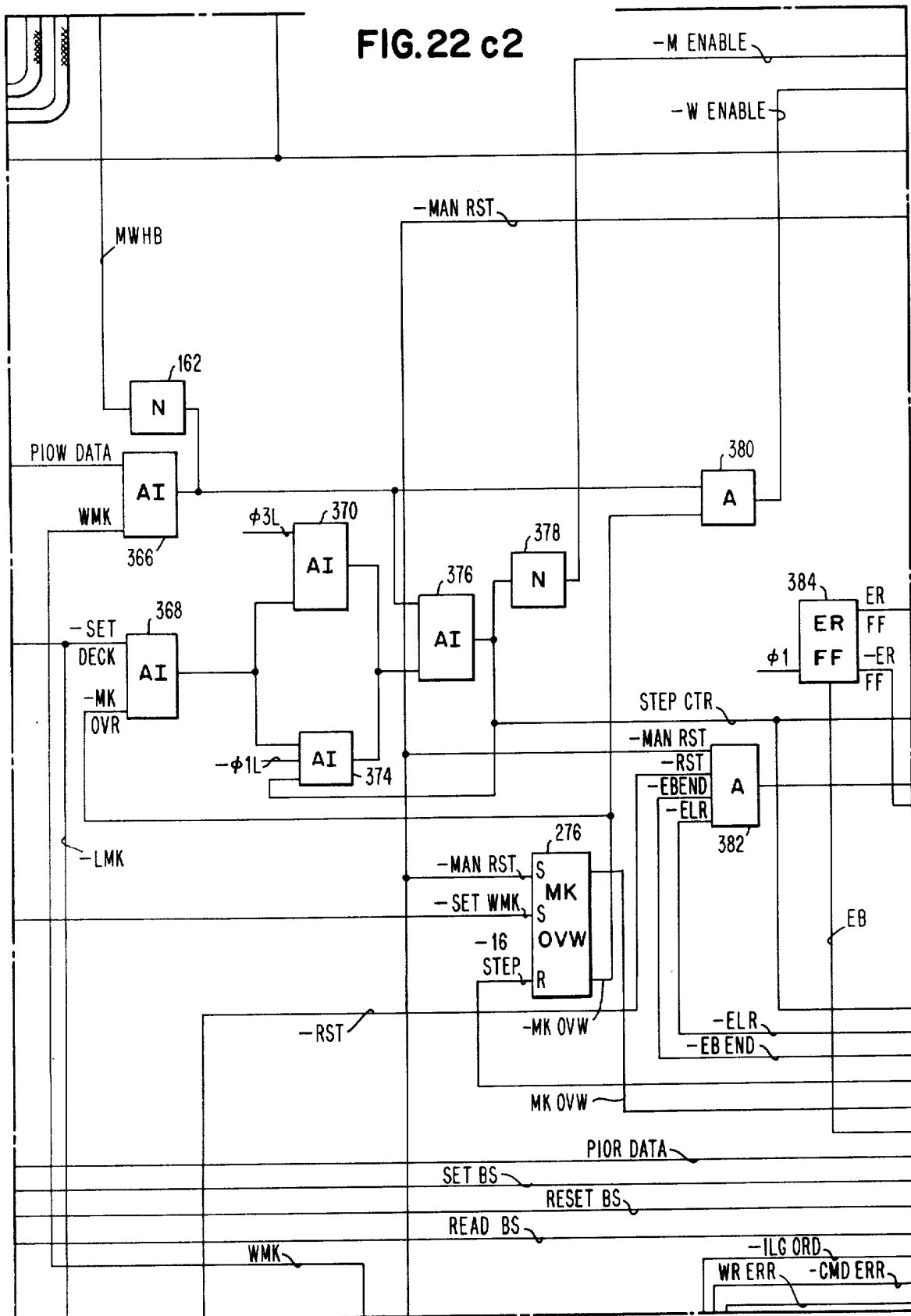


FIG.22 b3

FIG. 22c1





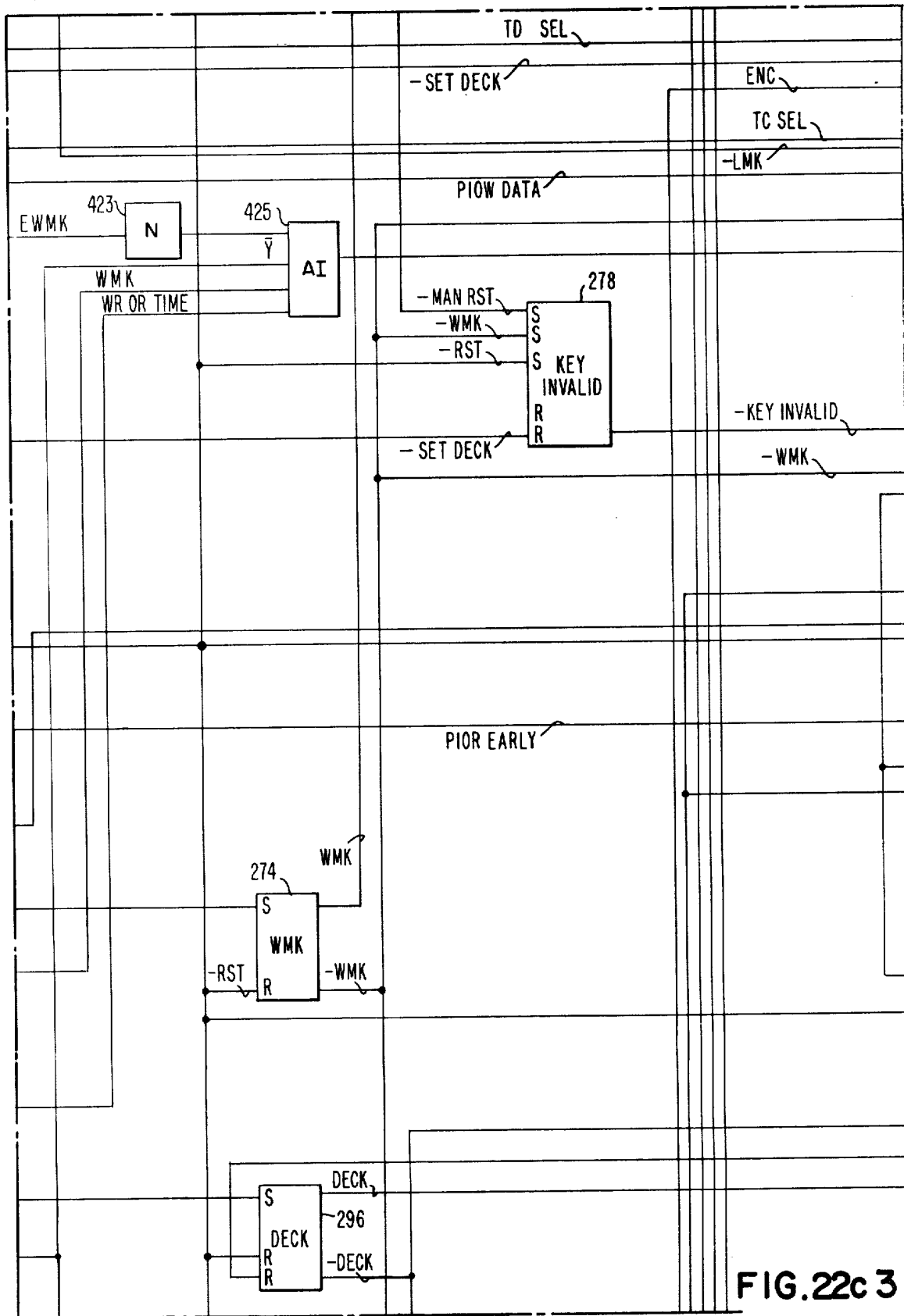
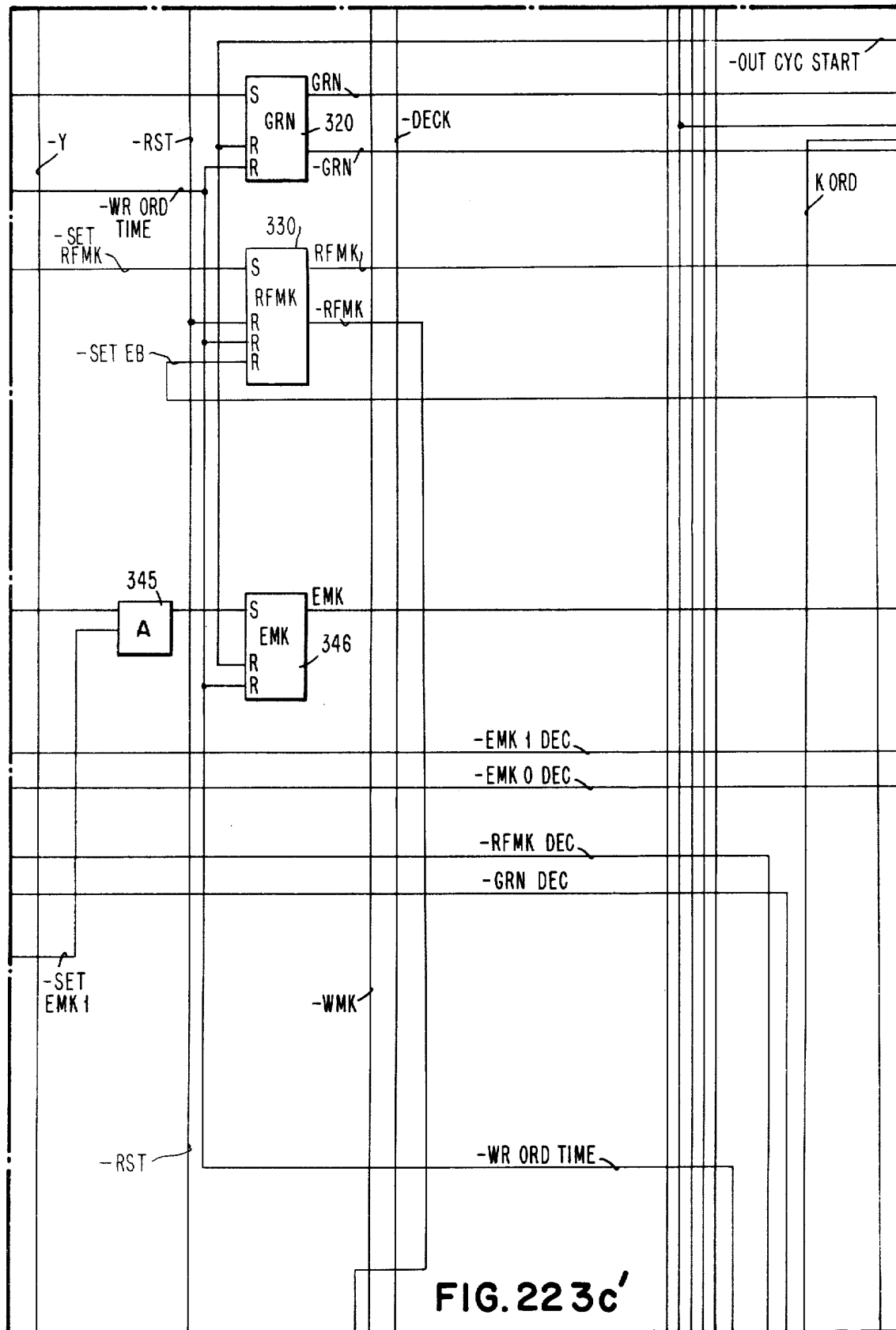


FIG. 22c 3



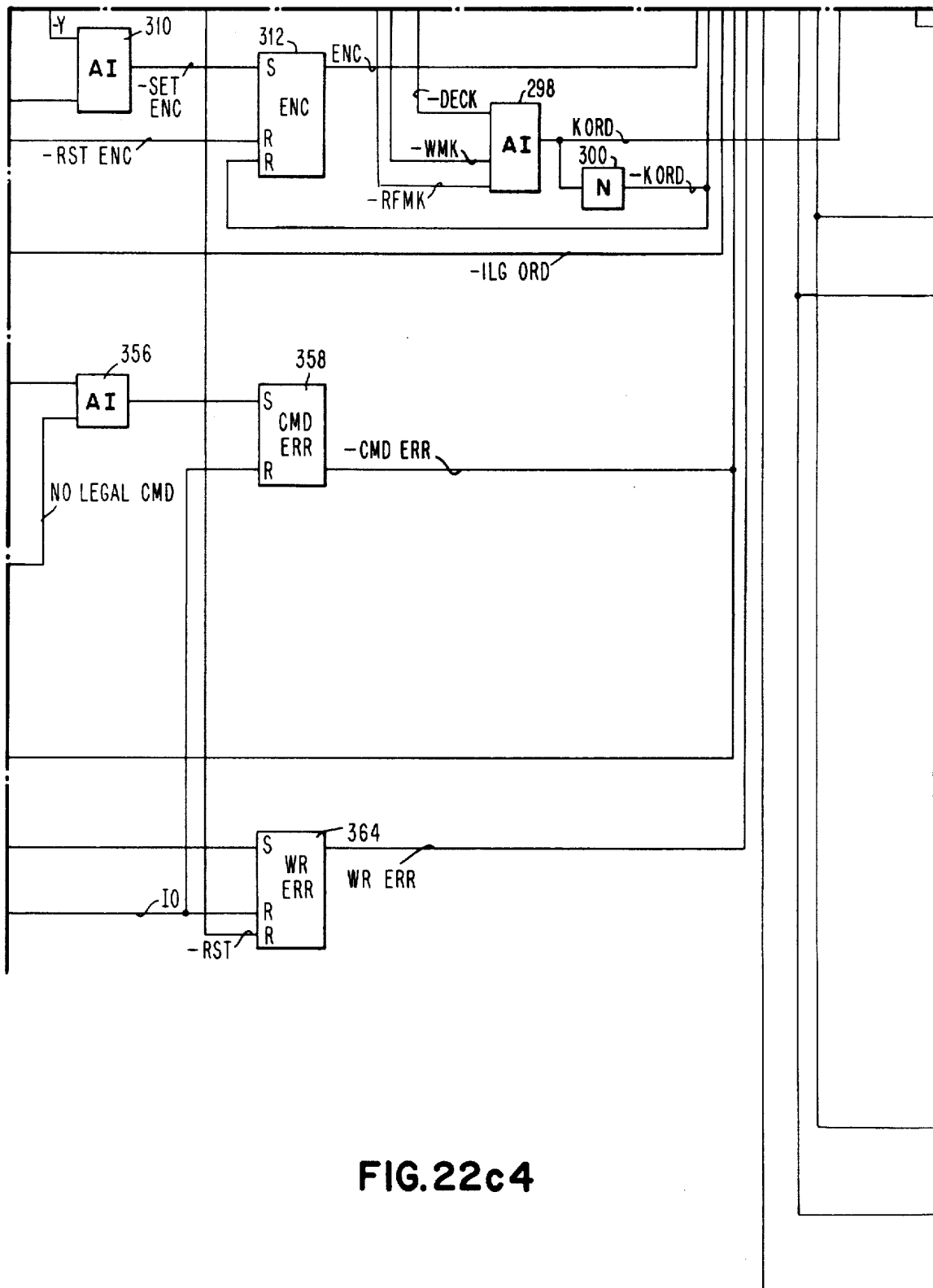


FIG. 22c4

FIG. 22 d1

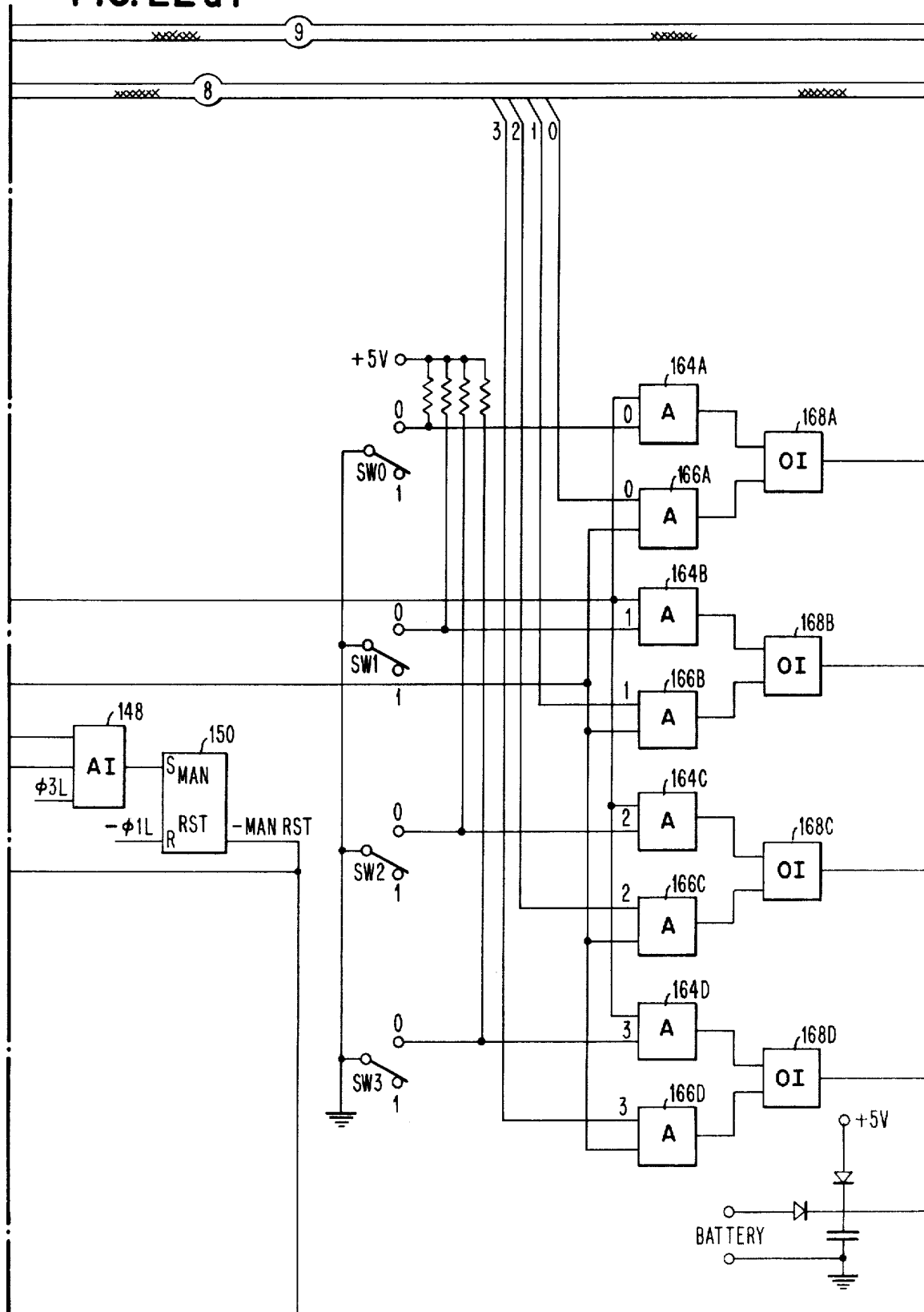
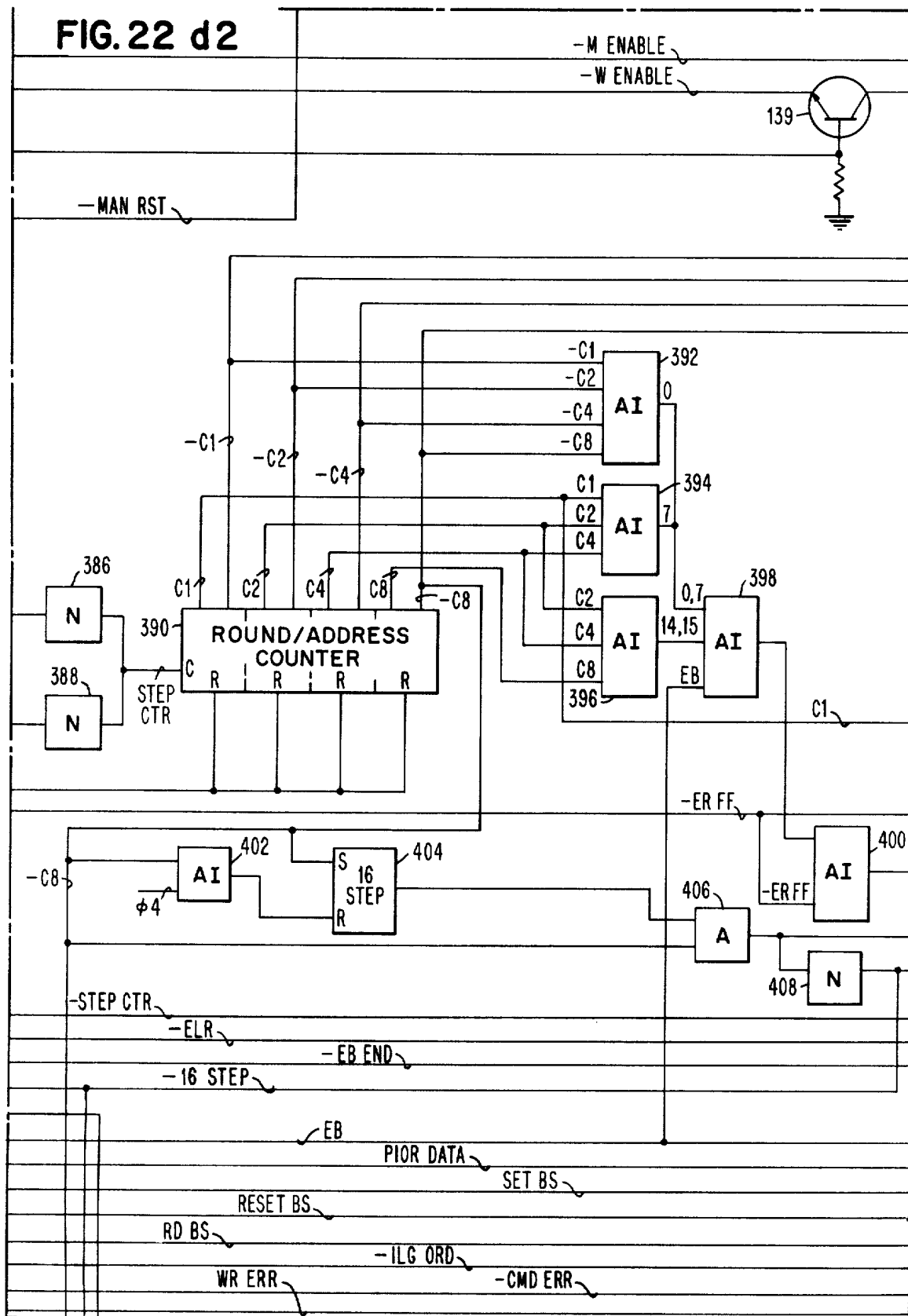
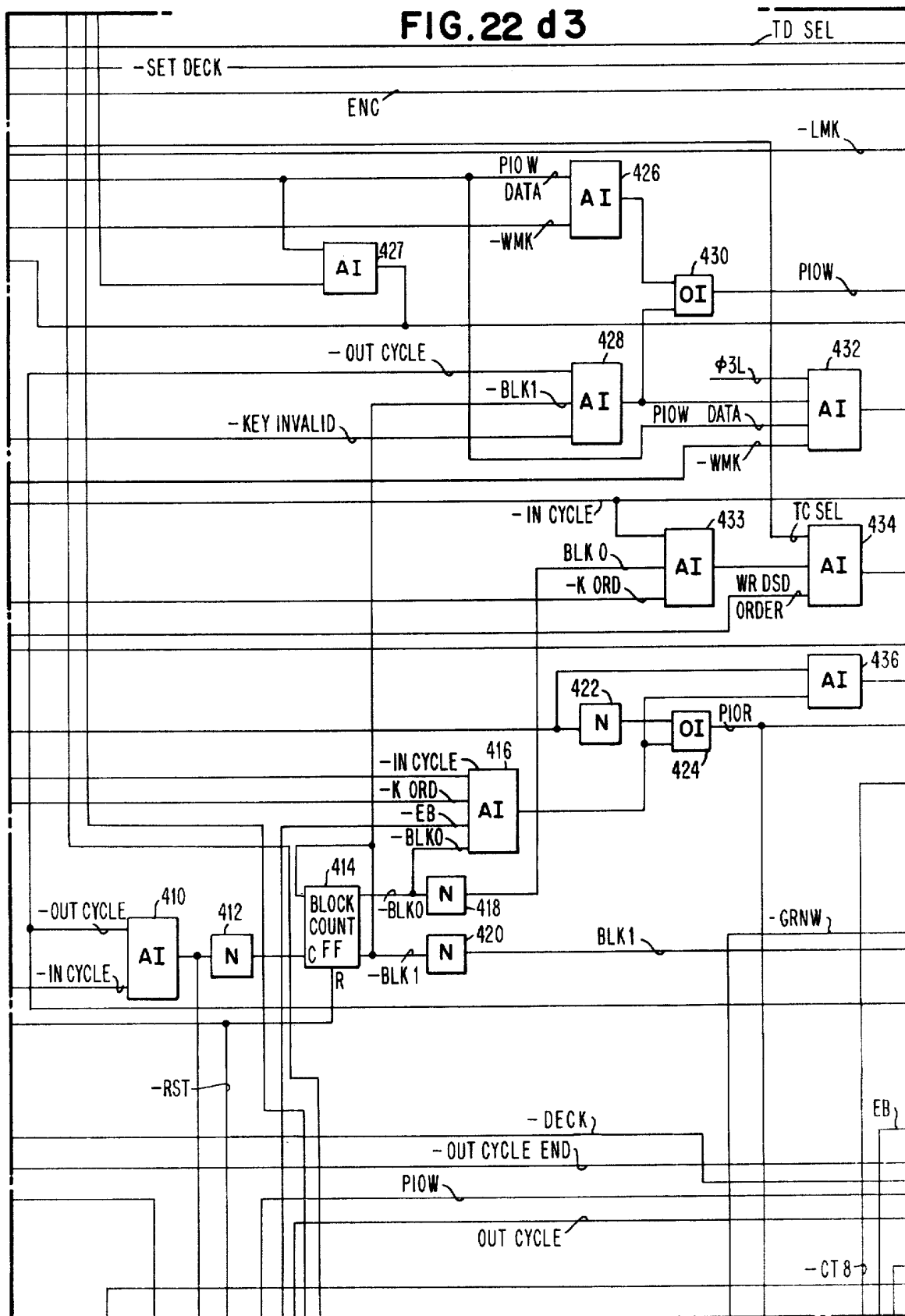
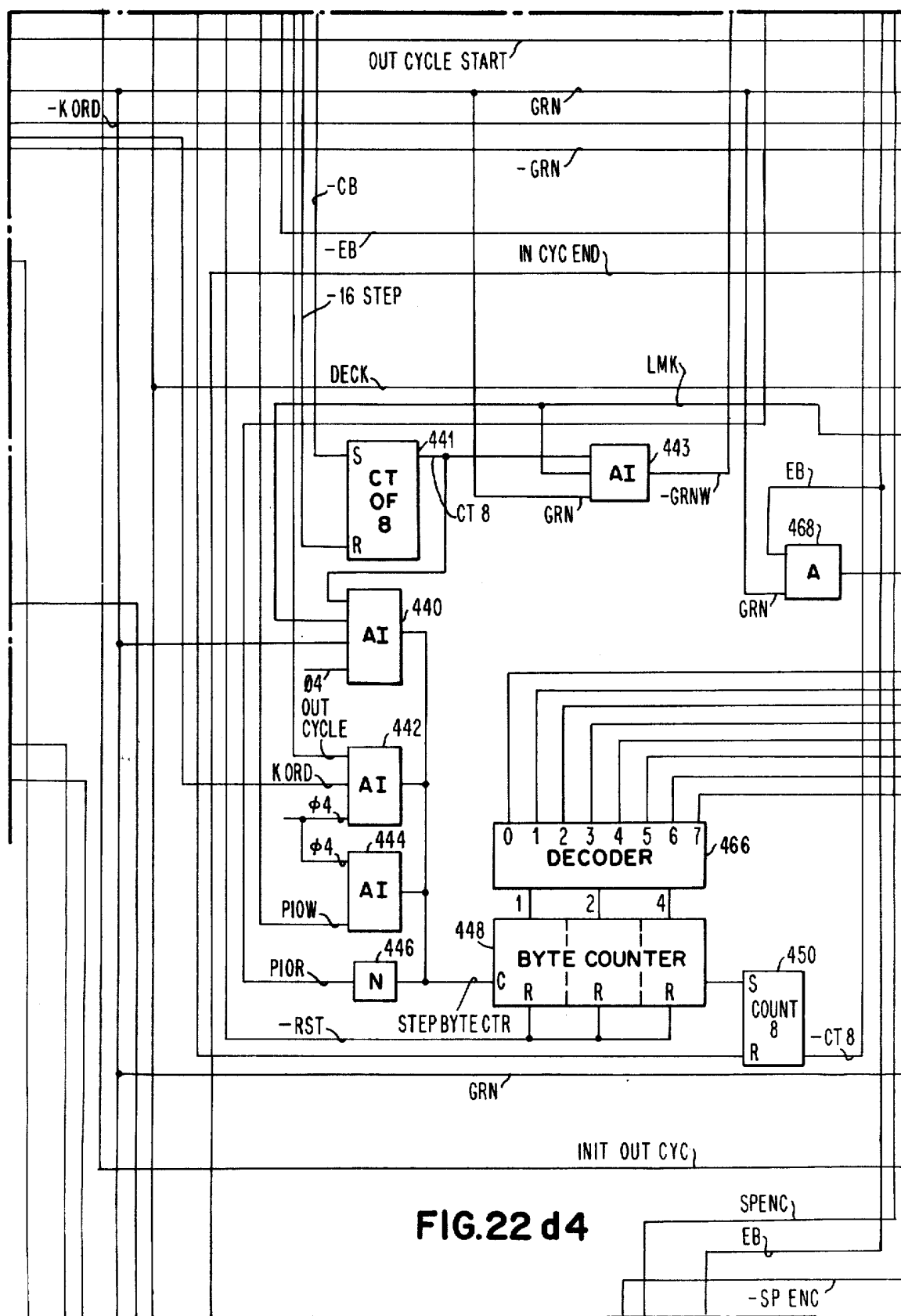


FIG. 22 d2







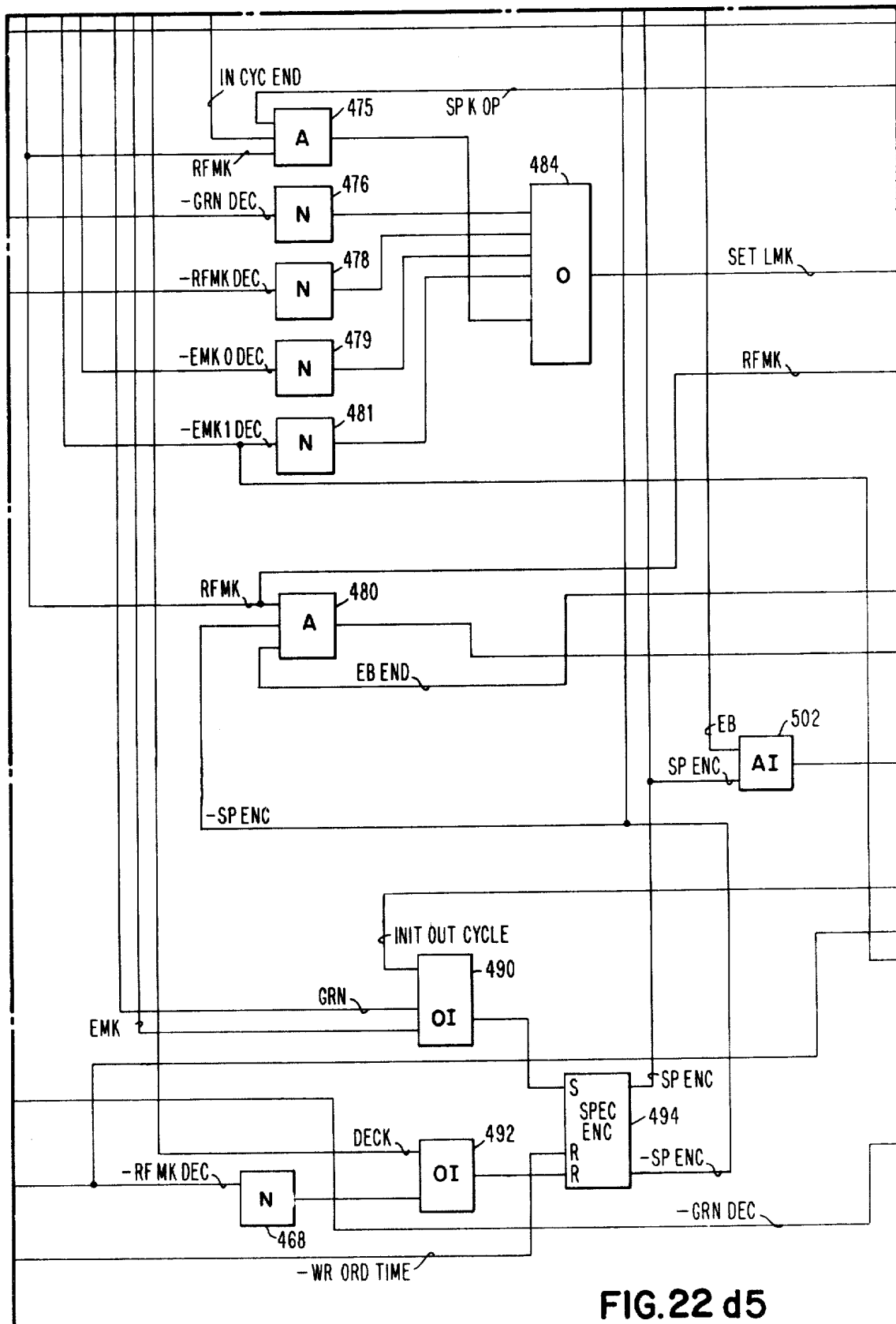
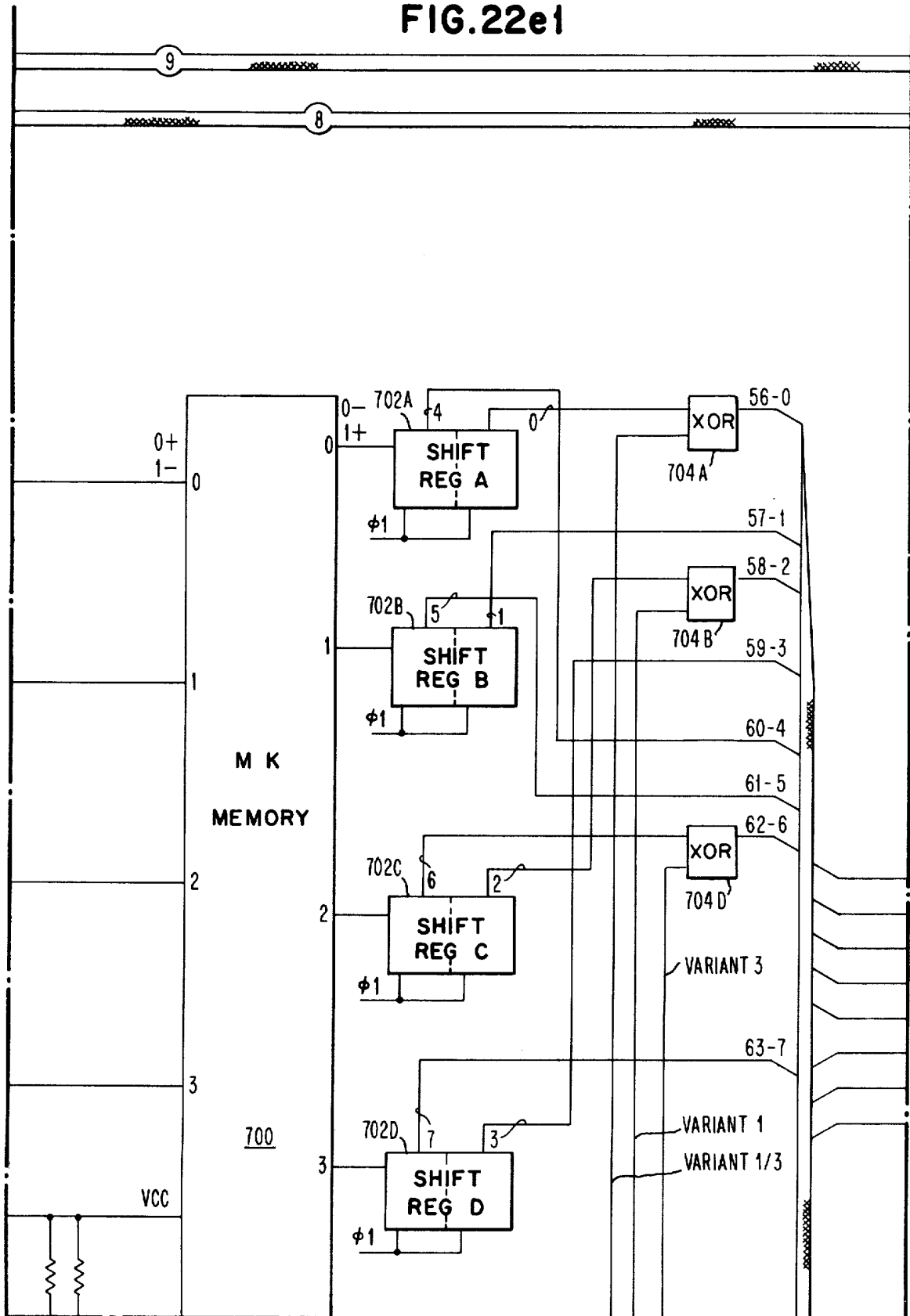


FIG. 22 d5

FIG.22e1



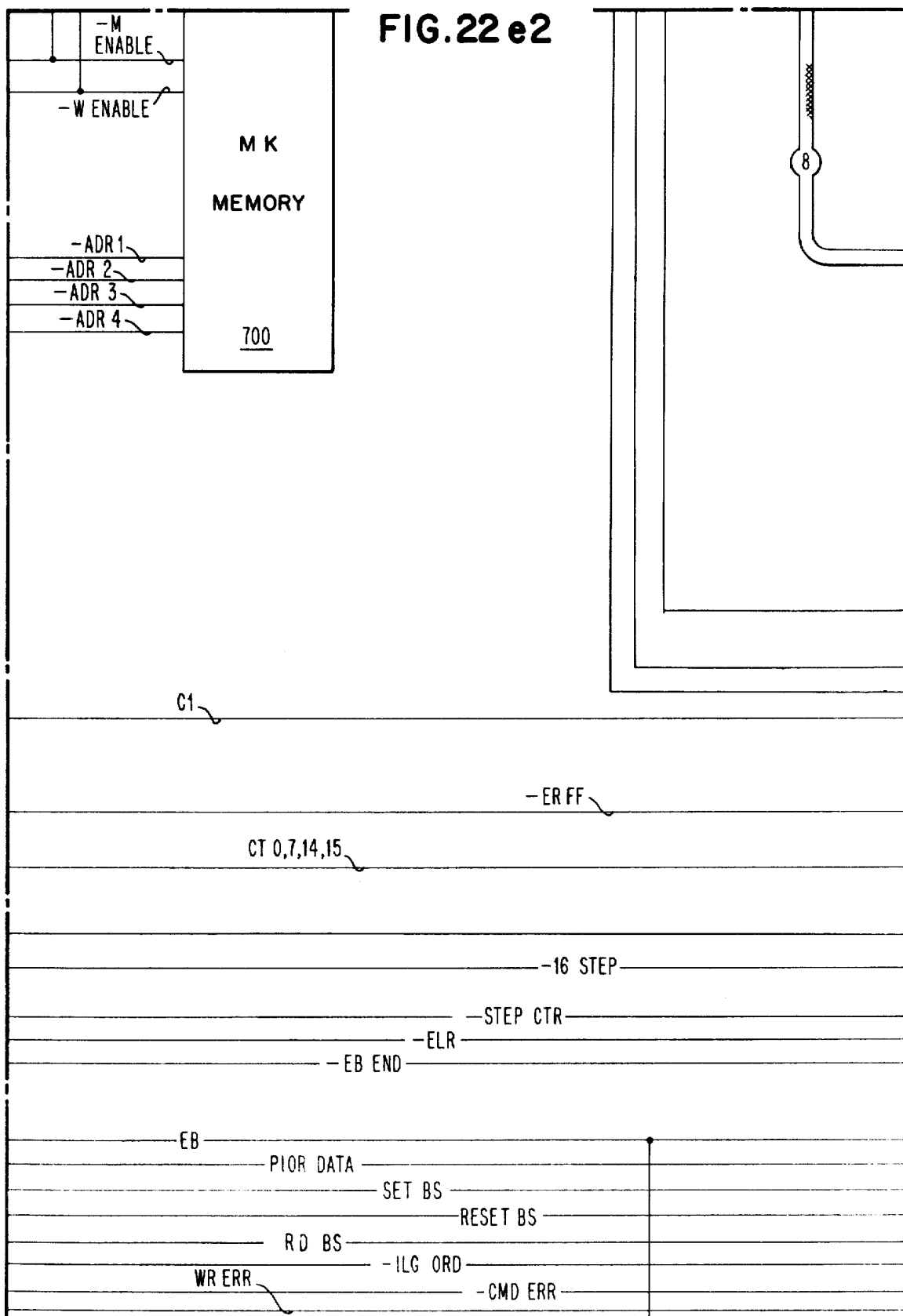
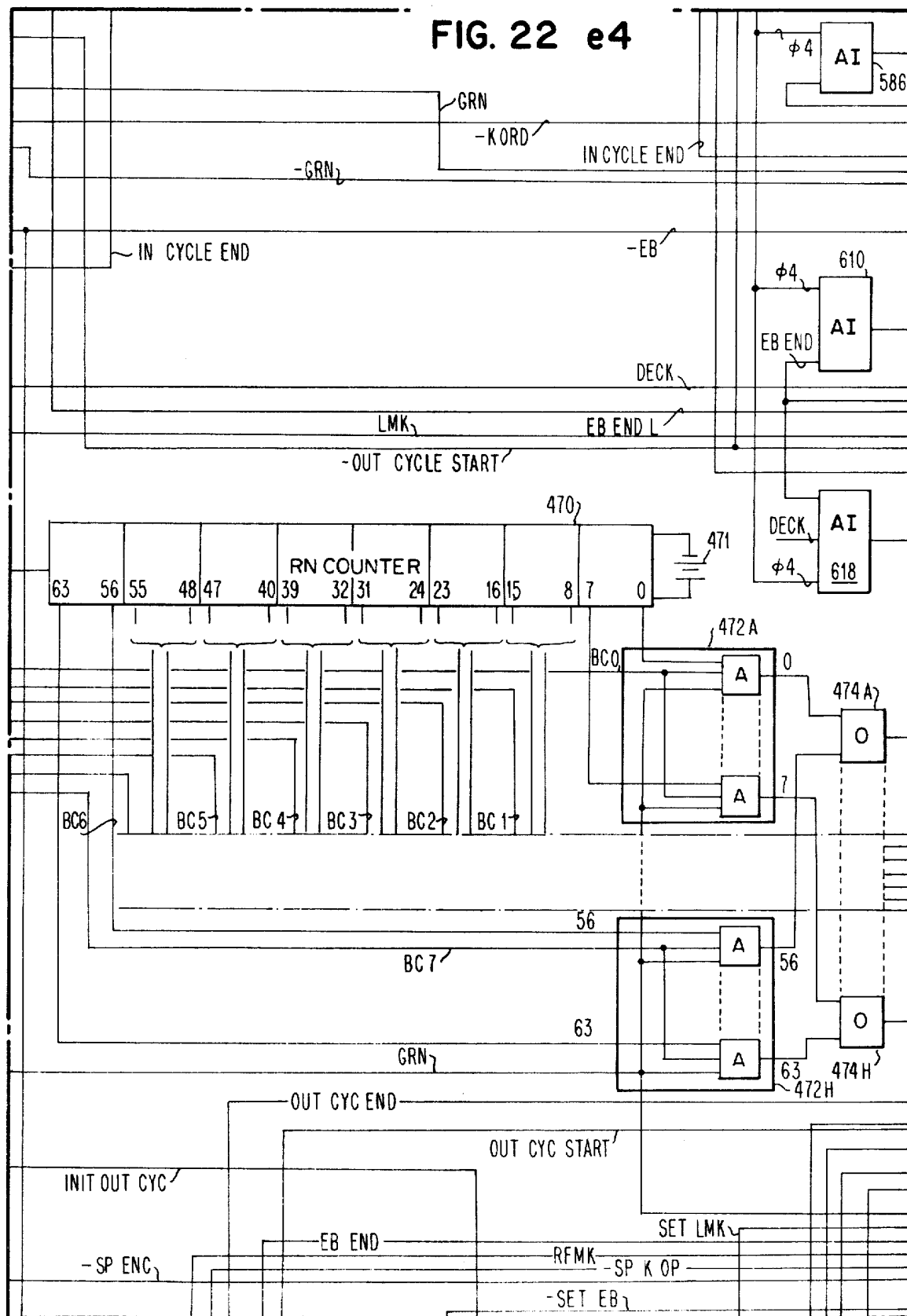


FIG. 22 e4



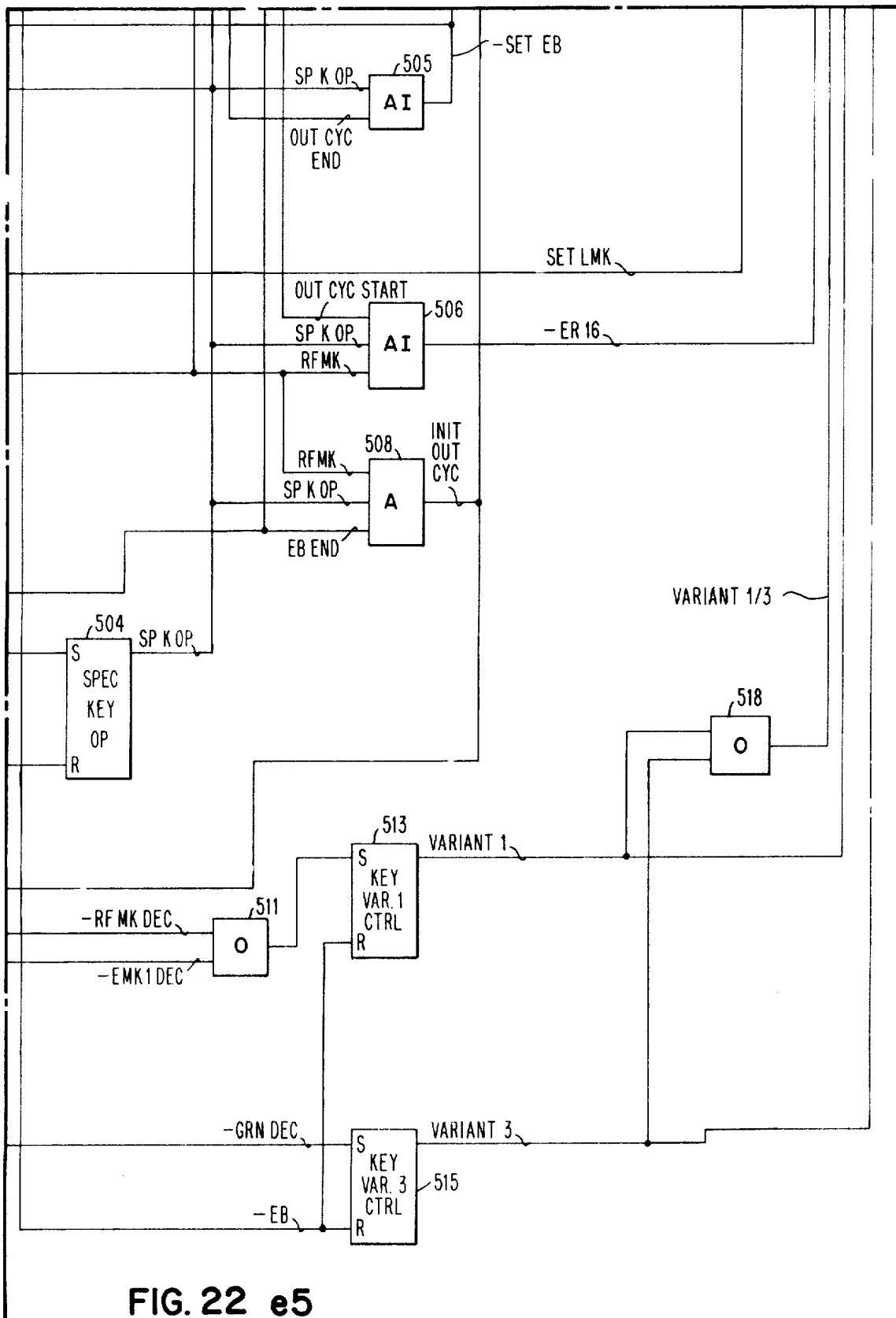
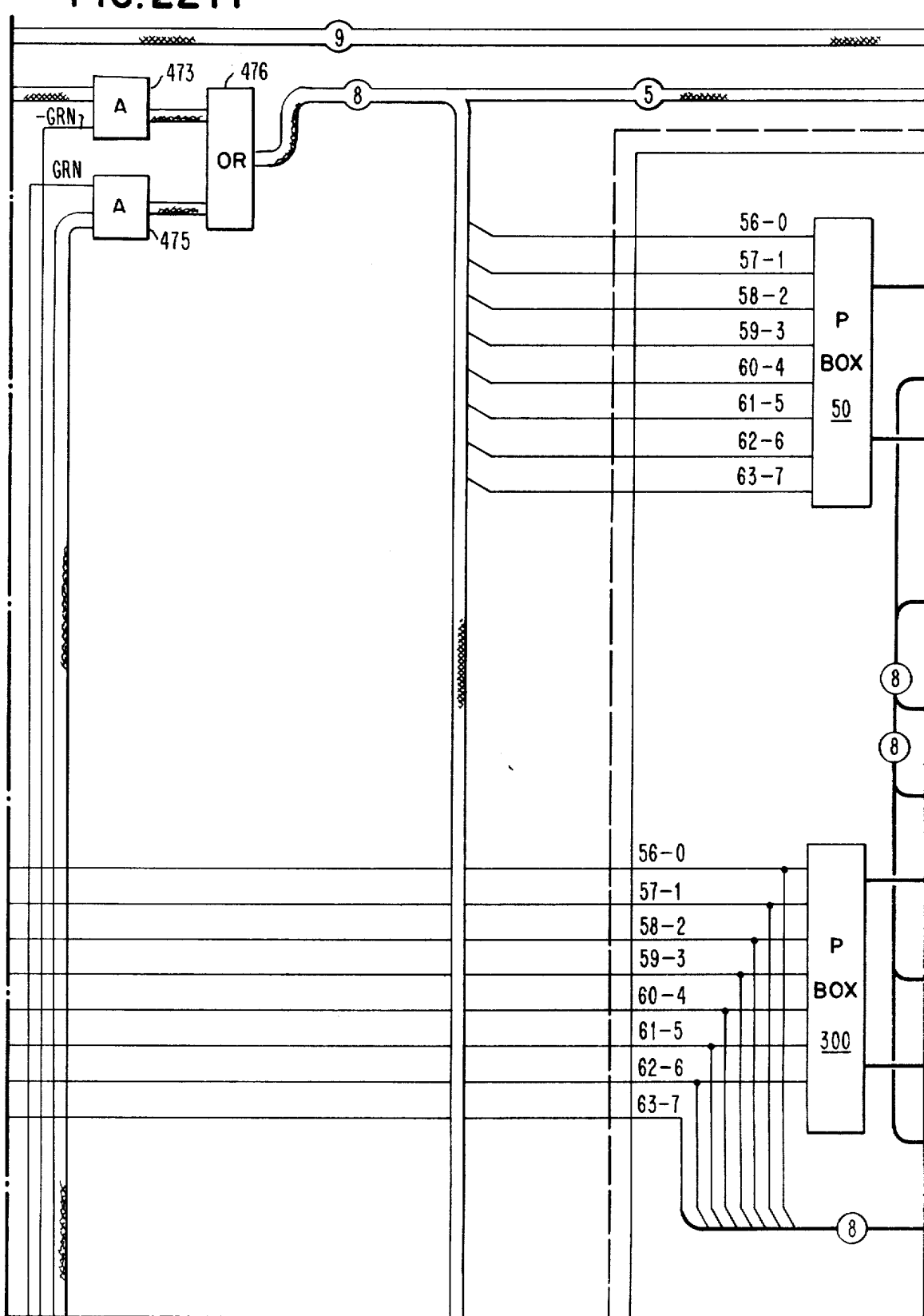


FIG. 22 e5

FIG. 22f1



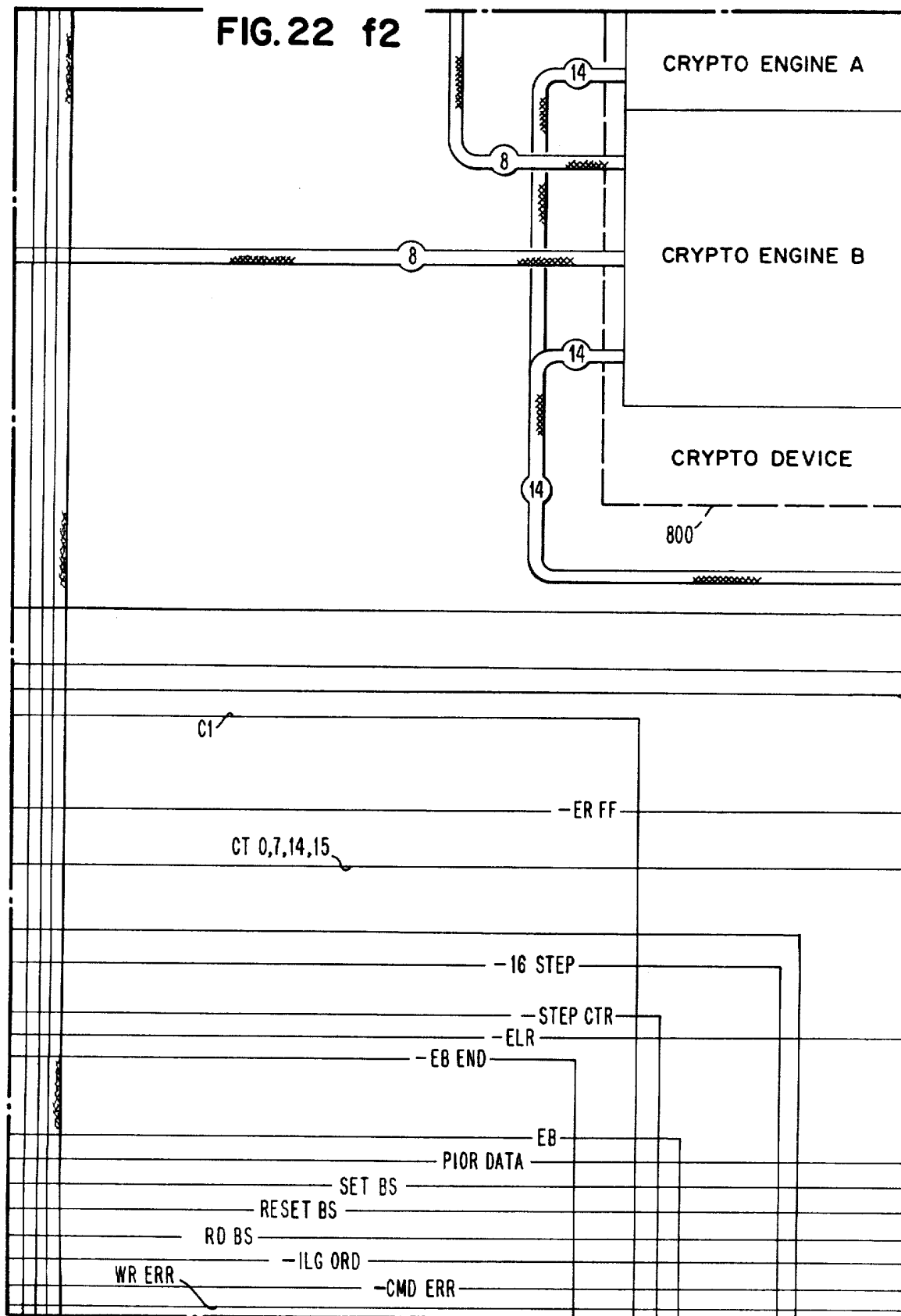
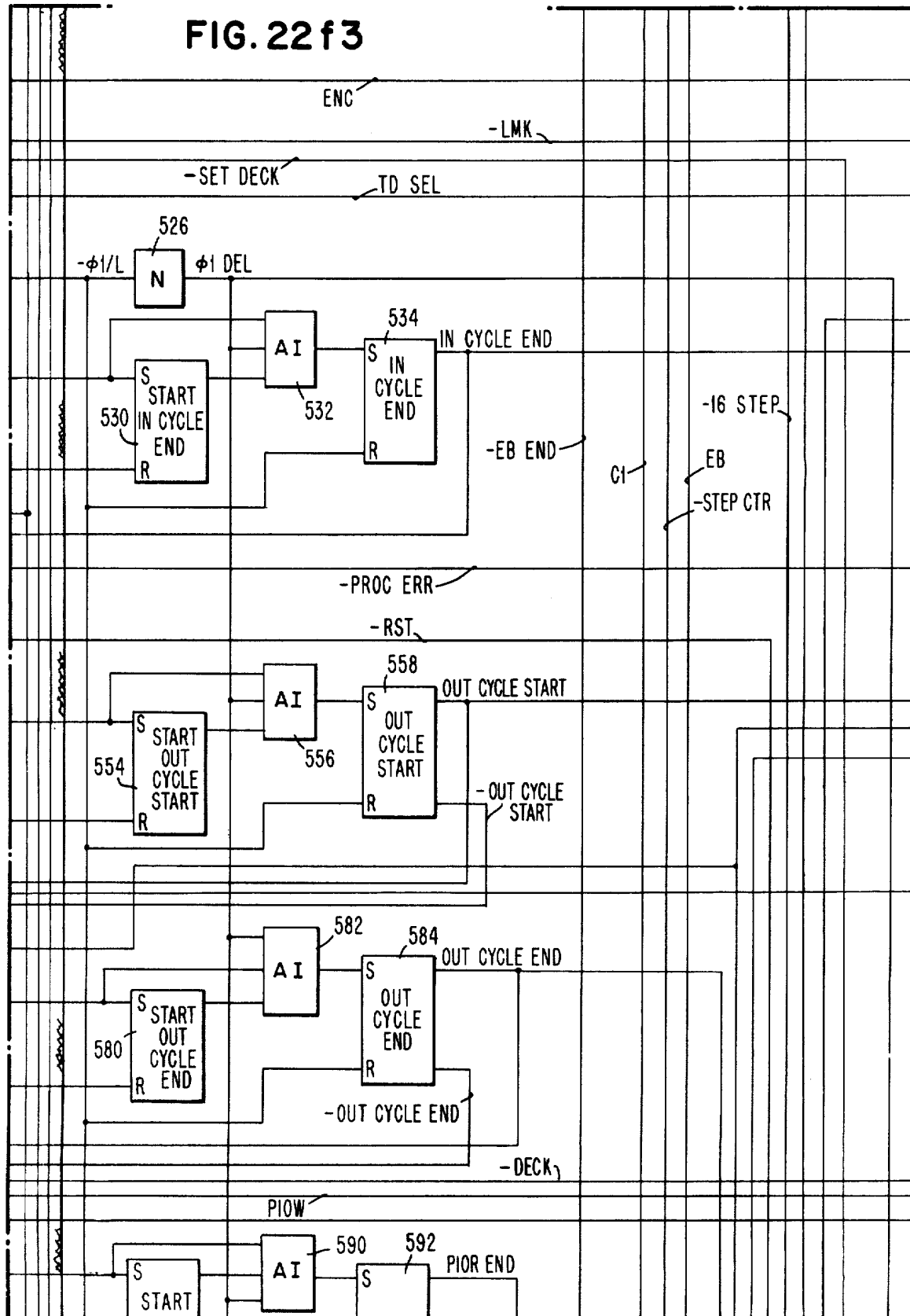


FIG. 22f3



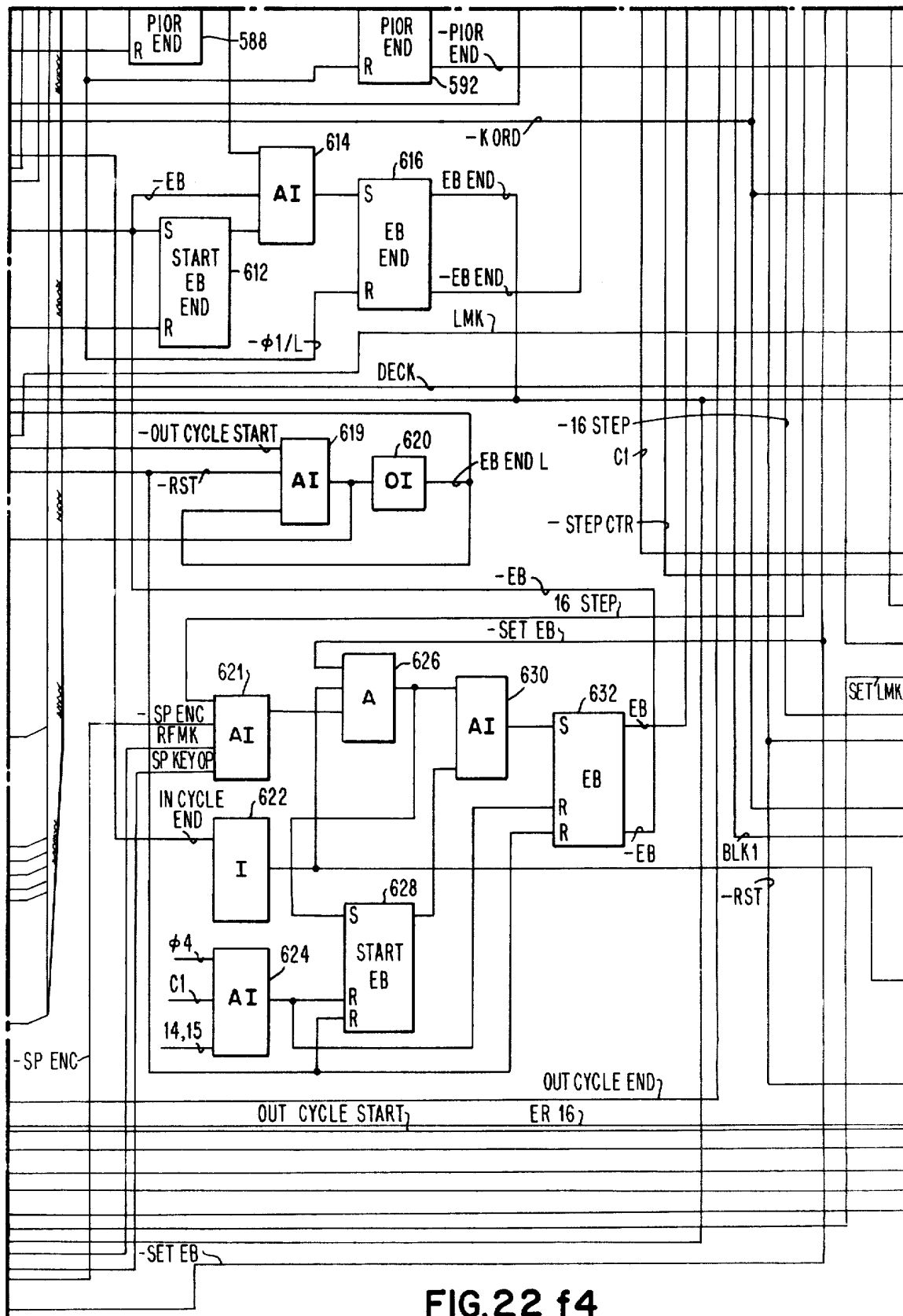
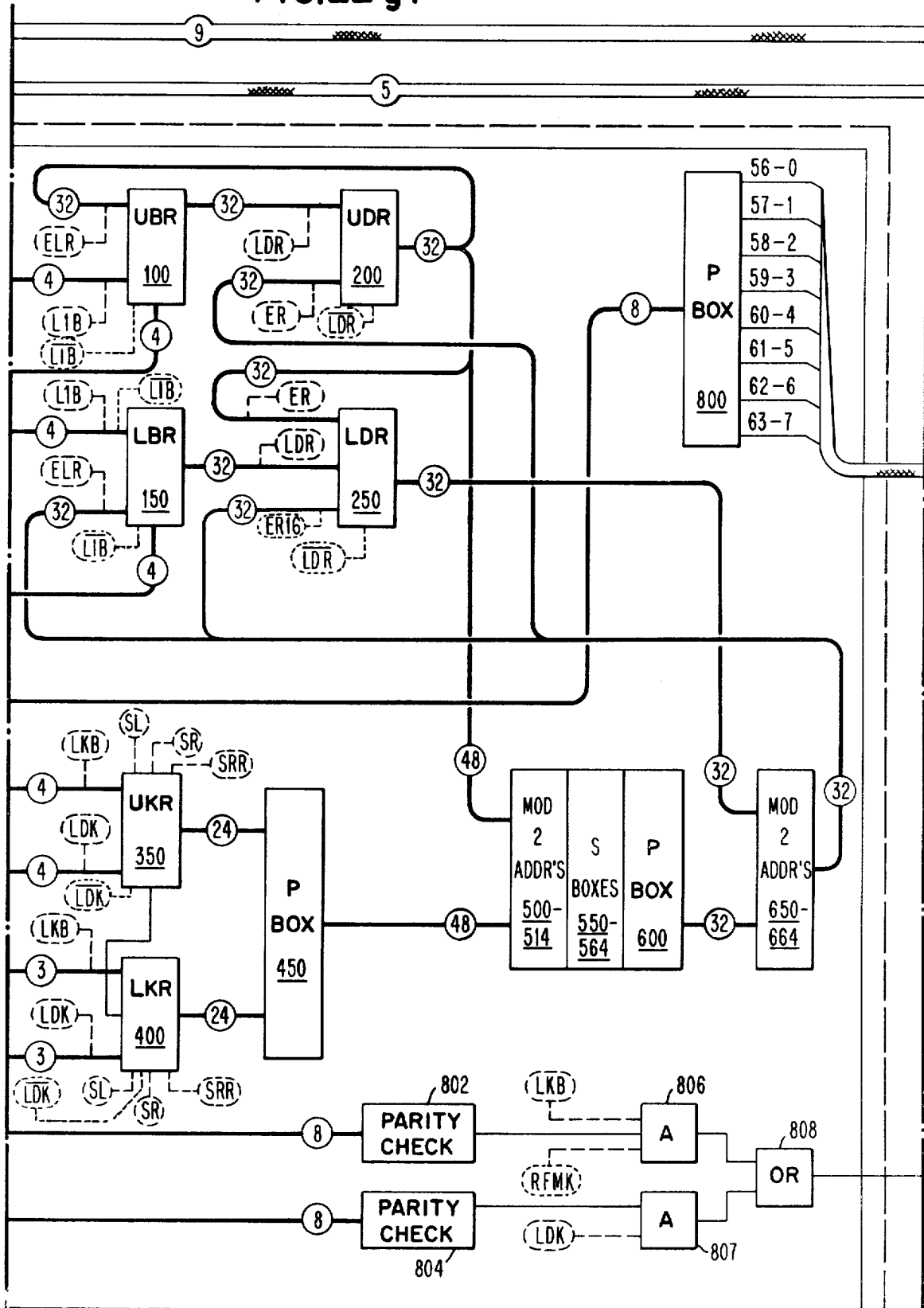


FIG. 22 g1



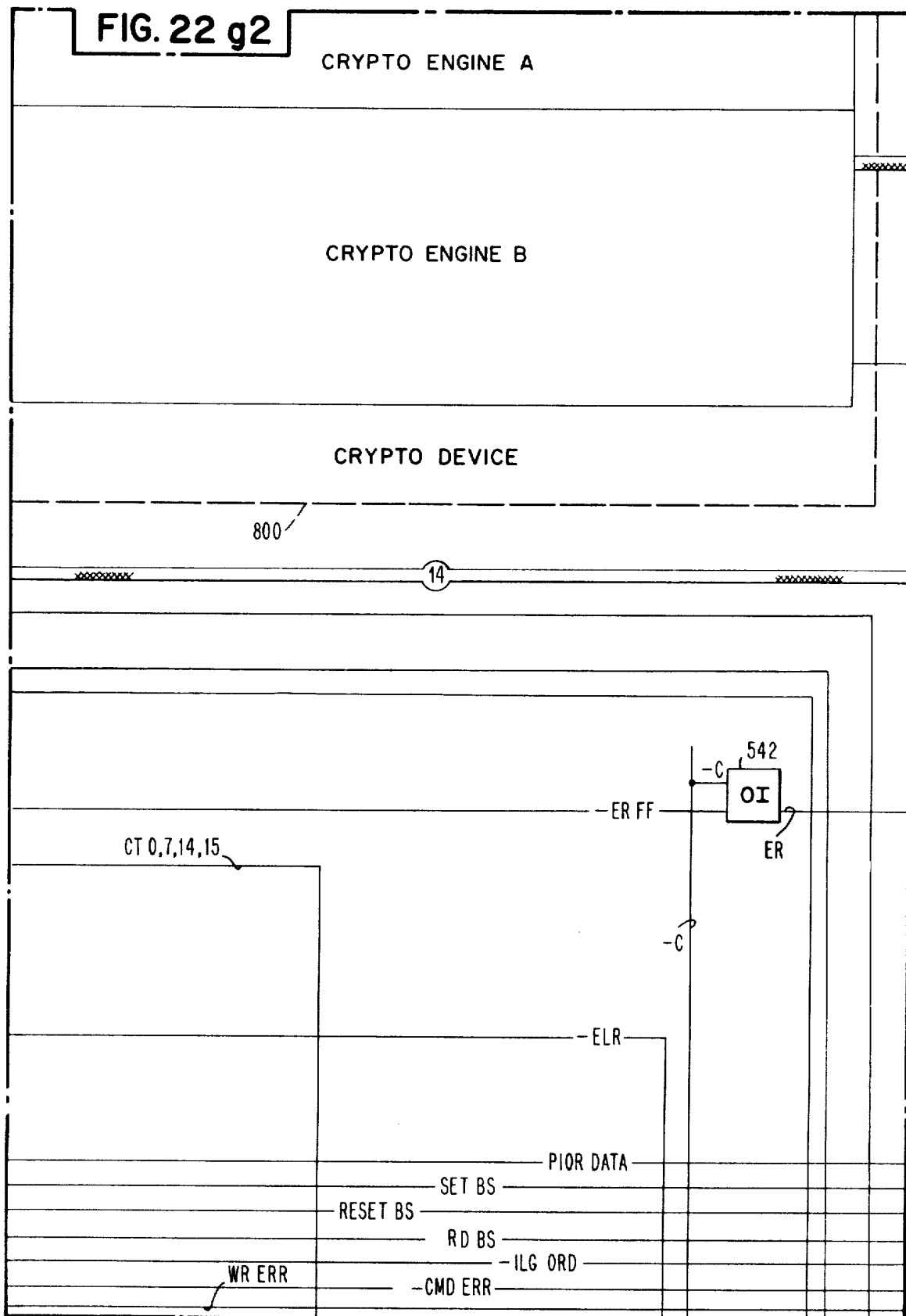
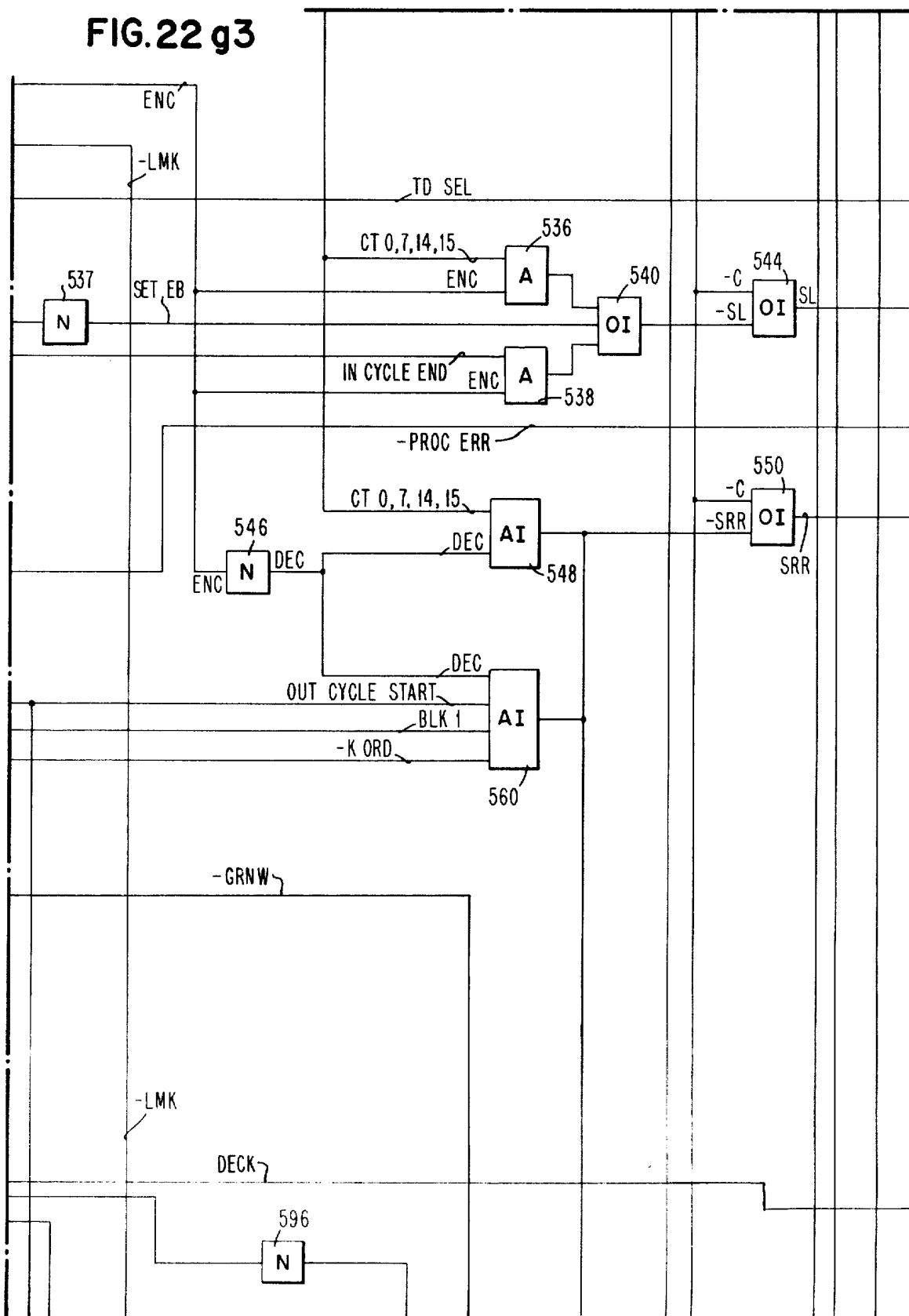


FIG. 22 g3



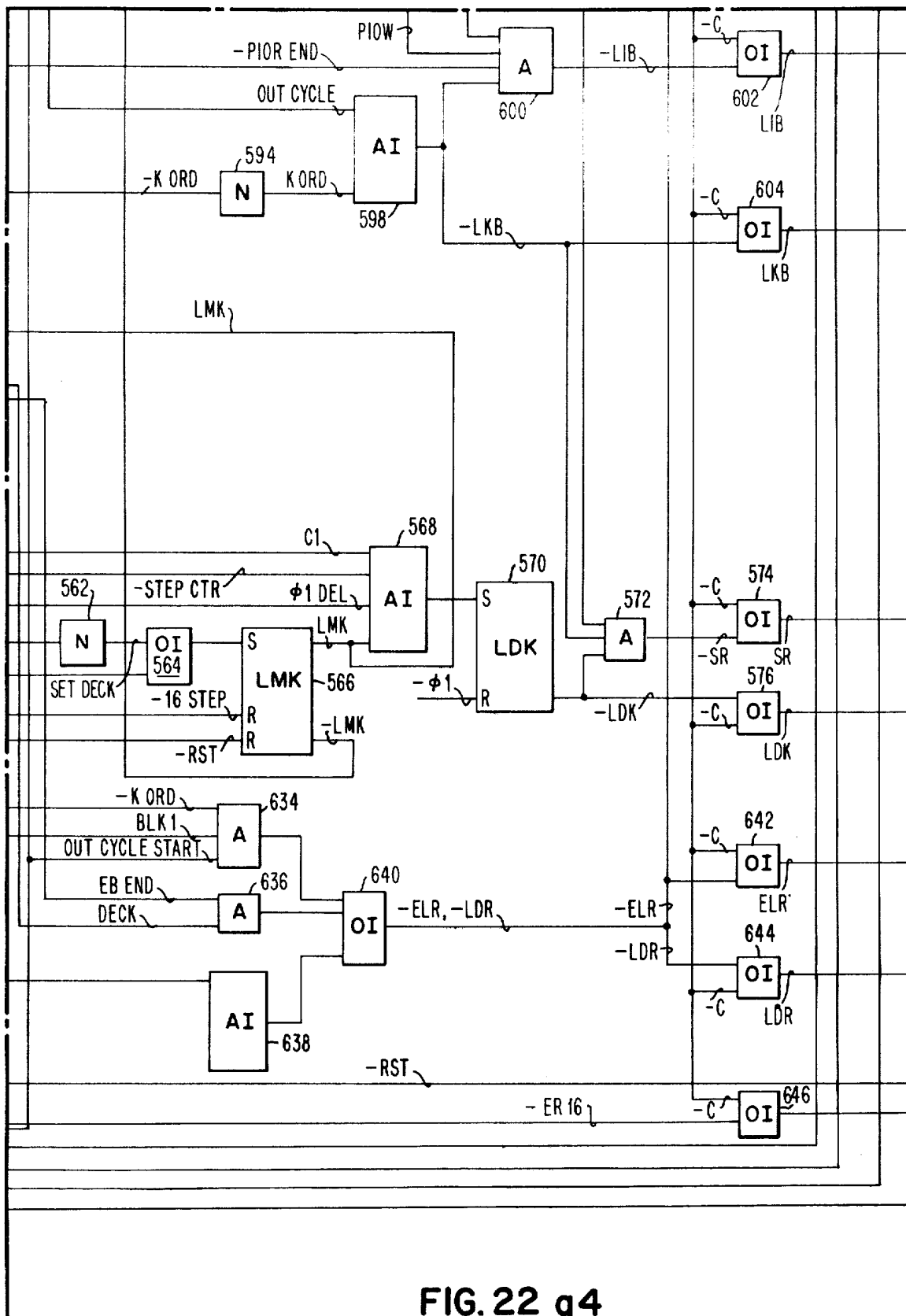


FIG. 22 g4

FIG.22h1

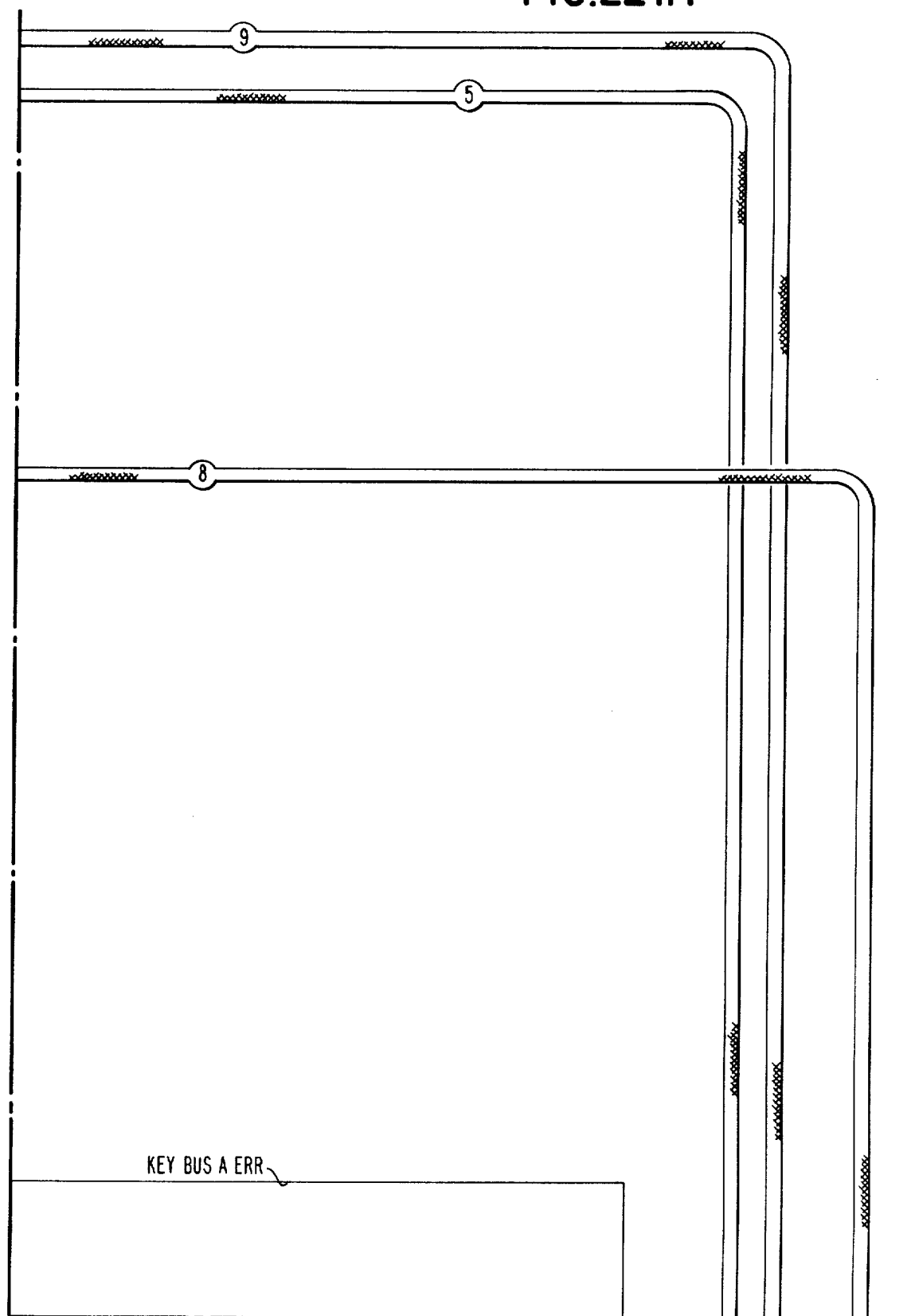
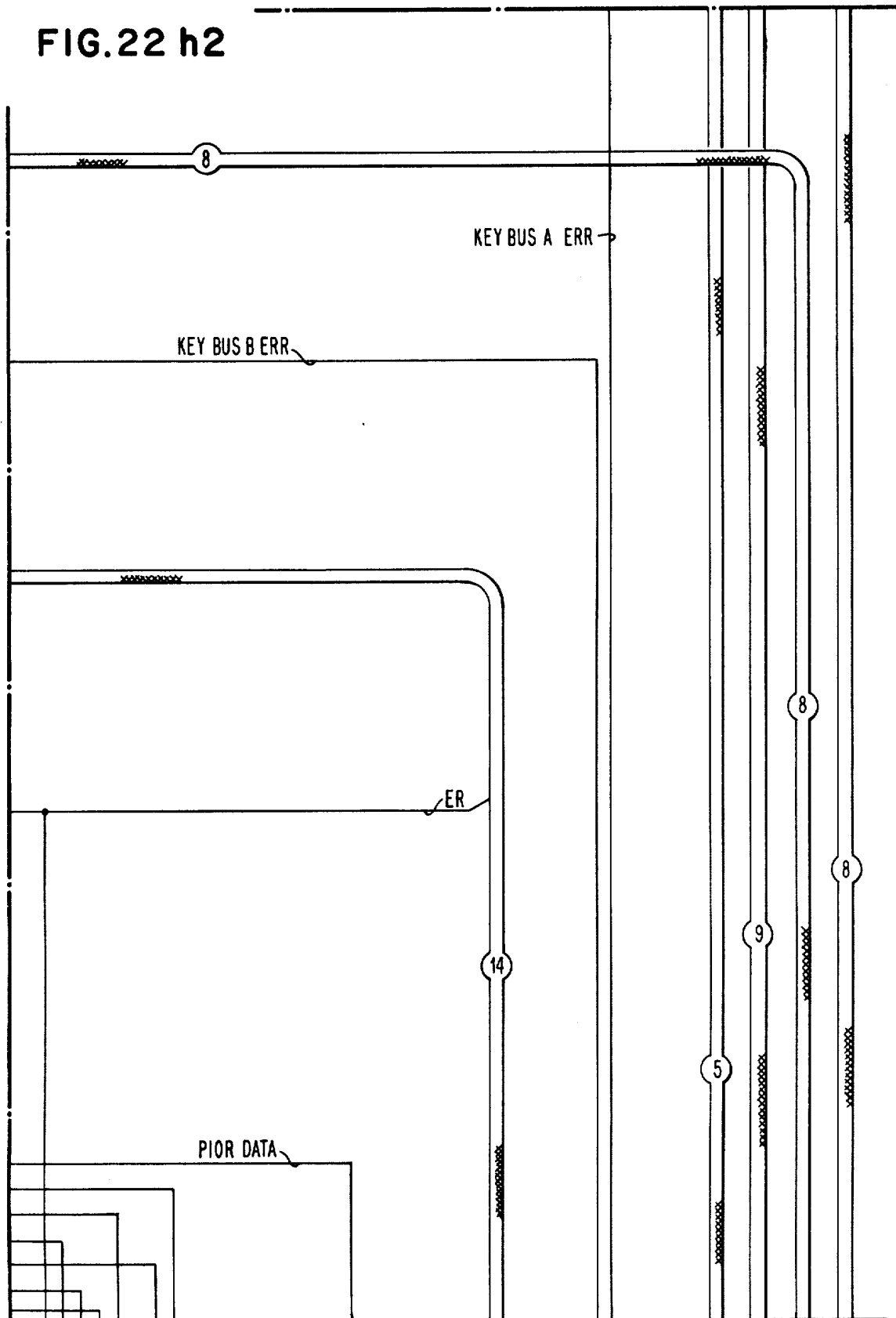


FIG.22 h2



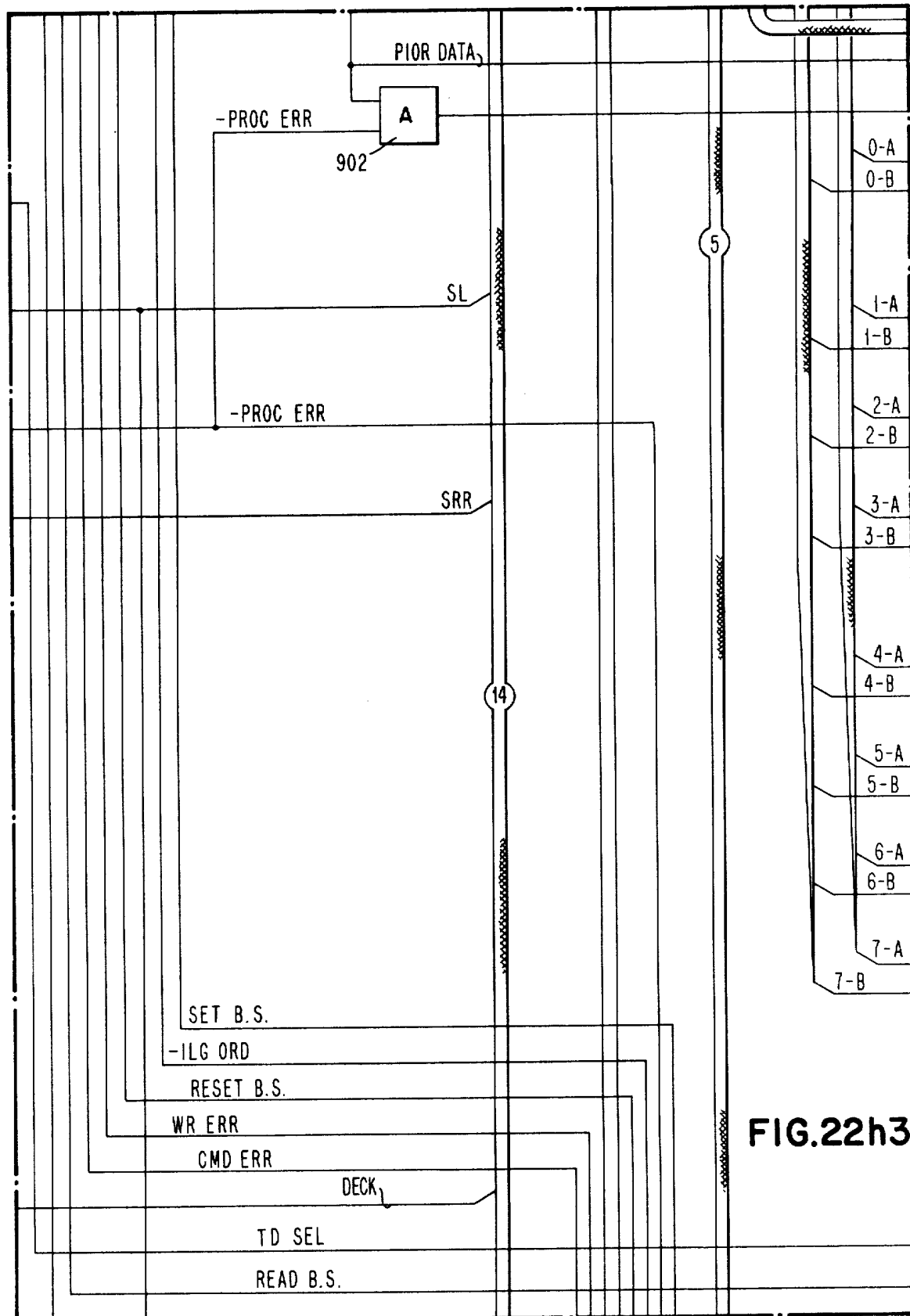


FIG. 22h3

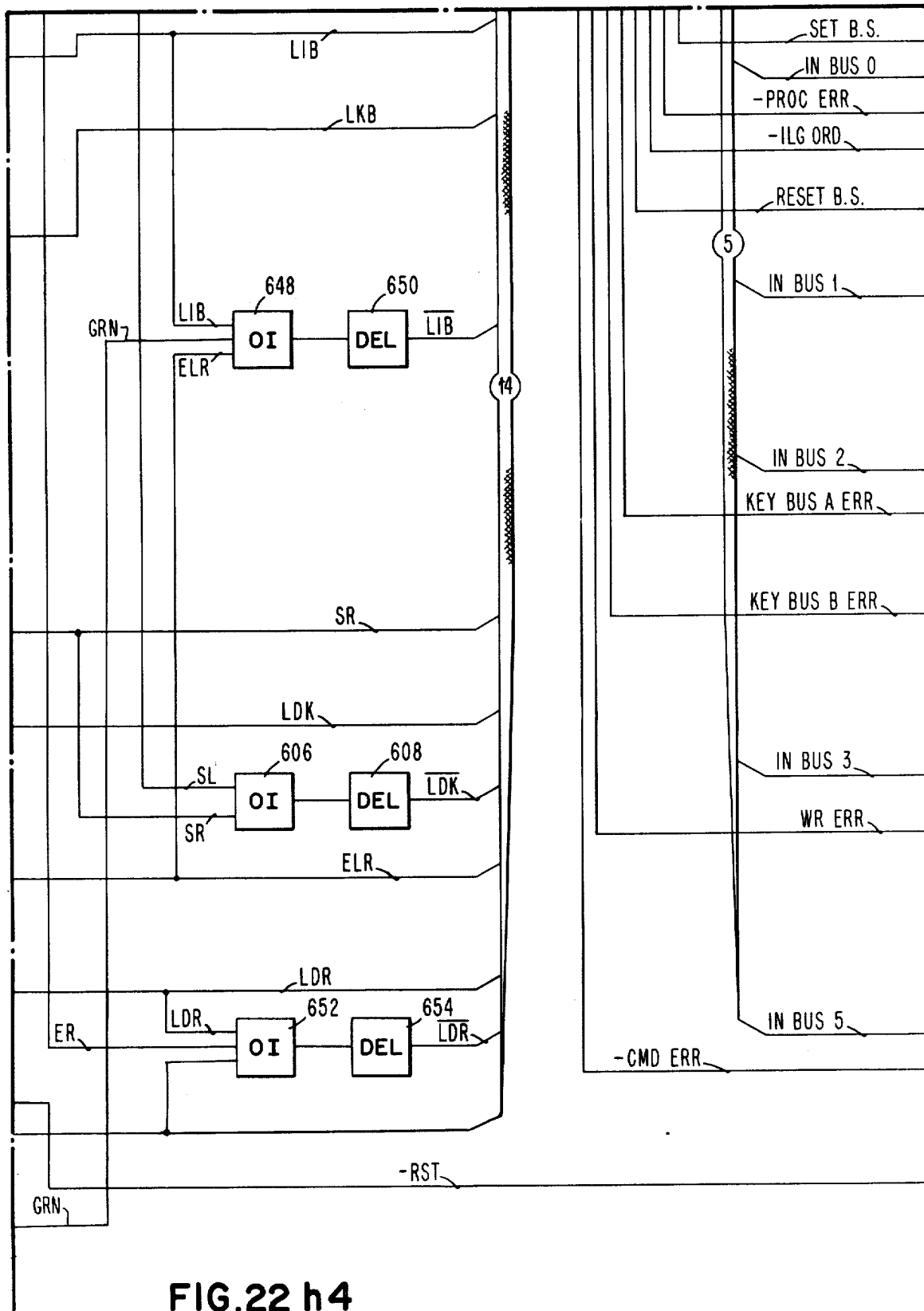
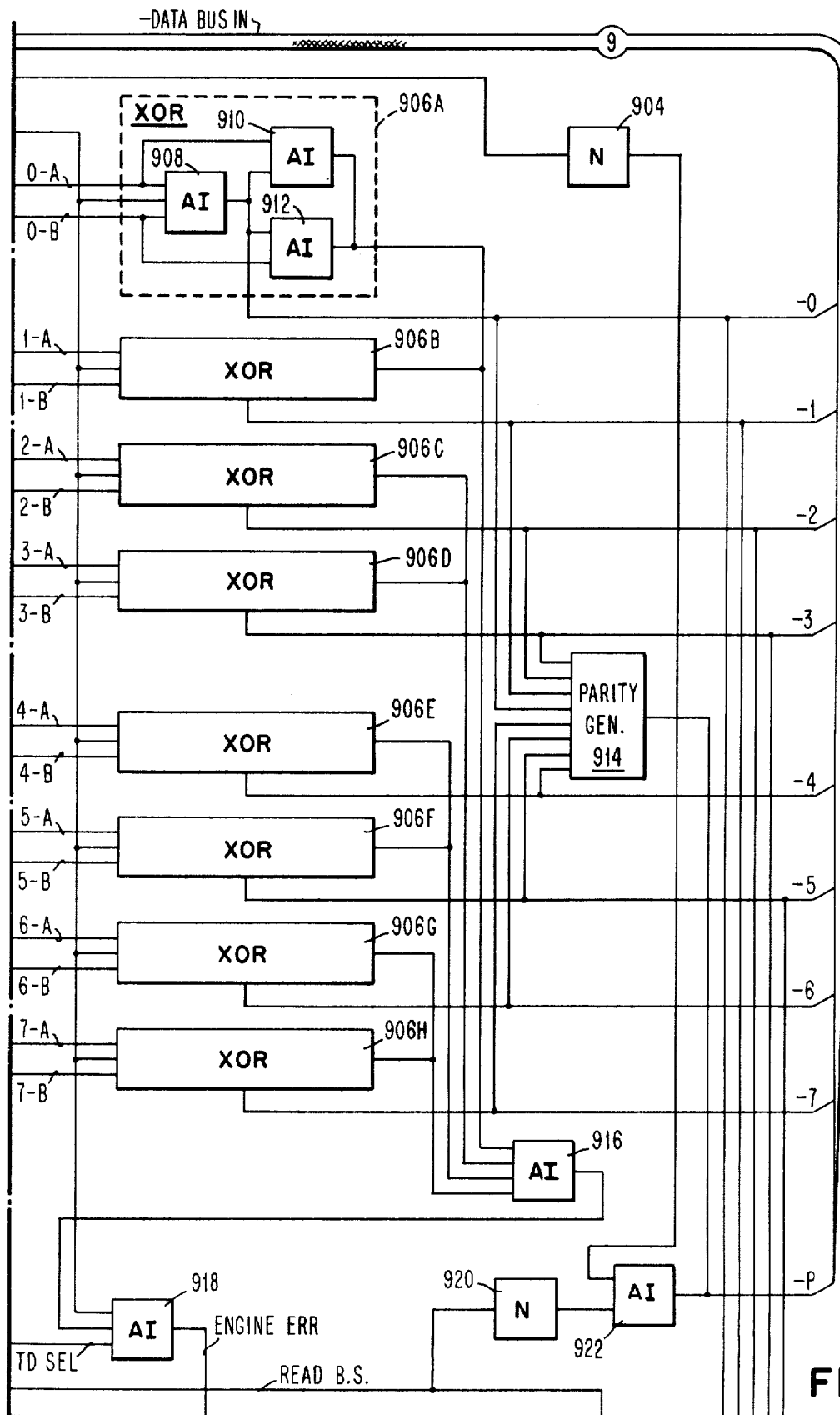


FIG. 22 h4



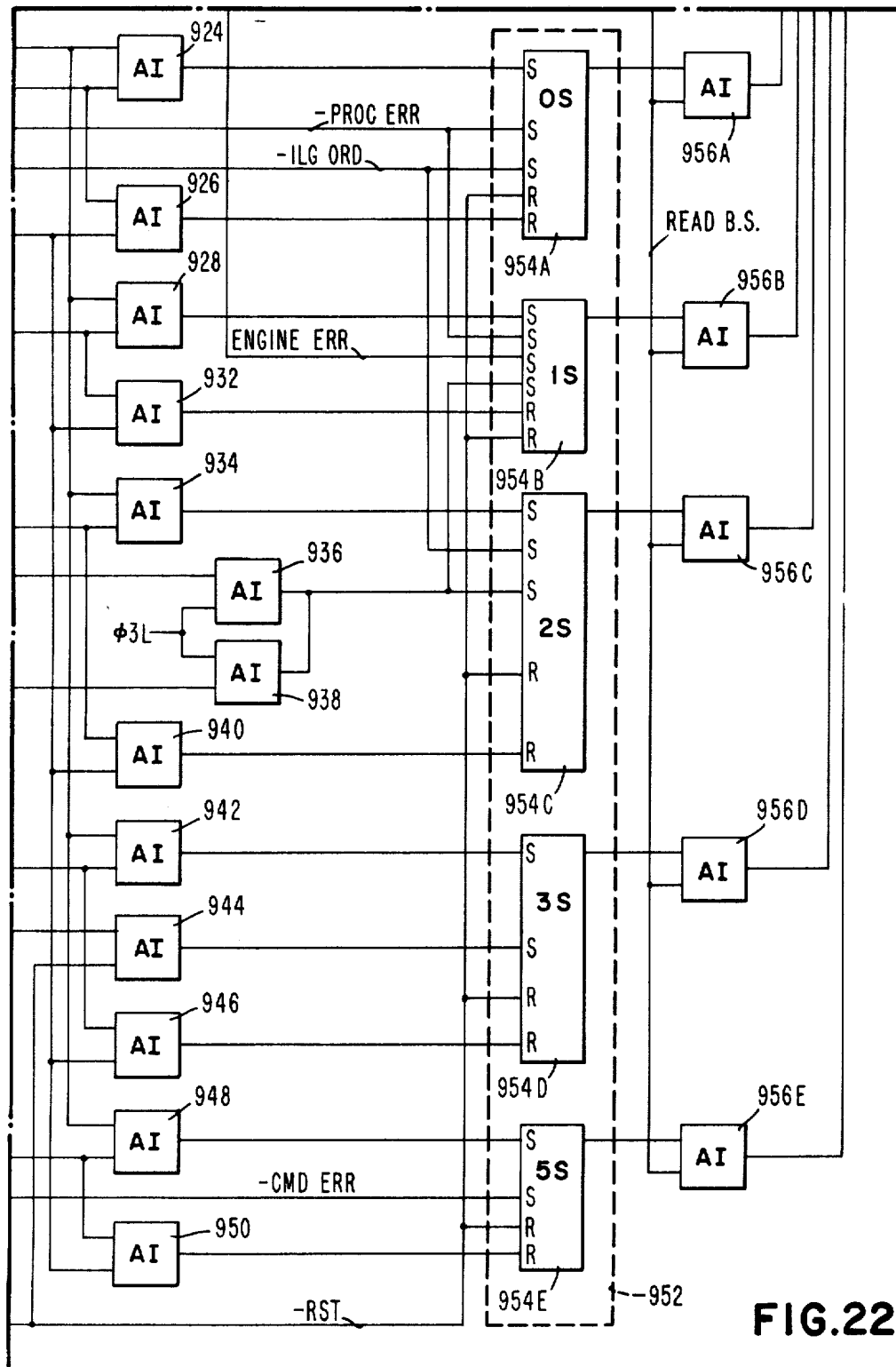


FIG. 22i2

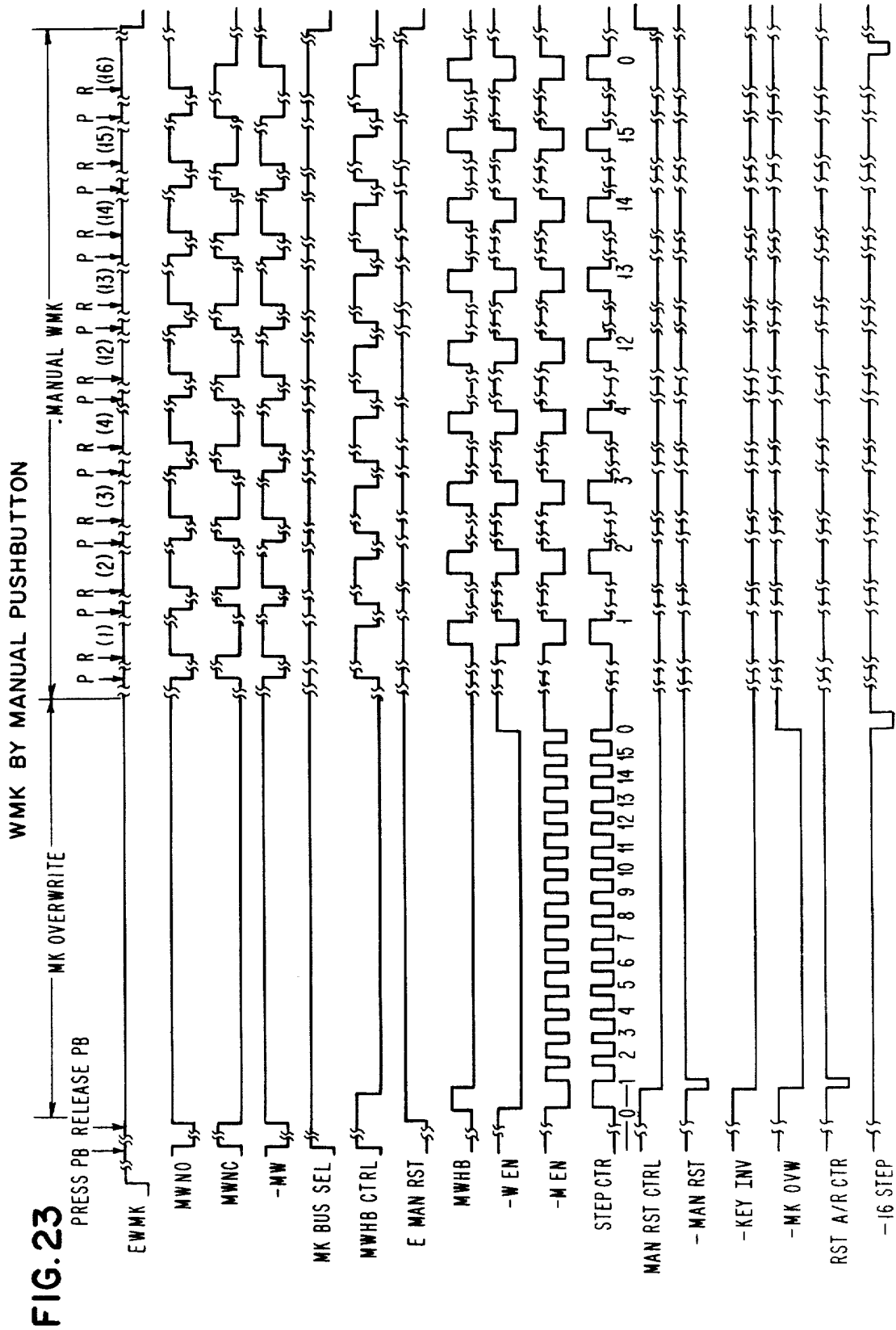


FIG. 24B

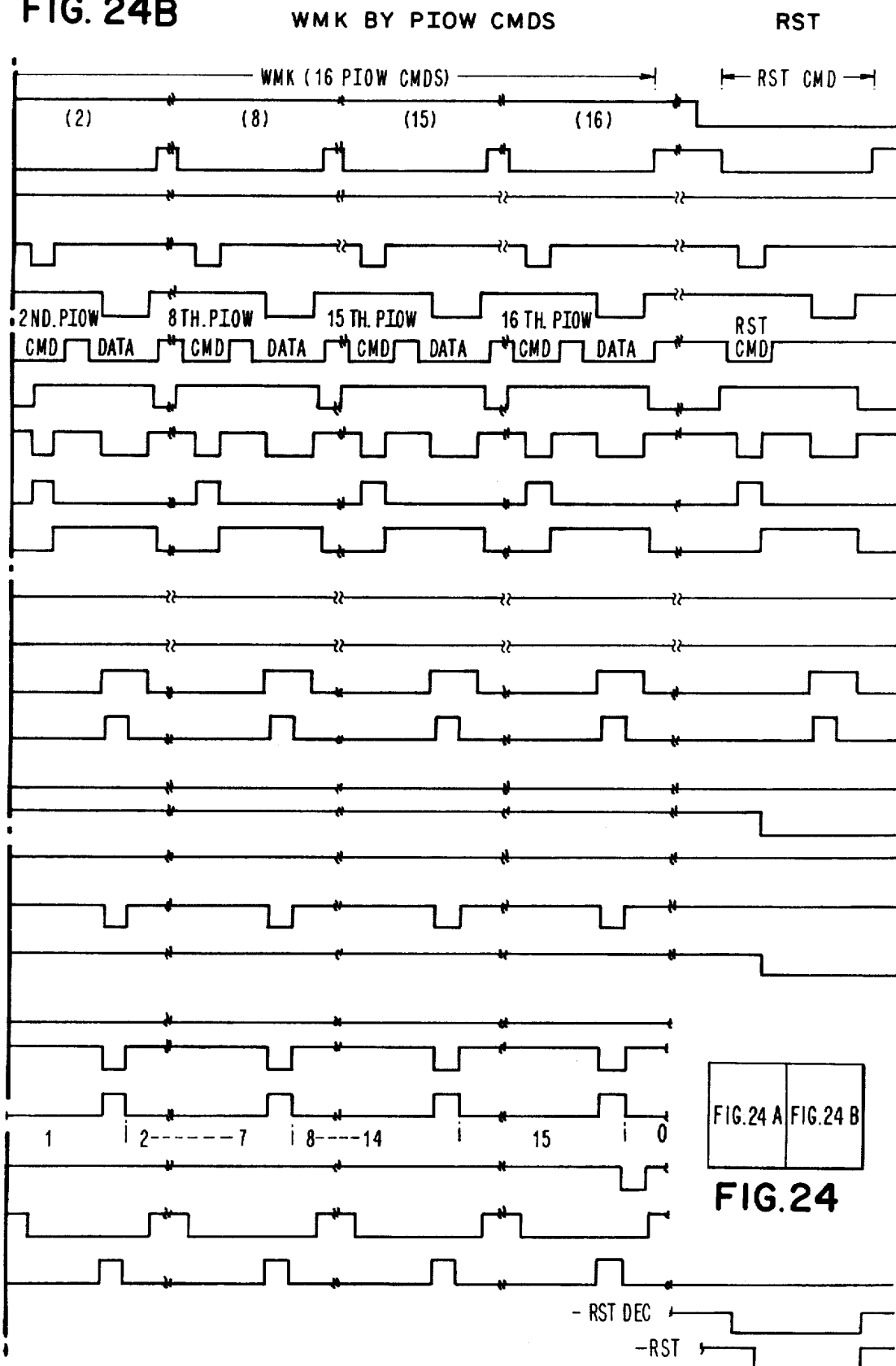
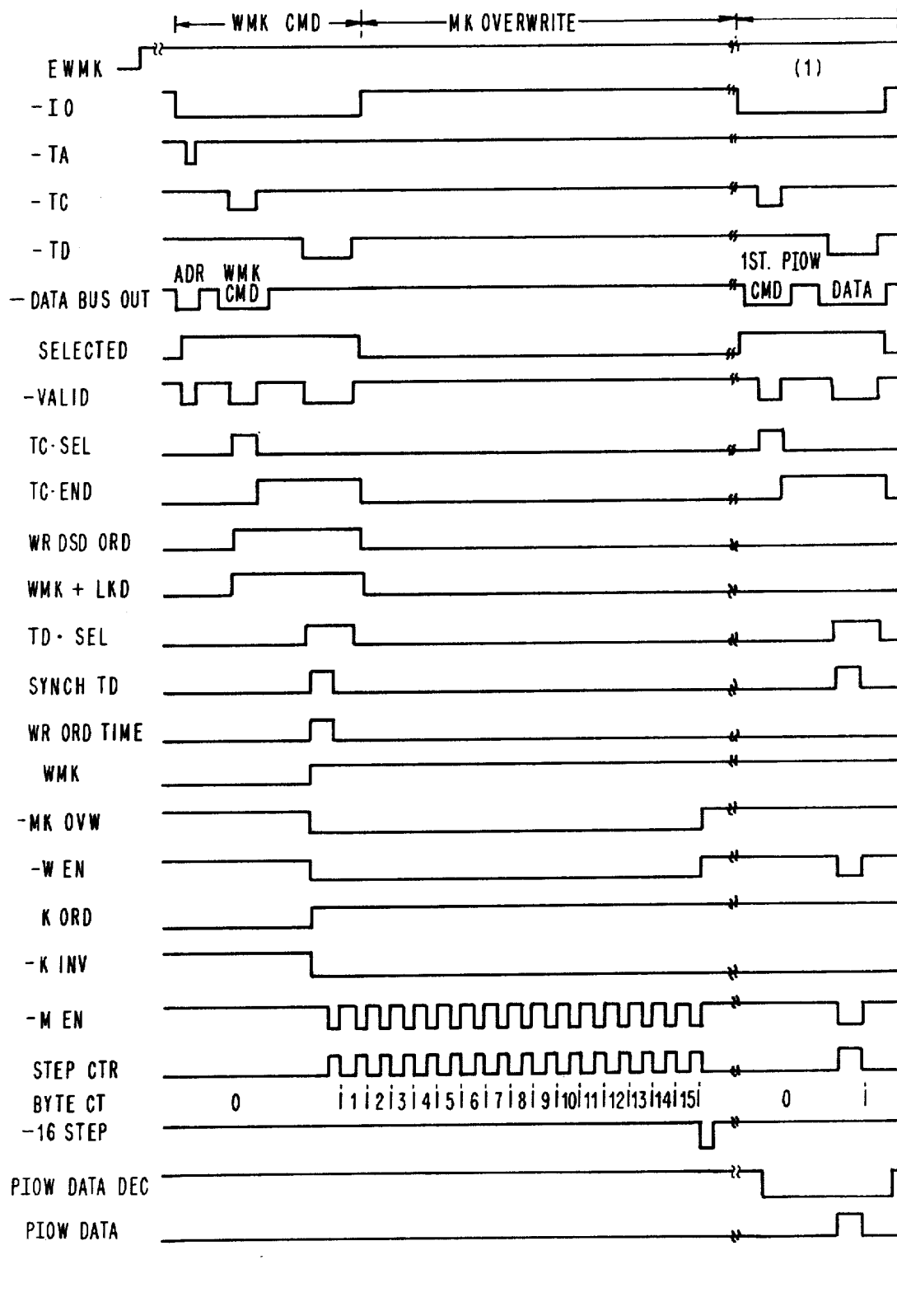


FIG. 24 A FIG. 24 B

FIG. 24

FIG. 24A

WMK BY PIOW CMDS



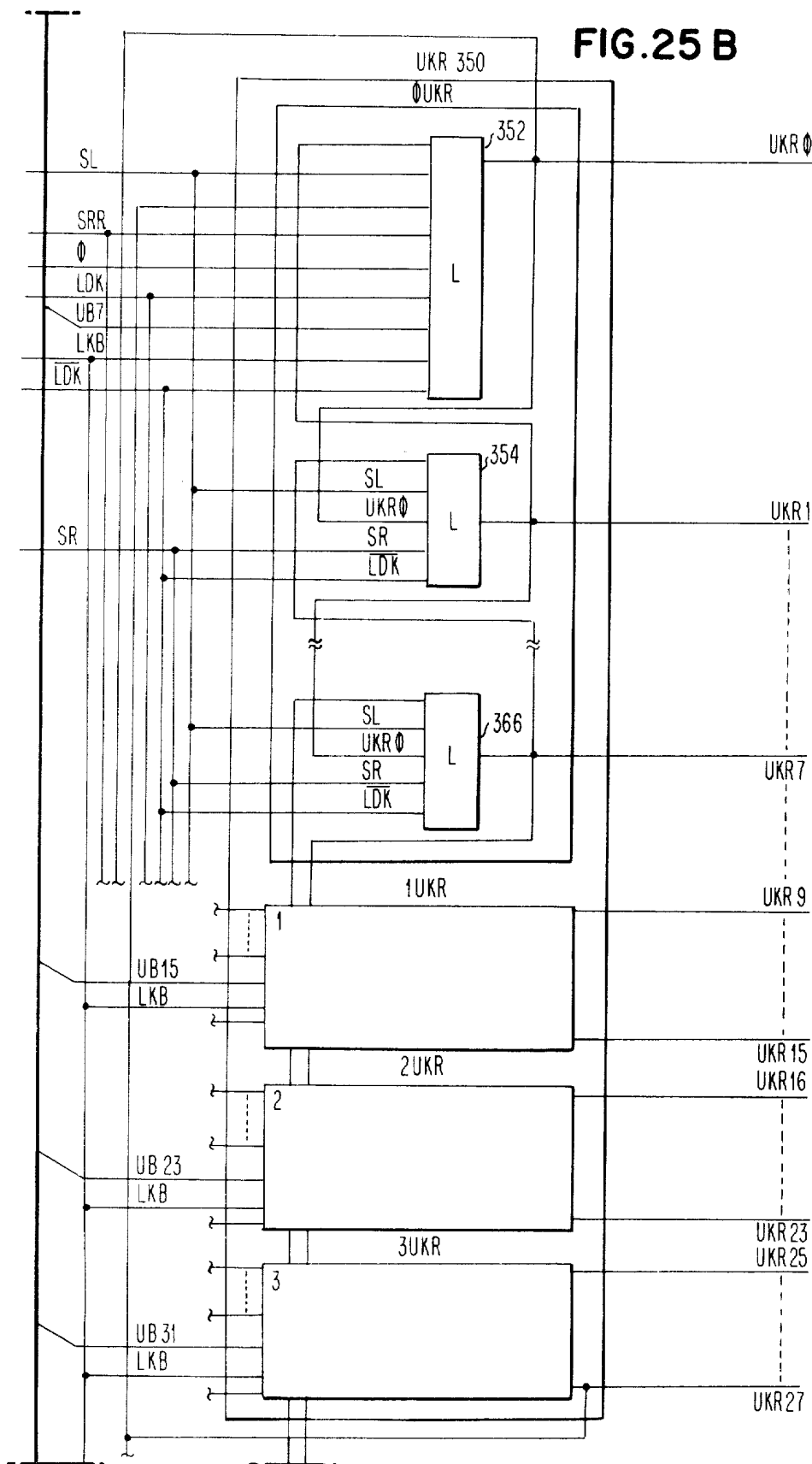
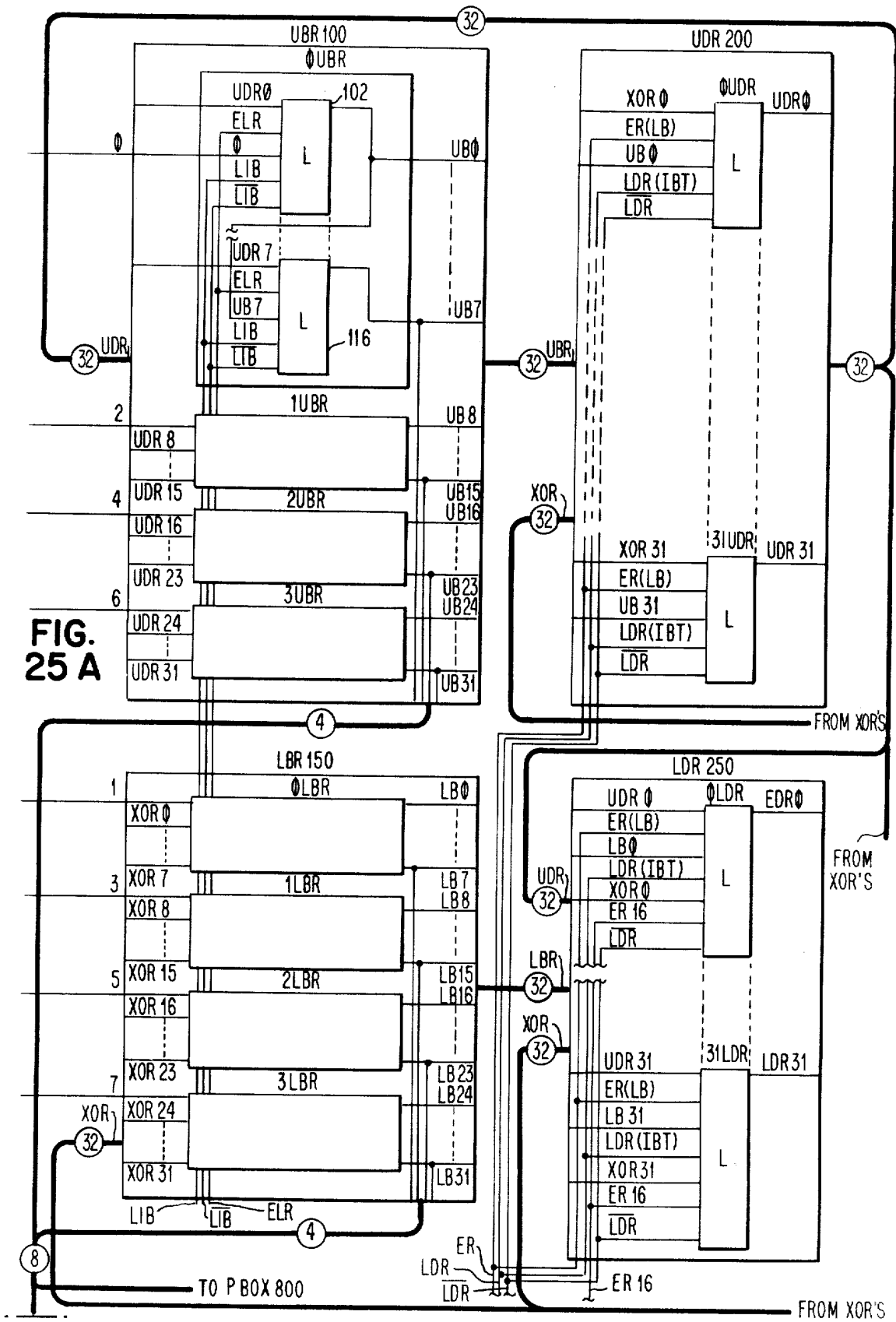


FIG. 25

FIG. 25 A

FIG. 25 B

FIG. 25 C



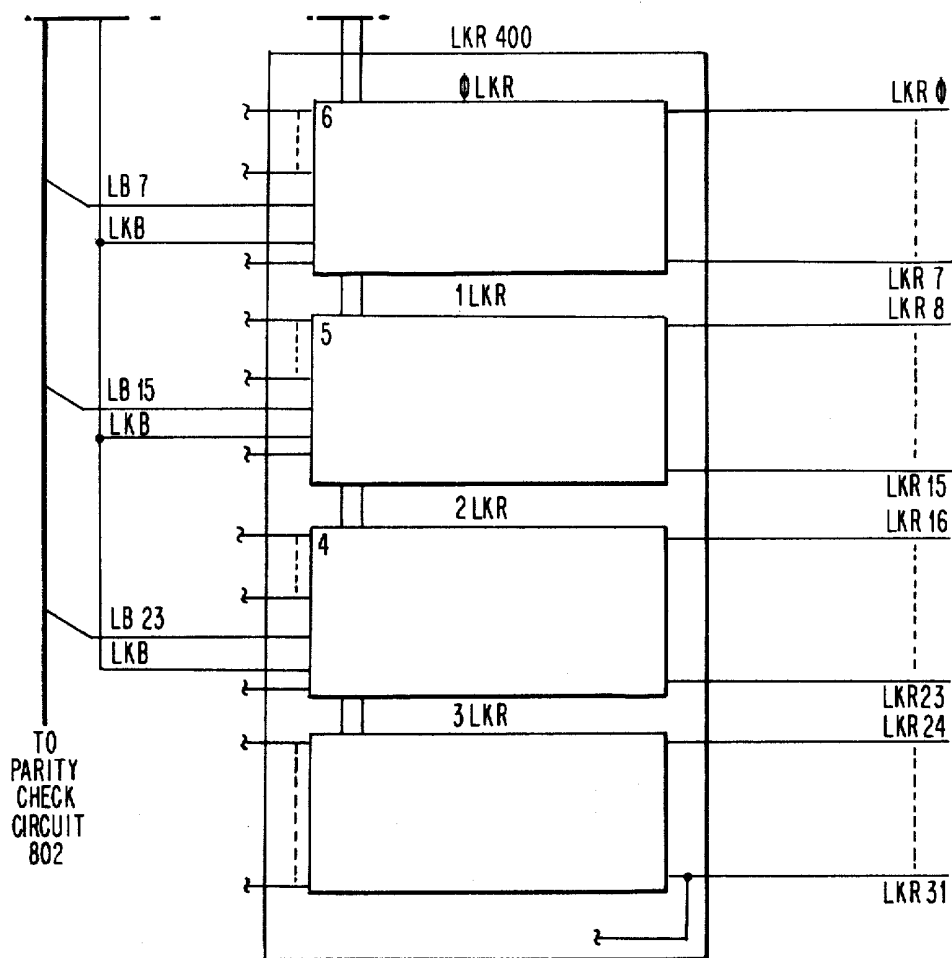


FIG. 25C

FIG. 26C

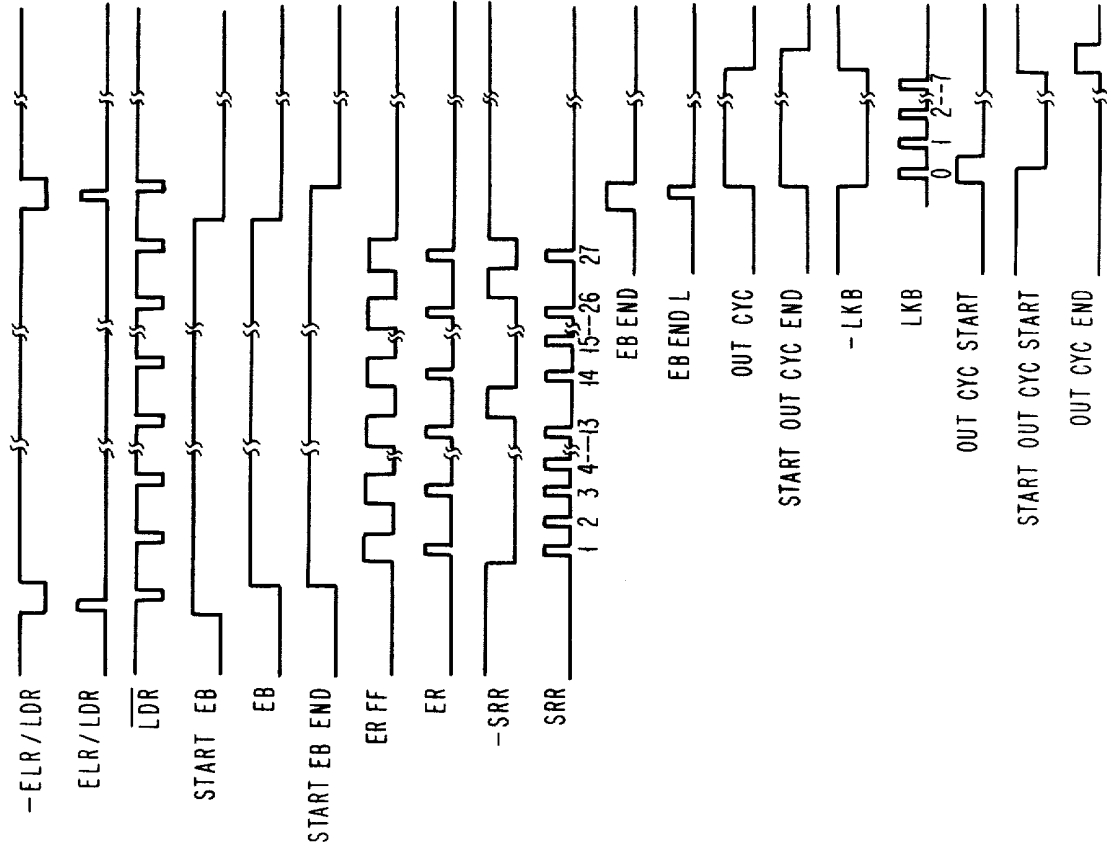
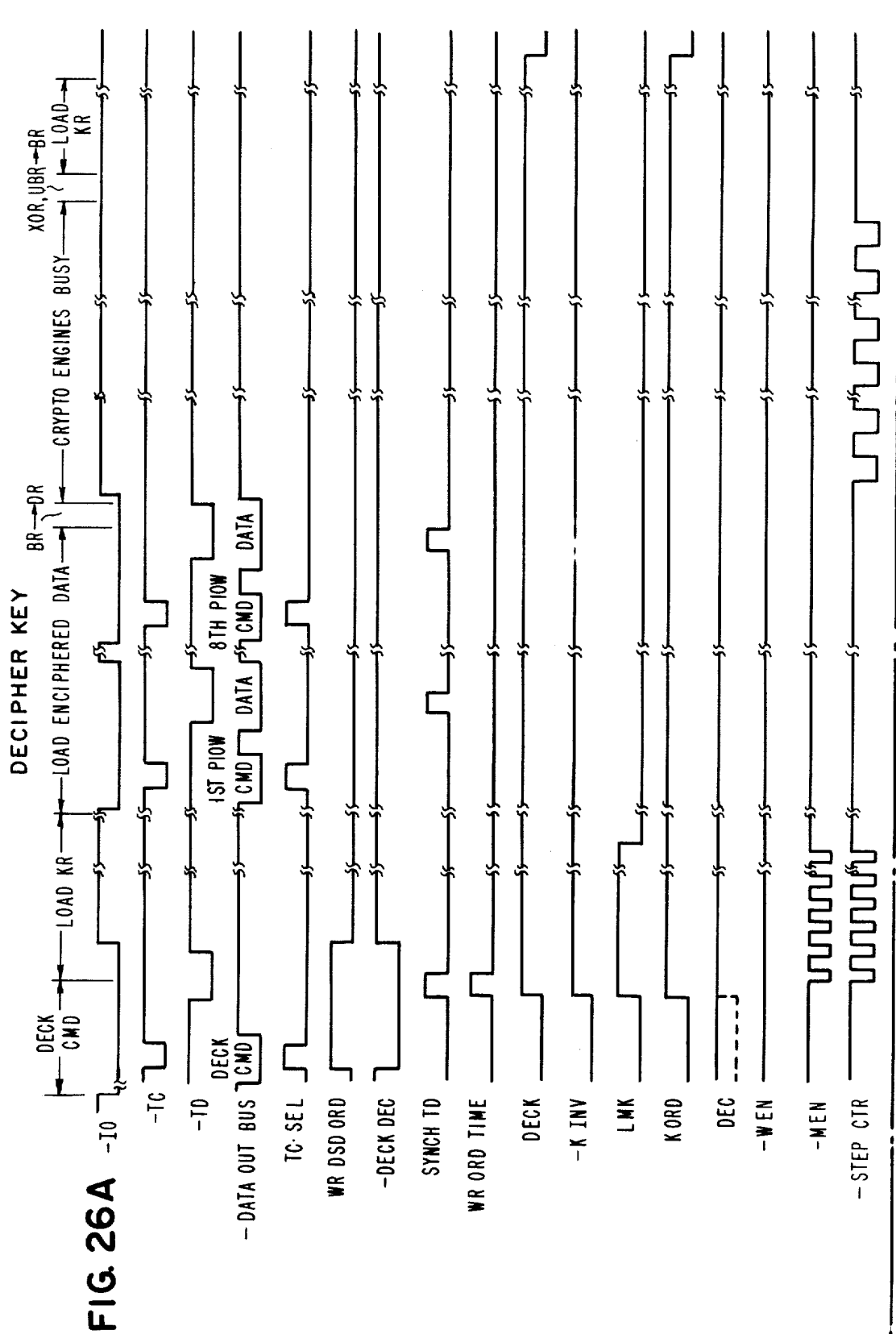


FIG. 26

FIG. 26A
FIG. 26B
FIG. 26C



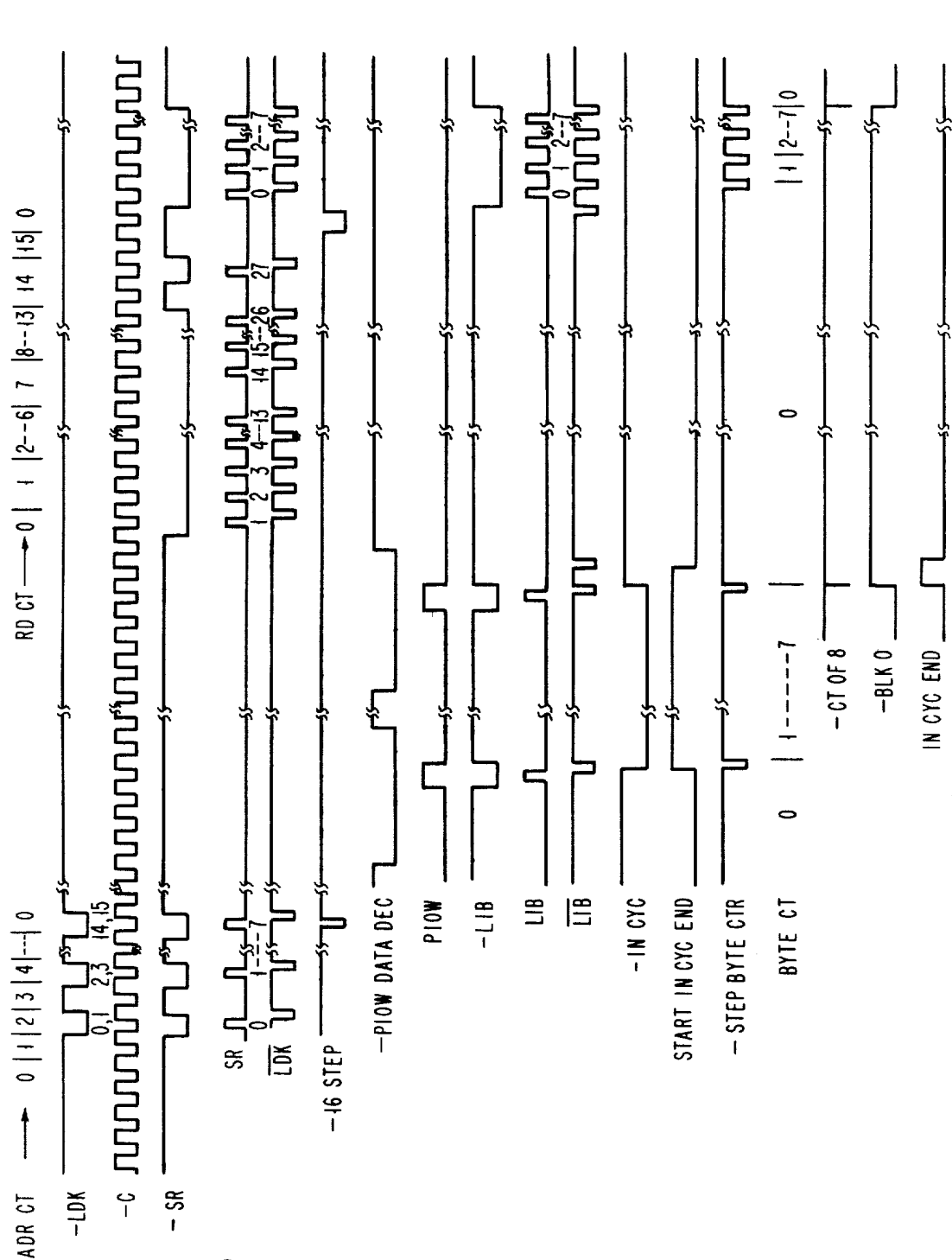


FIG. 27C

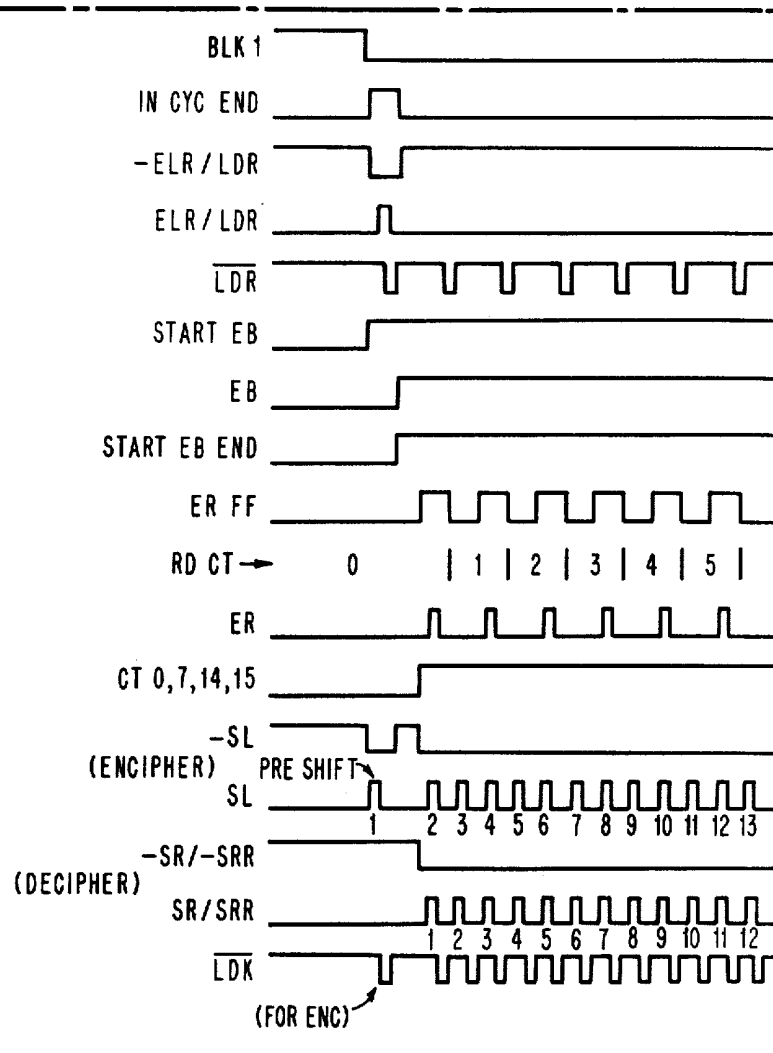


FIG. 27

FIG. 27A	FIG. 27B
FIG. 27C	FIG. 27D

FIG. 27A

DECIPHER / ENCIPHER

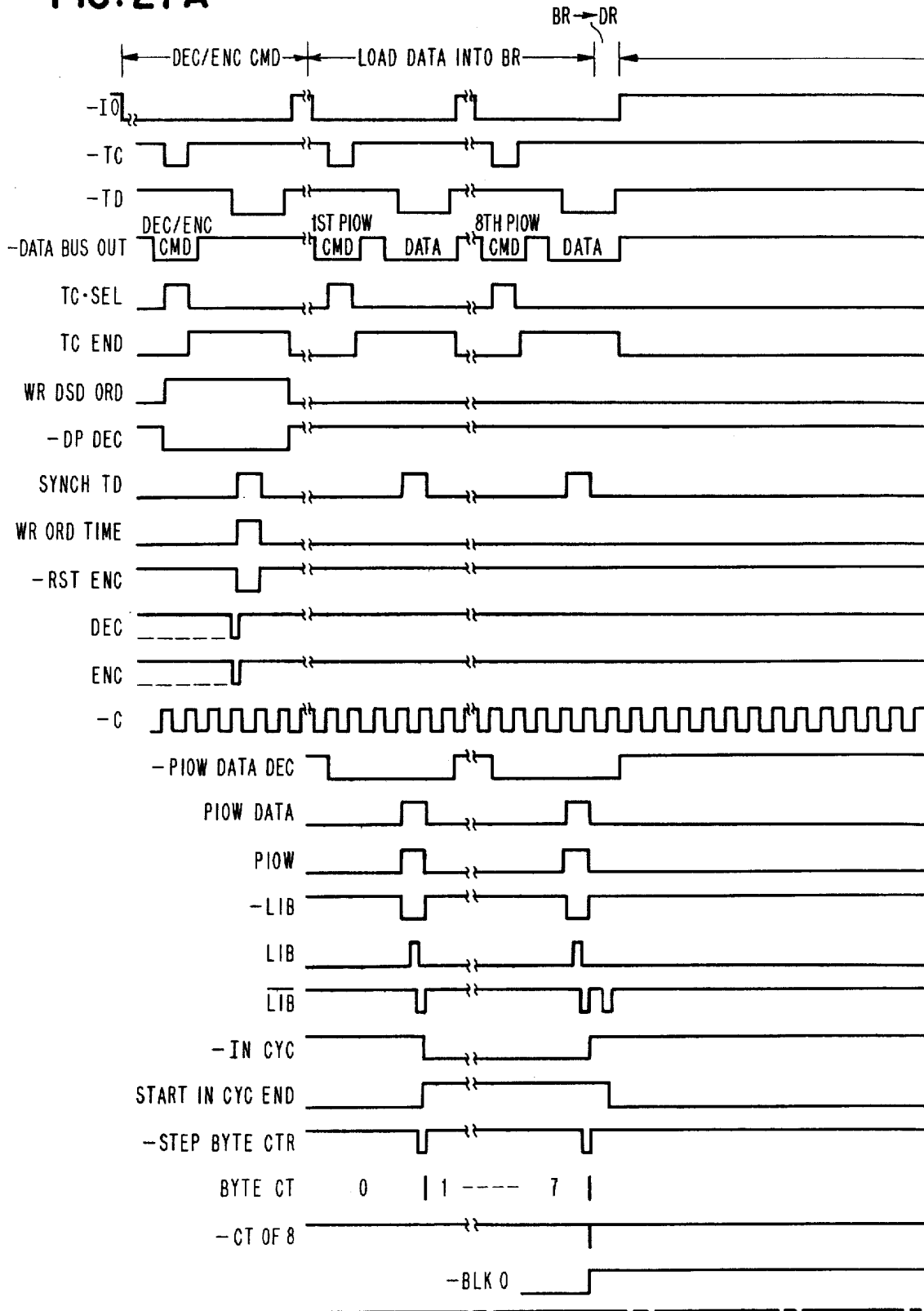
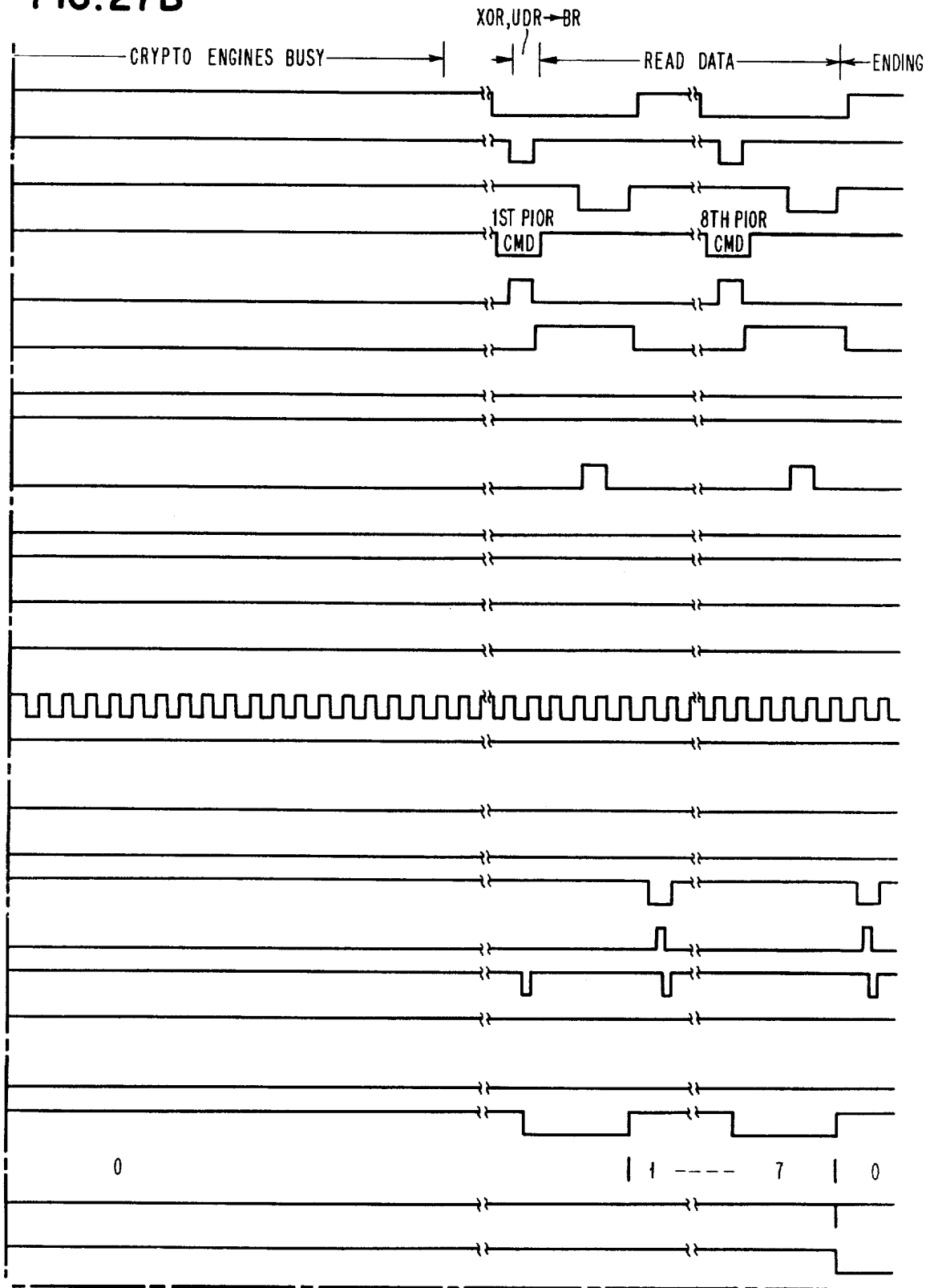
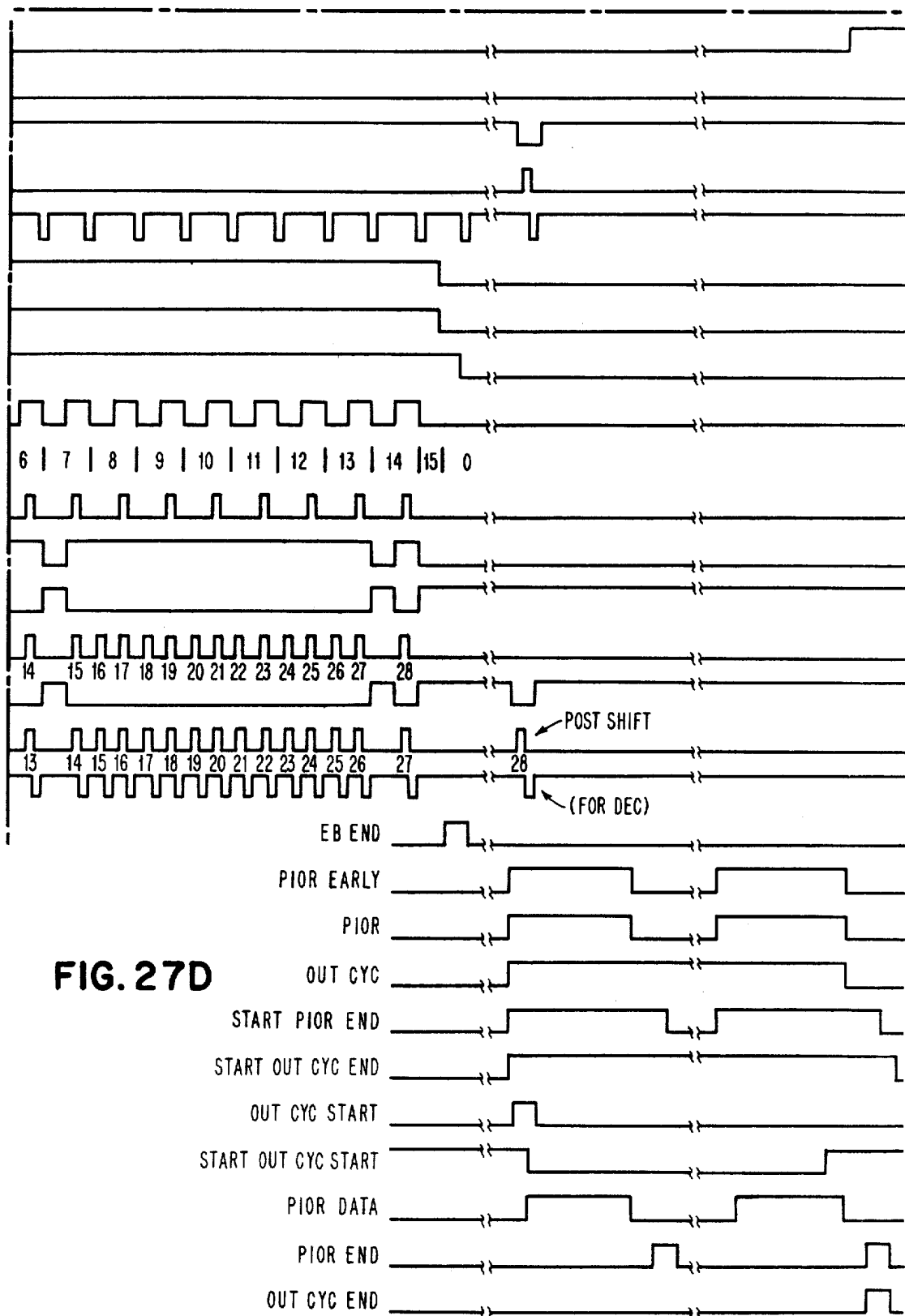


FIG. 27B

DECIPHER / ENCIPHER





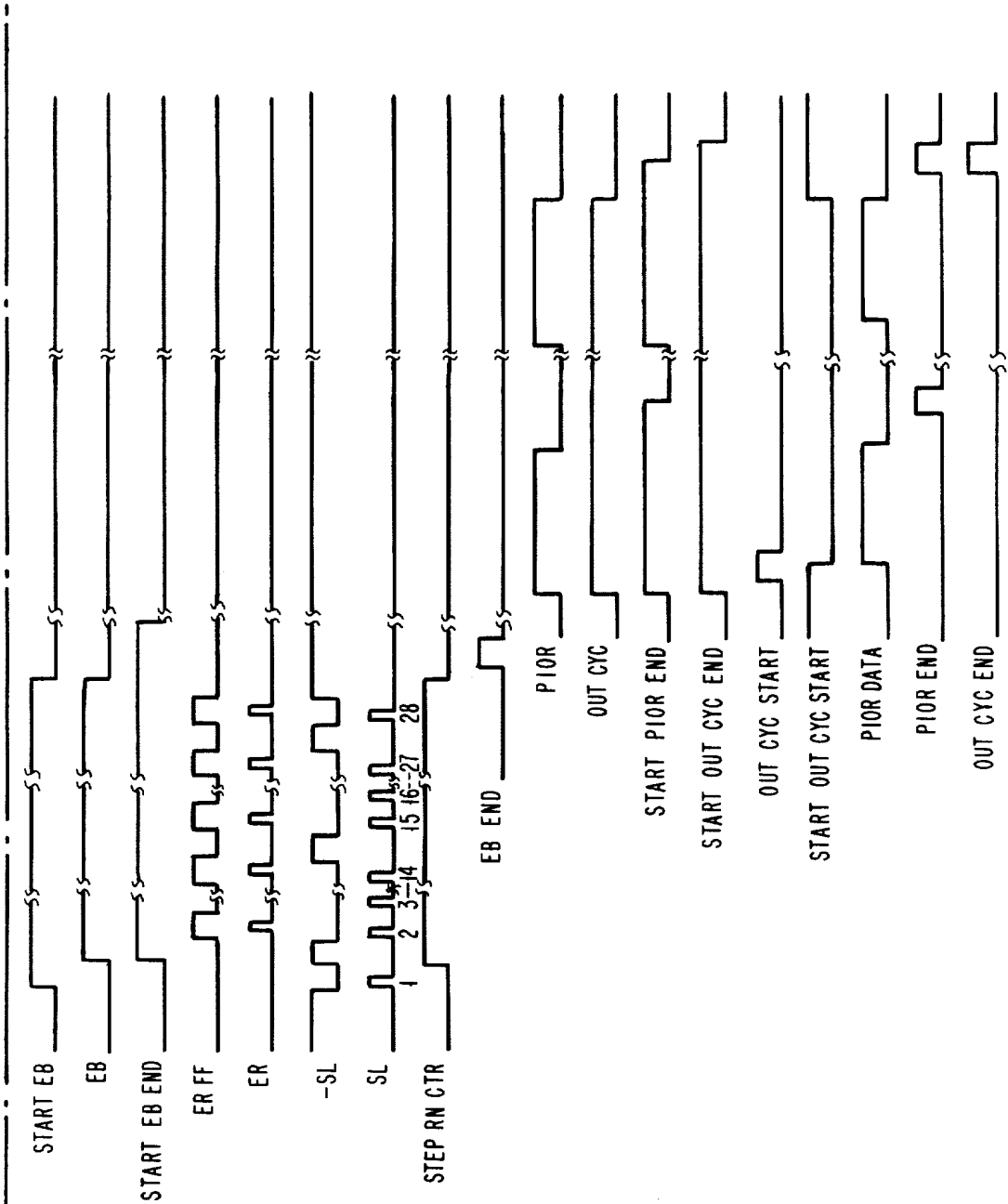
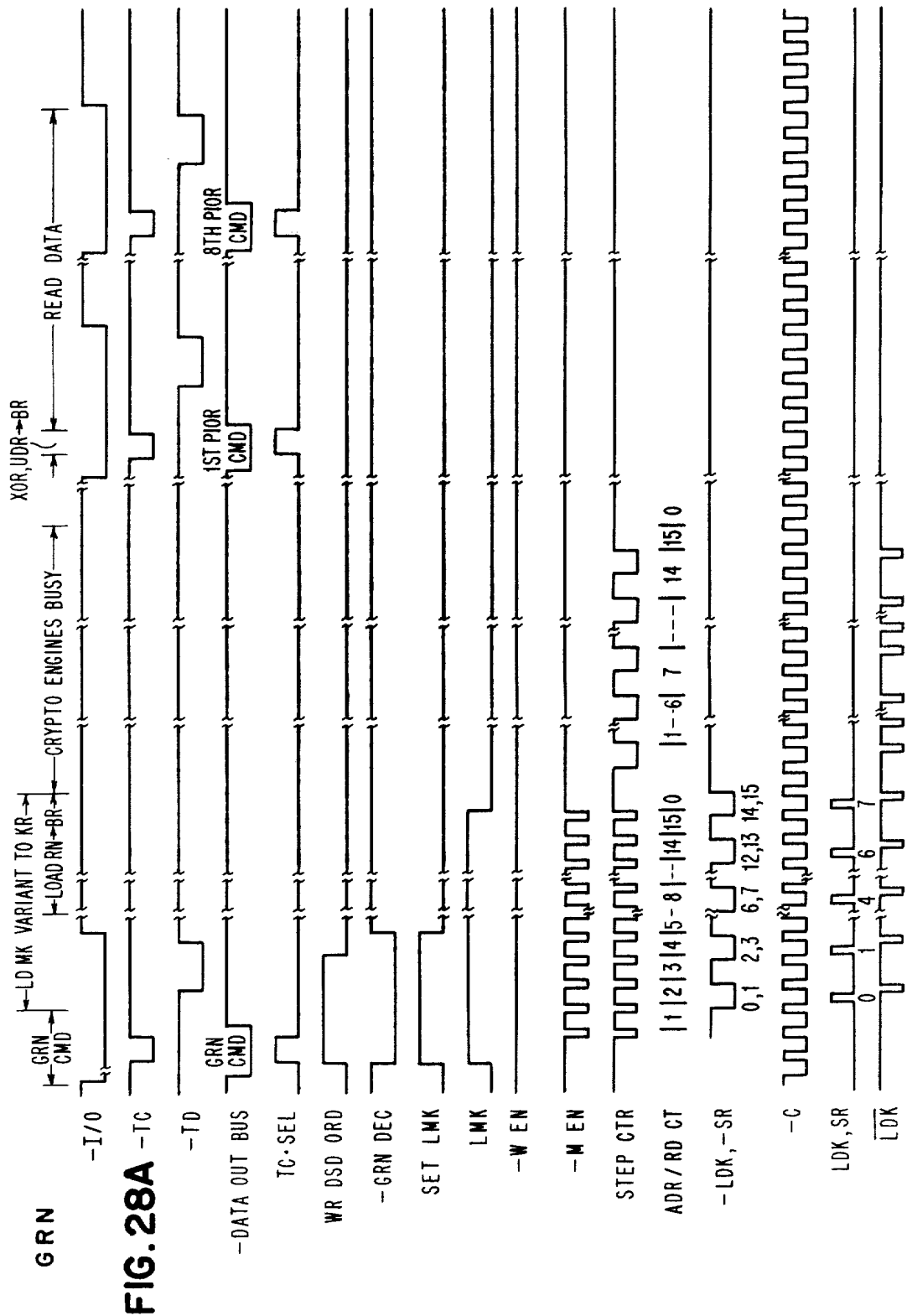


FIG. 28C

FIG. 28

FIG. 28 A
FIG. 28 B
FIG. 28 C



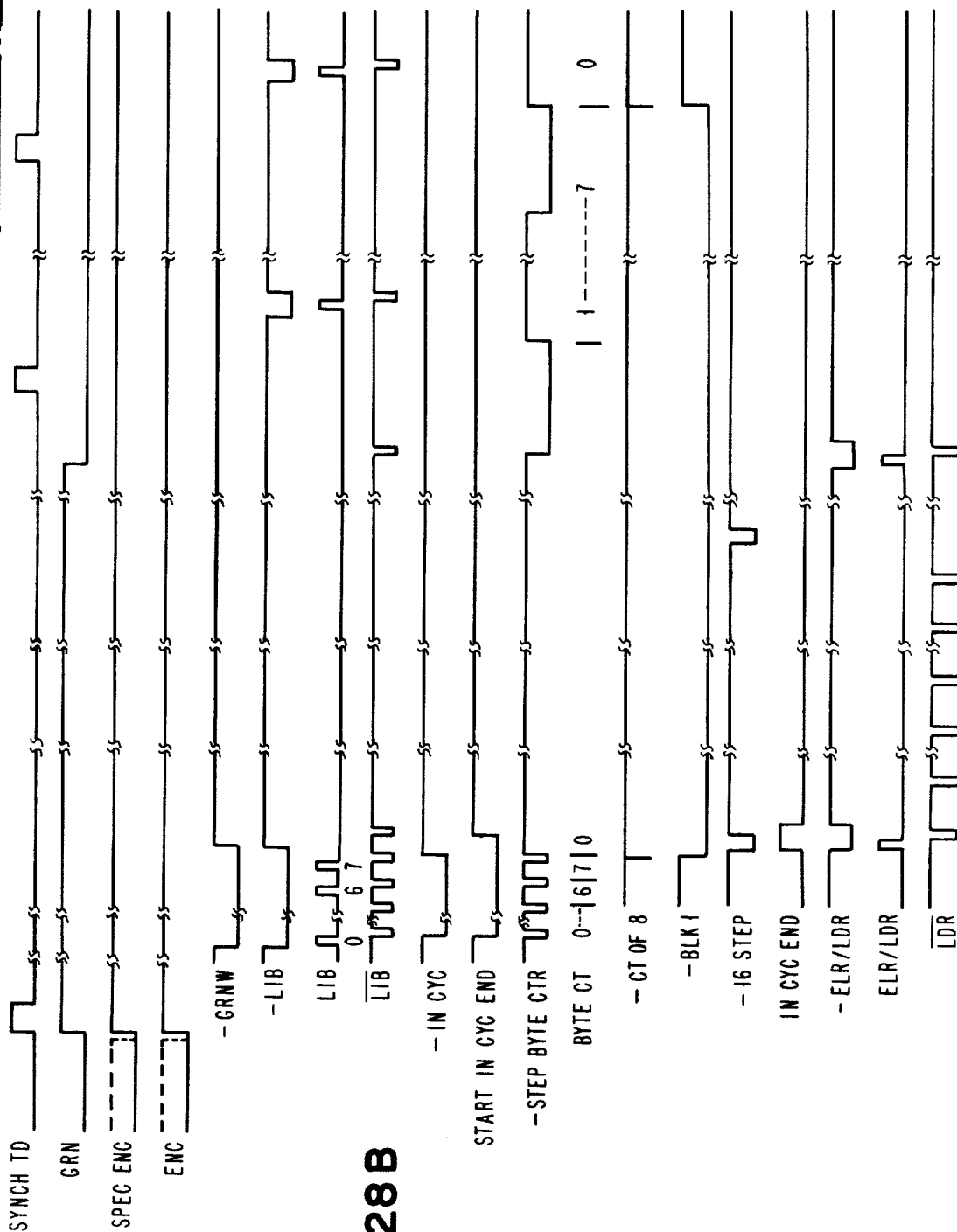
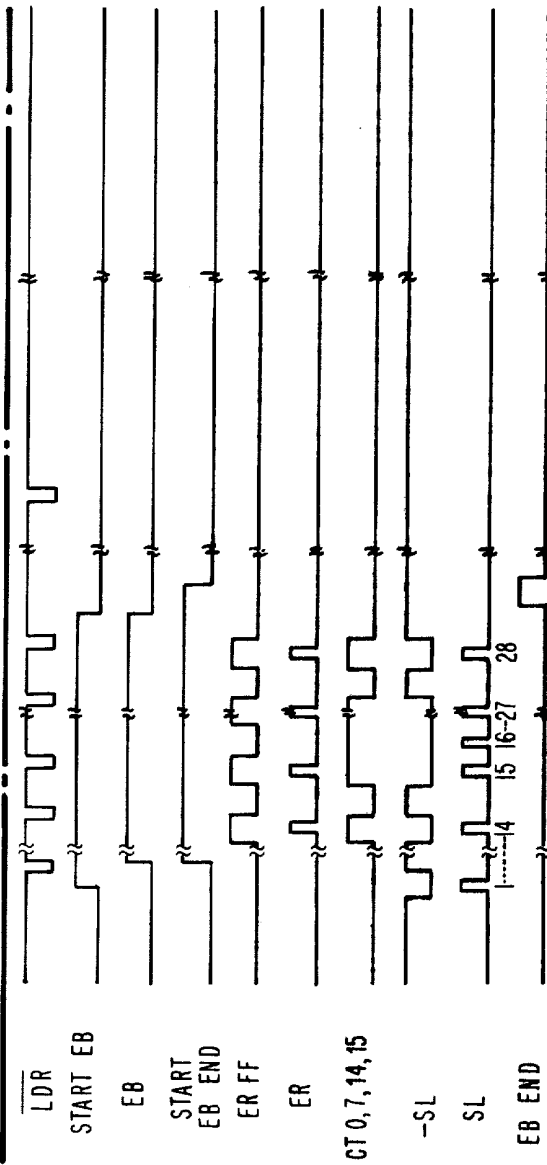


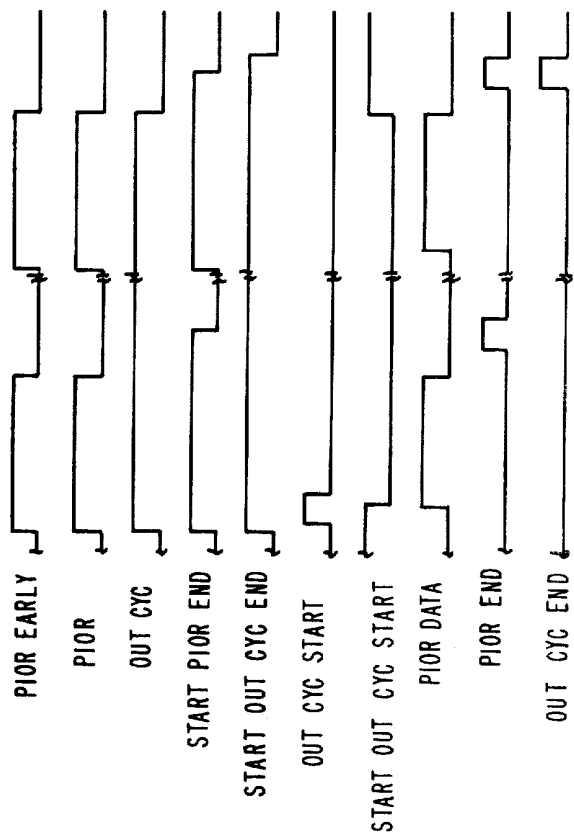
FIG. 29C



ENCIPHER MASTER KEY

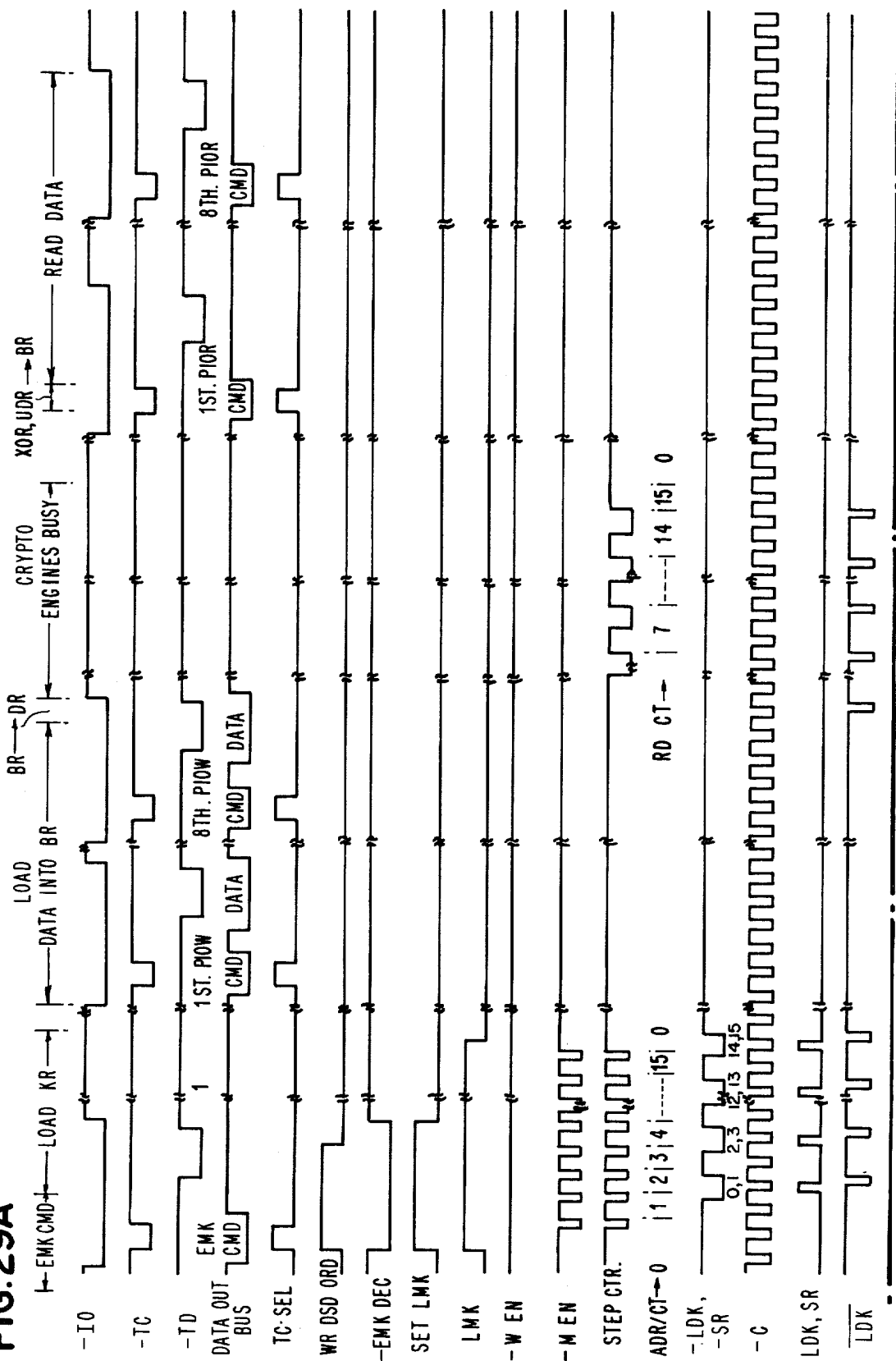
FIG. 29

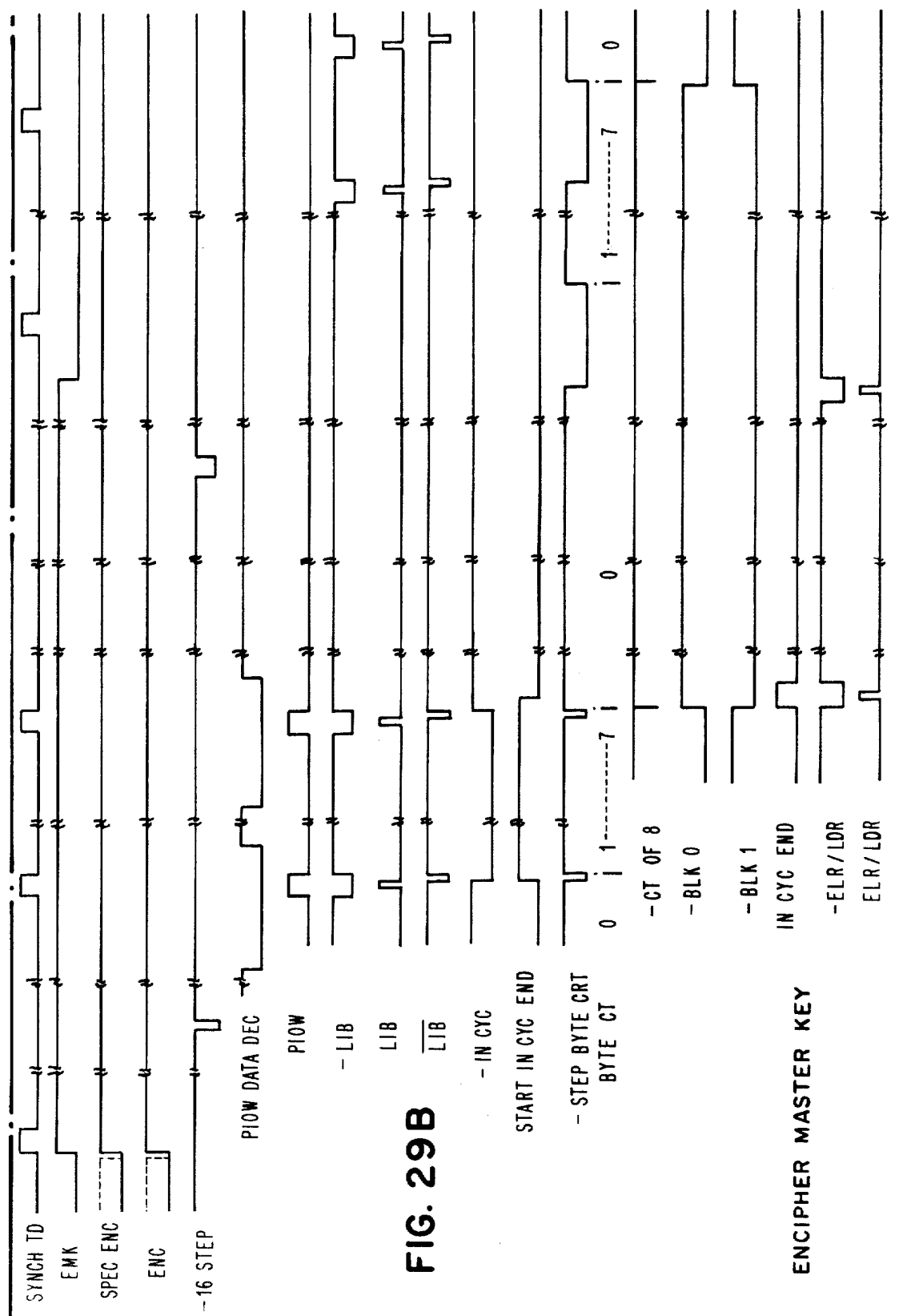
FIG. 29A
FIG. 29B
FIG. 29C



ENCIPHER MASTER KEY

FIG. 29A





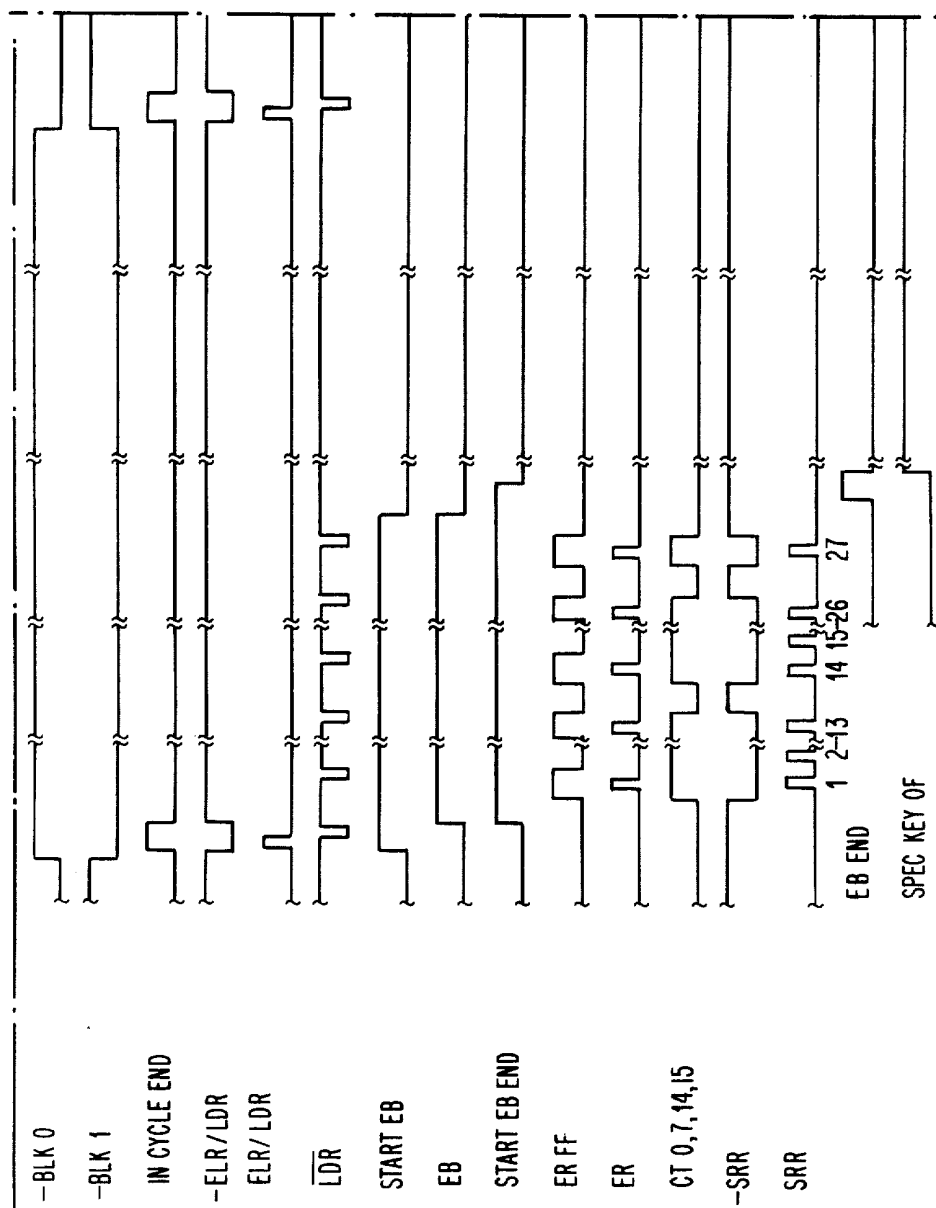


FIG. 30E

FIG. 30

FIG. 30A	FIG. 30B
FIG. 30C	FIG. 30D
FIG. 30E	FIG. 30F
	FIG. 30G

REENCIPHER FROM MASTER KEY (RFMK)

FIG. 30A

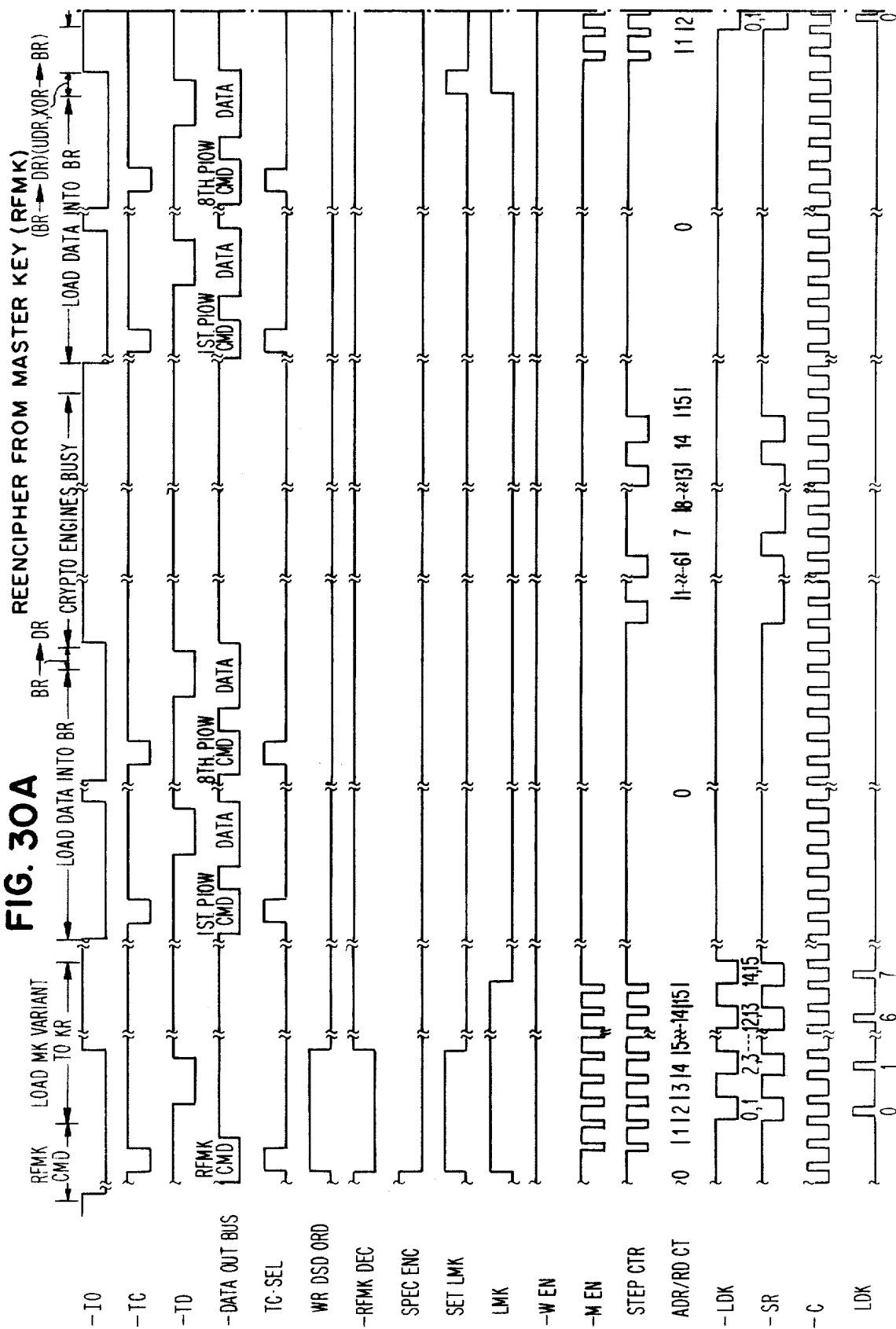
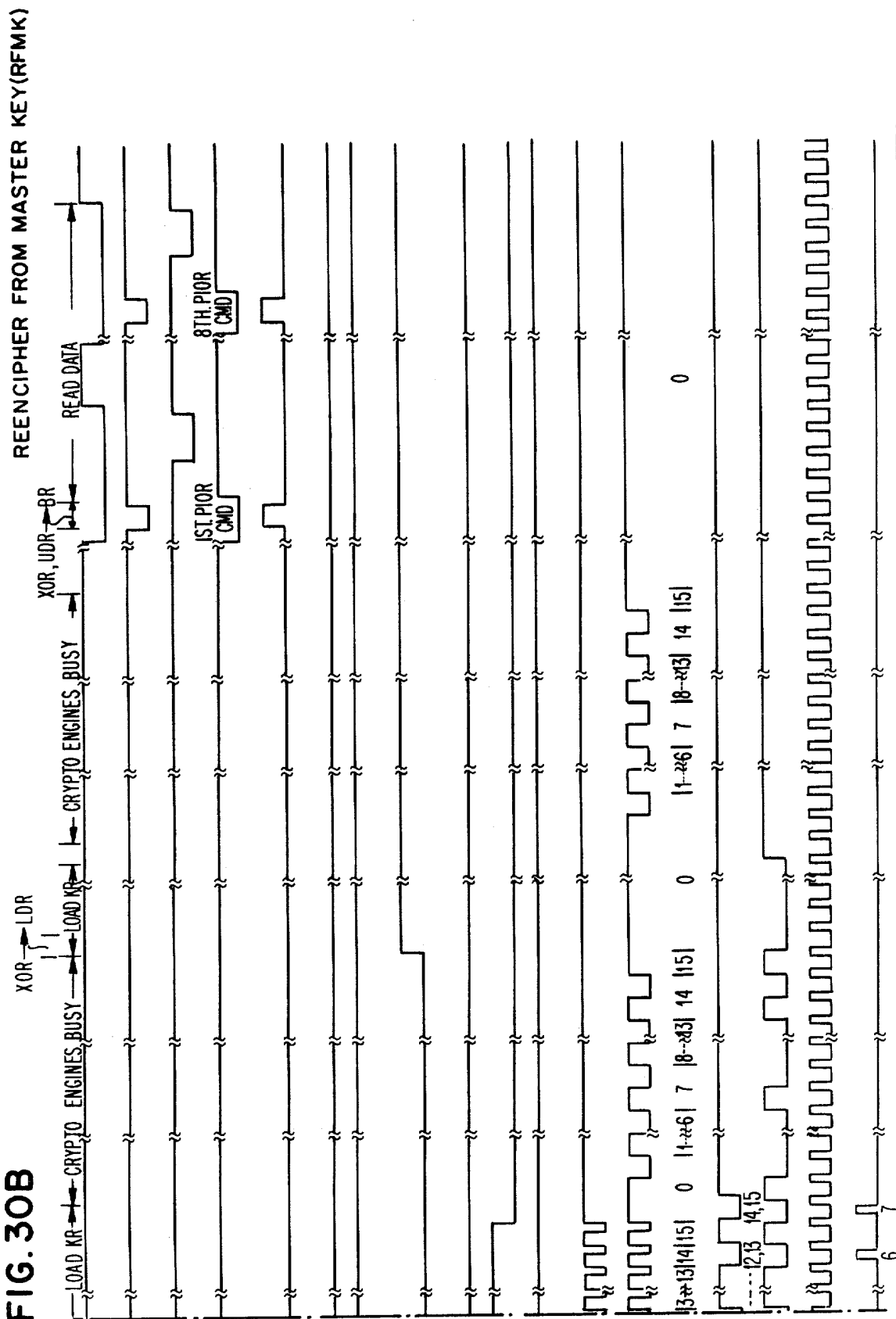
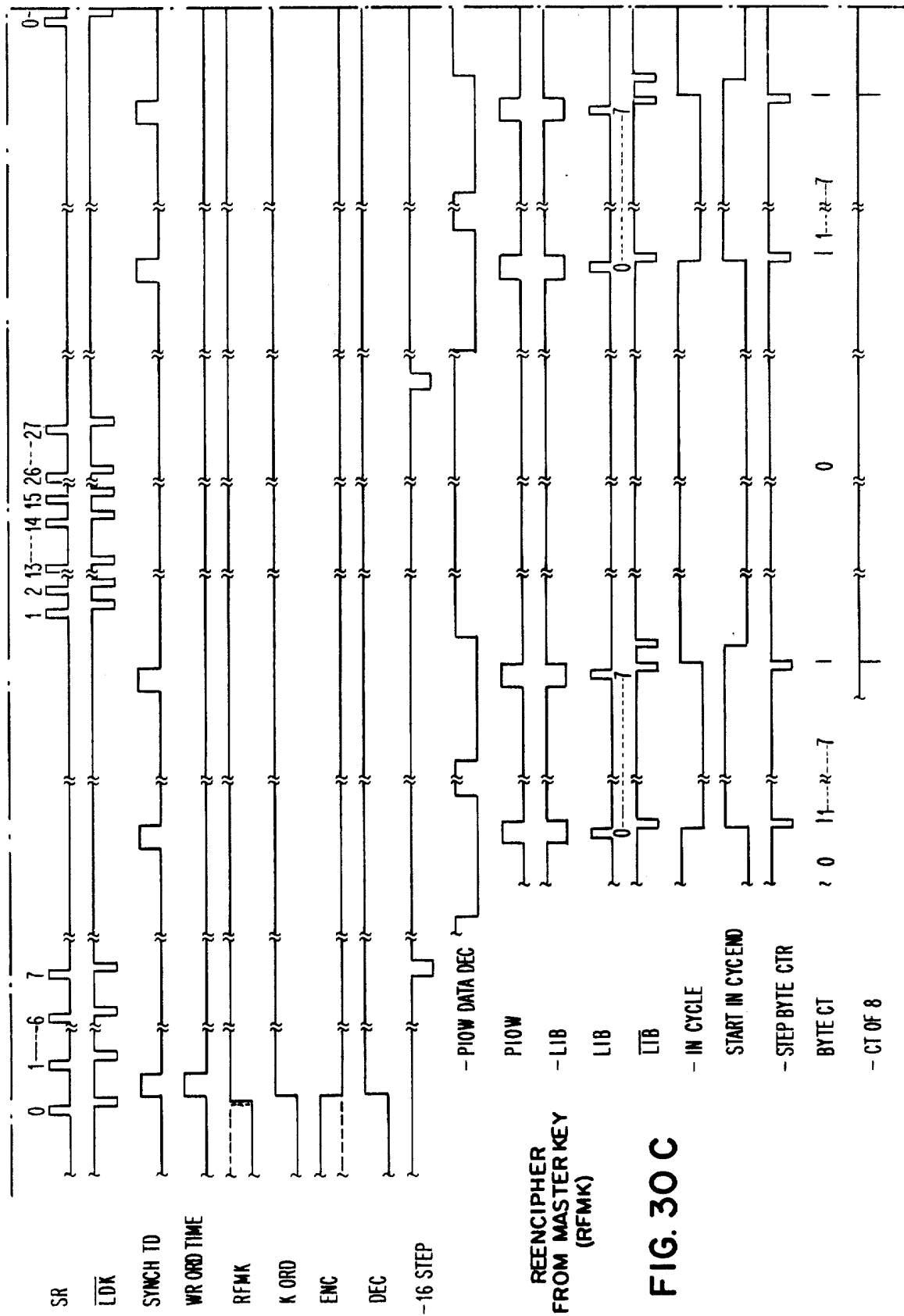
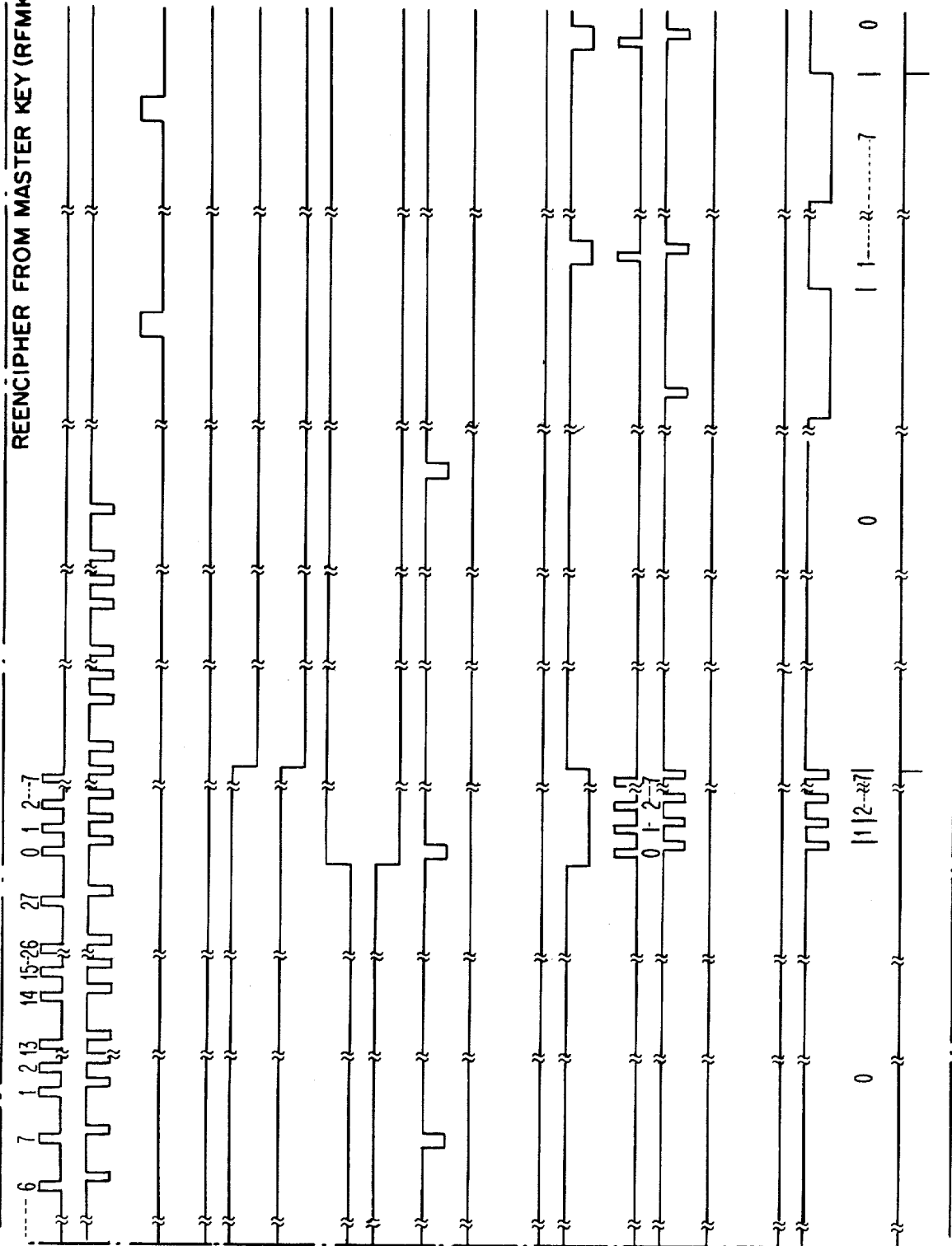


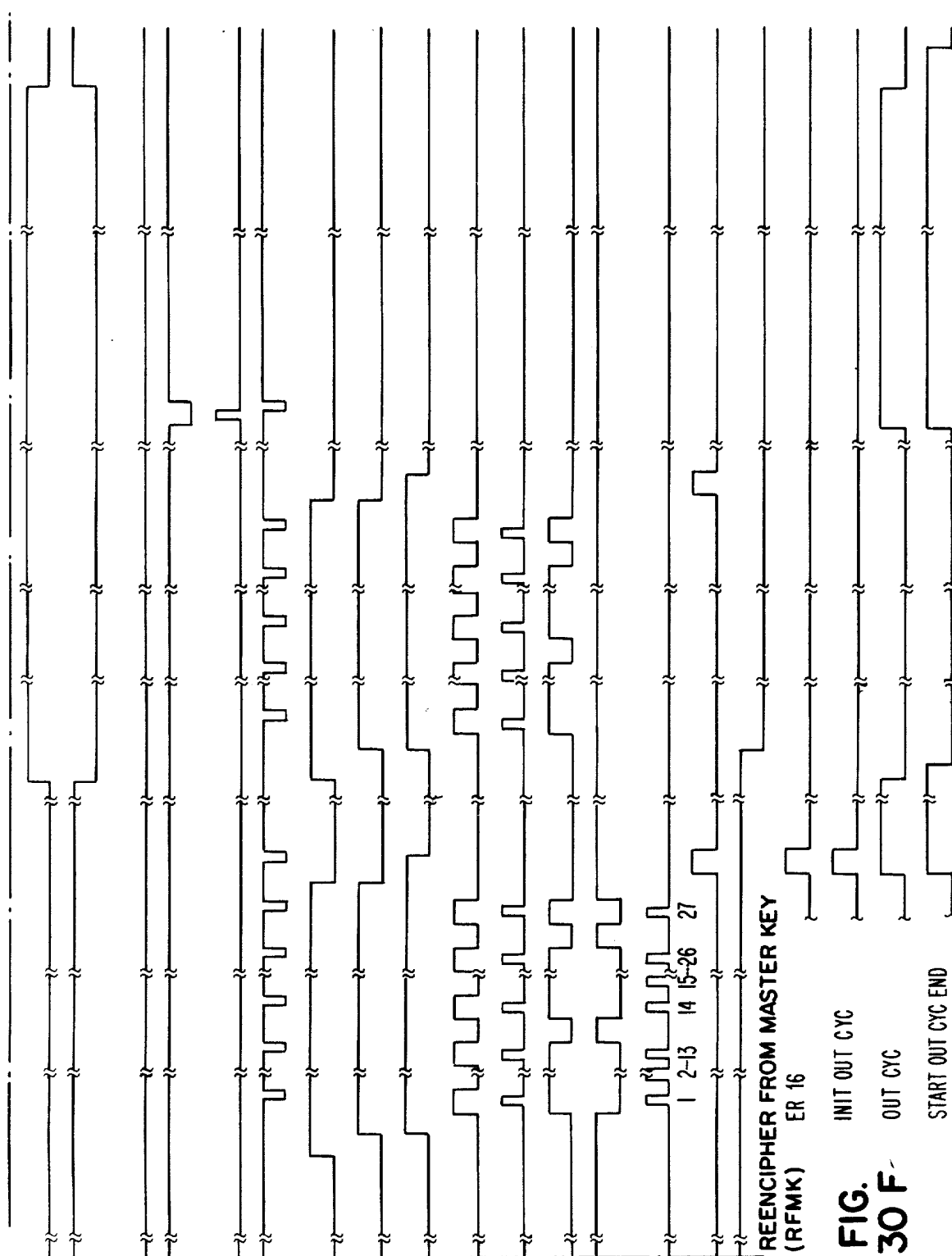
FIG. 30B

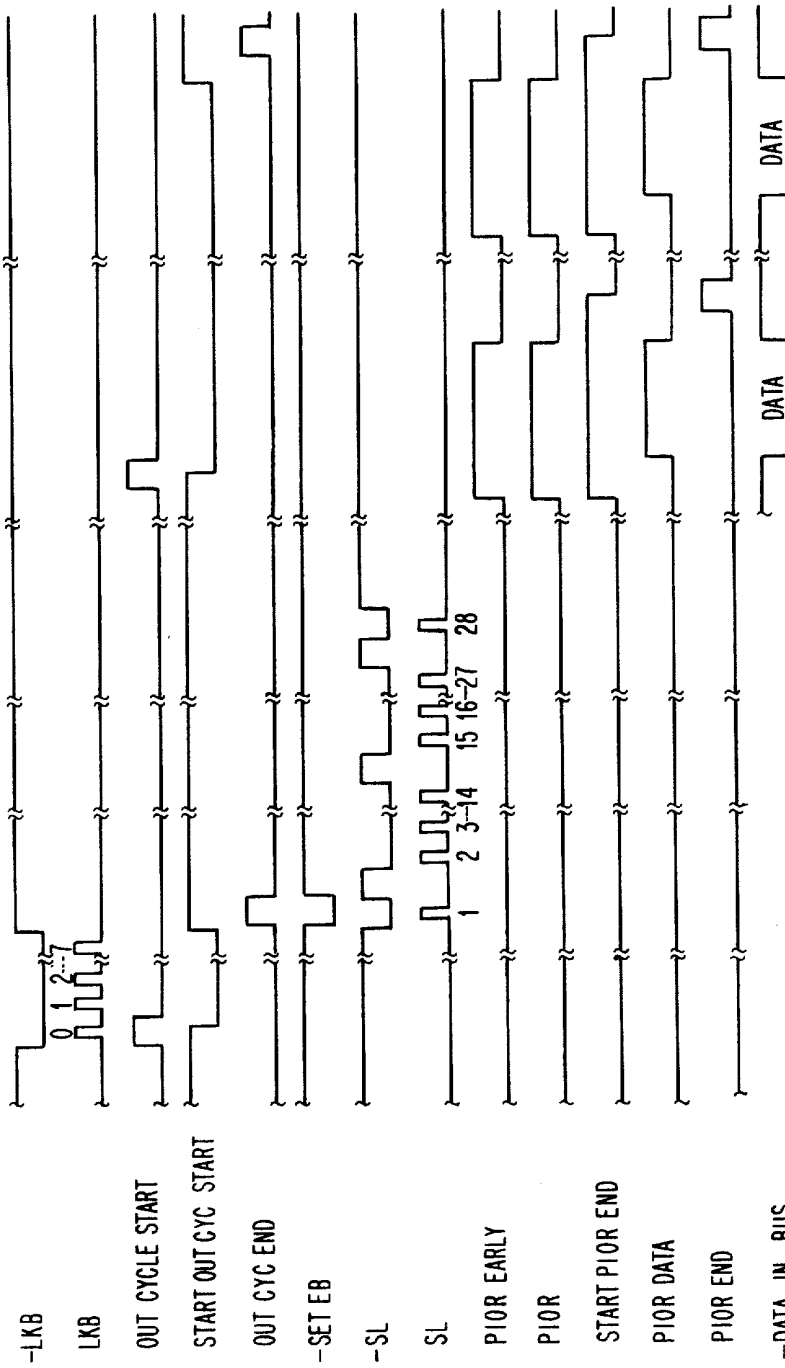




REENCIPHER FROM MASTER KEY (RFMK)







REENCIPHER FROM MASTER KEY (RFMK)

FIG. 30G

CRYPTOGRAPHIC COMMUNICATION SECURITY FOR SINGLE DOMAIN NETWORKS

CROSS REFERENCE TO RELATED APPLICATIONS

This application is related to the following patent applications which are concurrently filed herewith and assigned to the same assignee as the present application:

1. "Cryptographic Communication and File Security Using Terminals", Ser. No. 857,533, filed Dec. 5, 1977, by Ehrsam et al.
2. "Cryptographic File Security for Single Domain Networks", Ser. No. 857,534, filed Dec. 5, 1977, by Ehrsam et al.
3. "Cryptographic Communication and File Security for Multiple Domain Networks", Ser. No. 857,531, filed Dec. 5, 1977, by Ehrsam et al.
4. "Cryptographic File Security for Multiple Domain Networks", Ser. No. 857,535, filed Dec. 5, 1977, by Ehrsam et al.
5. "Cryptographic Verification of Operational Keys Used in Communication Networks", Ser. No. 857,546, filed Dec. 5, 1977, by Lennon et al.

BACKGROUND OF THE INVENTION

This invention relates to cryptographic communication security techniques in a single domain network and, more particularly, to a single domain network which includes a host and communication terminals each having a data security device which performs enciphering and deciphering operations using system or private keys to permit cryptographic communication security in a data processing network.

With the increasing number of computer end users, sharing of common system resources such as files, programs and hardware and the increasing use of distributed systems and telecommunications, larger and more complex computer base information systems are being created. In such systems, an increasing amount of sensitive data may be transmitted across unsecure communication lines. Because of the insecurity of communication lines, there is an increasing concern over the interception or alteration of sensitive data which must pass outside a controlled or protected environment or which may become accessible if maintained for too long a period of time. Cryptography has been recognized as an effective data security measure in that it protects the data itself rather than the medium over which it is transmitted or the media on which it is stored.

Cryptography deals with methods by which message data called cleartext or plaintext is encrypted or enciphered into unintelligible data called ciphertext and by which the ciphertext is decrypted or deciphered back into the plaintext. The encipherment/decipherment transformations are carried out by a cipher function or algorithm controlled in accordance with a cryptographic or cipher key. The cipher key selects one out of many possible relationships between the plaintext and the ciphertext. Various algorithms have been developed in the prior art for improving data security in data processing systems. Examples of such algorithms are described in U.S. Pat. No. 3,796,830 issued Mar. 12, 1974 and U.S. Pat. No. 3,798,359 issued Mar. 19, 1974. Another more recent algorithm providing data security in data processing systems is described in U.S. Pat. No. 3,958,081 issued May 18, 1976. This algorithm was

adopted by the National Bureau of Standards as a data encryption standard (DES) algorithm and is described in detail in the Federal Information Processing Standards publication, Jan. 15, 1977, FIPS PUB 46.

A data communication network may include a complex of communication terminals connected via communication lines to a single host system and its associated resources such as the host programs and locally attached terminals and data files. Within the data communication network, the domain of the host system is considered to be the set of resources known to and managed by the host system. Various single domain data communication networks have been developed in the prior art using cryptographic techniques for improving the security of data communication within the network. In such networks, a cryptographic facility is provided at the host system and at various ones of the remote terminals. In order for the host system and a remote terminal to perform a cryptographic communication, both must use the same cryptographic algorithm and a common operational cryptographic key so that the data enciphered by the sending station can be deciphered at the receiving station. In prior art cryptographic communication arrangements, the operational key to be used at the sending station is communicated by mail, telephone or courier to the receiving station so that a common operational key is installed at both stations to permit the cryptographic communications to be performed. Furthermore, the operational key was kept for a relatively long period of time. In order to present a "moving target" to an opponent, other prior art arrangements developed techniques which improved security by changing operational keys dynamically where the frequency of changing keys is done automatically by the system. One such technique is provided in the IBM 3600 Finance Communication System utilizing the IBM 3614 consumer transaction facility as remote terminals and is exemplified by U.S. Pat. No. 3,956,615 issued May 11, 1976. In that system, an enciphered operational or data encrypting key is transmitted over the communication line from the host system to the remote communication terminal. The enciphered data encrypting key is deciphered and then used as the current data encrypting key for all data transmissions. However, with this type of arrangement, since the current data encrypting key must be readily available for the data transmissions it is stored in the clear at the remote terminal thereby making the system somewhat unsecure by the clear keys being susceptible to possible accessibility by unauthorized personnel. Additionally, with this type of system, when the current data encrypting key is to be changed, a new data encrypting key enciphered under the old data encrypting key is transmitted to the remote terminal where it is deciphered and then used as the new current data encrypting key. However, with this type of arrangement, since each new current data encrypting key is a function of the preceeding current data encrypting key, the system becomes unsecure if one current data encrypting key becomes accessible as it will permit the current ciphertext to be deciphered and will permit all succeeding data encrypting keys to be obtained thereby allowing all succeeding ciphertext to be deciphered.

Accordingly, it is an object of the invention to maintain the security of data transmissions in a data communication network.

Another object of the invention is to provide a host system having a data security device for enciphering/deciphering message blocks of data under control of a protected host cryptographic key.

A further object of the invention is to provide a host cryptographic facility in a data communication network without having to provide host cryptographic keys in the clear outside of the facility.

Still another object of the invention is to establish cryptographic communication sessions between a terminal and a host system in a data communication network in a secure manner.

Still a further object of the invention is to provide a common operational key for a terminal and the host in a data communication network to permit enciphering/deciphering operations to be performed using the common operational key.

Still another object of the invention is to dynamically create a common operational key by generating a pseudo random number defined as an enciphered operational key.

Still a further object of the invention is to create secondary communication keys for the secure terminals associated with the data communication network by generating pseudo random numbers each being defined as a secondary communication key.

Still another object of the invention is to maintain the security of secondary communication keys by enciphering them under a variant of the host master key.

Still a further object of the invention is to reencipher the enciphered operational key to an operational key enciphered under the secondary communication key.

Still another object of the invention is to provide the reenciphered operational key to the terminal with which a communication session is desired.

Still a further object of the invention is to dynamically create a different operational key for each new communication session between the host and a terminal in the data communication network.

Still another object of the invention is to provide a host cryptographic facility which is maintained in a logically and physically protected area.

Still a further object of the invention is to provide a host data security device which includes a hardware implementation of the data encryption standard algorithm adopted as the United States Federal Data Processing Standard.

Still another object of the invention is to provide a host data security device having interfaces to which plaintext/ciphertext input data and operation requests are presented and from which ciphertext/plaintext output data is presented.

Still a further object of the invention is to provide a host cryptographic facility which includes cryptographic apparatus, a host master cryptographic key memory and a working key register whereby the contents of the host master key memory, the working key register and intermediate results of the cryptographic operation are only accessible to the cryptographic apparatus.

Still another object of the invention is to provide a host cryptographic facility for performing a write master key function to selectively store a host cryptographic key used for encrypting/decrypting other cryptographic keys in a master key memory by manual or host control means.

Still a further object of the invention is to provide a host cryptographic facility having a battery powered

host master key memory to allow host master key retention when system power is not present.

Still another object of the invention is to provide a host cryptographic facility for performing a host master key overwrite function whenever a new host master key is to be used by the facility.

Still a further object of the invention is to provide a host cryptographic facility having a working key register for storing a host cryptographic key used to personalize the encrypting/decrypting operation of the host cryptographic facility.

Still another object of the invention is to provide a host cryptographic facility for performing a decipher key function to decipher a data encrypting key enciphered under a host master key to obtain the data encrypting key in clear form for storage in a working key register.

Still a further object of the invention is to provide a host cryptographic facility for performing an encipher function for enciphering input plaintext under control of a data encrypting key stored in a working key register to produce output ciphertext.

Still another object of the invention is to provide a host cryptographic facility for performing a decipher function for deciphering input ciphertext under control of a data encrypting key stored in a working key register to produce output plaintext.

Still another object of the invention is to provide a host cryptographic facility for performing a decipher function for deciphering a data encrypting key enciphered under a host master key to obtain the data encrypting key in clear form within the facility for use in enciphering input cleartext into output ciphertext.

Still a further object of the invention is to provide a host cryptographic facility for performing a decipher function for deciphering a data encrypting key enciphered under a host master key to obtain the data encrypting key in clear form within the facility for use in deciphering ciphertext enciphered under the data encrypting key into cleartext.

Still another object of the invention is to provide a host data security device which deciphers an enciphered data encrypting key used for data enciphering/deciphering operations under selective control of a system or private key encrypting key to permit cryptographic data transmissions in a data communication network.

Still a further object of the invention is to provide a host data security device which performs data enciphering/deciphering operations under control of a private data encrypting key to permit private cryptographic data transmissions in a data communication network.

In accordance with the invention, a data communication network is provided having a host with an integrated data security device and associated terminals each having an integrated data security device to permit cryptographic data transmissions between the host and the associated terminals. The host data security device includes a memory for storing a host master key, cryptographic apparatus for ciphering input data under control of a cryptographic key stored in a working key register to produce ciphered output data and an interface adapter to which operation requests are presented and plaintext/ciphertext are presented for application as input data to the cryptographic apparatus and from which ciphertext/plaintext data is presented as applied from the ciphered output data of the cryptographic

apparatus. The host master key may be loaded into the master key memory by manual means or under host control by a write master key operation request to the interface adapter. The host data security device then generates a series of random numbers each of which is defined as the terminal master key for an associated terminal in the network and communicated to each terminal user in a secure manner for loading into the data security device of the respective terminals. The host data security device then enciphers and stores each of the terminal master keys under a variant of the host master key to maintain the terminal keys in a secure manner. When communication is desired between the host and one of the associated terminals, the host data security device generates a pseudo random number which is defined as an operational key enciphered under the host master key. The host data security device then performs a transformation function which reenciphers the operational key enciphered under the host master key to the operational key enciphered under the terminal master key by using the previously produced enciphered operational key and the enciphered terminal master key. The operational key enciphered under the terminal master key is then transferred as key synchronizing data to the terminal over the communication line connecting the host and the terminal. The terminal is key synchronized with the host system by reception and deciphering of the synchronizing data from the host system. This is accomplished by deciphering the synchronizing data under control of the terminal master key to obtain the operational key, in clear form, which is loaded into the working key register replacing the terminal master key previously stored therein. Encipher operation requests may then proceed to encipher terminal plaintext under control of the operational key in the working key register to produce terminal ciphertext for transmission to the host. At the host, upon receipt of the terminal ciphertext, a decipher operation request causes the host cryptographic apparatus to decipher the enciphered operational key under control of the host master key to obtain the operational key, in clear form, which is loaded into the working key register replacing the host master key previously stored therein. The ciphertext received from the terminal i.e. terminal data enciphered under the operational key, is then deciphered under control of the operational key presently in the working key register to produce the terminal plaintext. In a similar manner, plaintext at the host is enciphered under the operational key at the host and transmitted to the terminal where it is deciphered under control of the common operational key now stored at the terminal.

Other arrangements are also provided which permit a variety of communication security applications using a pre-defined private terminal master key. Additionally a further arrangement is provided which permits a communication security application using a pre-defined private data encrypting key. At the terminal, the private data encrypting key can be loaded directly into the working key register by a load key direct function. At the host, after the private data encrypting key has been received in a secure manner and loaded into the host, an encipher operation is performed to encipher the private key under the host master key in order to maintain it in a secure manner. Then, when communication is to be had between the host and the terminal, the host decipher the enciphered private data encrypting key and loads it as the working key in the host working key register. With the private data encrypting key now

present in the key registers of the host and terminal, subsequent encipher/decipher operations can proceed under control of the common private data encrypting key.

The foregoing and other objects, features and advantages of the invention will be apparent from the following particular description of a preferred embodiment of the invention, as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWING

FIG. 1 is a block diagram illustrating a cryptographic data communication network.

FIG. 2 is a block diagram of a representative network illustrating, in block form, the details of a host and terminal in such a network.

FIG. 3 is a block diagram of a cryptographic engine which performs cryptographic functions in a logically and physically secure manner.

FIG. 4 illustrates in block diagram form a manual WMK function.

FIG. 5 illustrates in block diagram form a host controlled WMK function.

FIG. 6 illustrates in block diagram form a DECK function.

FIG. 7 illustrates in block diagram form a ENC function.

FIG. 8 illustrates in block diagram form a DEC function.

FIG. 9 illustrates in block diagram form a GRN function.

FIG. 10 illustrates in block diagram form an EMK0 function.

FIG. 11 illustrates in block diagram form an EMK1 function.

FIG. 12 illustrates in block diagram form a ECPH function.

FIG. 13 illustrates in block diagram form a DCPH function.

FIG. 14 illustrates in block diagram form a RFMK function.

FIG. 15 is a block diagram illustrating the basic concepts of cryptographic communication security in a single domain network using a system or private key as a key encrypting key.

FIG. 16 is a block diagram illustrating details of cryptographic communication security in a single domain network using system generated keys.

FIG. 17 is a block diagram illustrating details of cryptographic communication security in a single domain network using a private key.

FIG. 18 is a block diagram illustrating details of cryptographic communication security in a single domain network using a private key with a private end user protocol.

FIG. 19 is a block diagram illustrating cryptographic communication security in a single domain network using a private key as a data encrypting key.

FIG. 20 illustrates the details of a clock circuit used in the data security device of the present invention.

FIG. 21 is a timing diagram explaining the operation of the clock circuit illustrated in FIG. 20.

FIG. 22 is a diagram of how FIGS. 22a1 through 22i2 may be placed to form a detailed schematic diagram.

FIGS. 22a1 through 22i2, taken together, comprise a detailed schematic diagram of the data security device of the present invention.

FIG. 23 is a timing diagram of the manual WMK operation.

FIG. 24 illustrates how FIGS. 24a and 24b may be placed to form a composite timing diagram.

FIGS. 24a and 24b, taken together, comprise a timing diagram of the host controlled WMK operation.

FIG. 25 illustrates logic details of the crypto engine used in the data security device of the present invention.

FIG. 26 illustrates how FIGS. 26a to 26c may be placed to form a composite timing diagram.

FIGS. 26a to 26c, taken together, comprise a timing diagram of the DECK operation.

FIG. 27 illustrates how FIGS. 27a to 27d may be placed to form a composite timing diagram.

FIGS. 27a to 27d, taken together, comprise a timing diagram of the DEC/ENC operation.

FIG. 28 illustrates how FIGS. 28a to 28c may be placed to form a composite timing diagram.

FIGS. 28a to 28c, taken together, comprise a timing diagram of the GRN operation.

FIG. 29 illustrates how FIGS. 29a to 29c may be placed to form a composite timing diagram.

FIGS. 29a to 29c, taken together, comprise a timing diagram of the EMK operation.

FIG. 30 illustrates how FIGS. 30a to 30g may be placed to form a composite timing diagram.

FIGS. 30a to 30g, taken together, comprise a timing diagram of the RFMK operation.

GENERAL DESCRIPTION

INTRODUCTION

In a data communication network, a complex of communication terminals are connected via a plurality of communication lines to a host data processing system and its associated resources such as host programs, and locally attached terminals and secondary storage files. Because of the complexity and increasing size of such networks which may include single or multiple domain networks, it has been recognized that when data is transmitted over unsecure communication lines it is necessary to protect the data to maintain the confidentiality and integrity of the information represented by that data. Cryptography provides an effective data security measure for communication security in that it protects the confidentiality and integrity of the data itself rather than the medium over which it is transmitted. FIG. 1 illustrates a cryptographic arrangement in a representative single domain data communication network.

Most practical cryptographic systems require two basic elements, namely, (1) a cryptographic algorithm which is a set of rules that specify the steps required to transform or encipher plaintext into ciphertext or to transform or decipher ciphertext back into plaintext and (2) a cipher key. The cipher key is used to select one out of many possible relationships between the plaintext and the ciphertext. Various cryptographic algorithms have been developed in the prior art for improving data security in data processing systems. One such algorithm is described in U.S. Pat. No. 3,958,081 issued May 18, 1976 and was recently adopted as a United States Federal Data Processing Standard as set forth in the aforesaid Federal Information Processing Standard publication. A hardware implementation of this algorithm is incorporated in the present invention. The cryptographic algorithm operates to transform or encipher a 64 bit block of plaintext into a unique 64 bit block of ciphertext under control of a 56 bit cipher key or to

transform or decipher a 64 bit block of ciphertext back into an original 64 bit block of plaintext under control of the same 56 bit cipher key with the deciphering process being the reverse of the enciphering process. The effectiveness of this cipher process depends on the techniques used for the selection and management of the cipher key used in the cipher process. The only cipher key actually used in the cipher process to personalize the algorithm when encrypting or decrypting data or other keys is termed the working key and is accessible only by the cryptographic apparatus. All other keys hereafter discussed are used at different times as working keys depending upon the cipher operation to be performed.

There are basically two categories of cipher keys used in the cryptographic system, namely, operational keys (KO) and key encrypting keys (KEK) with operational keys being referred to and used as data encrypting keys. Data encrypting or operational keys are a category of keys used to encrypt/decrypt data while key encrypting keys are a category of keys used to encrypt/decrypt other keys.

Within the two basic categories, there are variously defined classes and types of cipher keys. Thus, in the data encrypting or operational class of cipher keys, the data encrypting or operational key which protects data during data communication sessions in a class of key called the primary communication key. One type of this class of keys is one which is a system generated, time variant, dynamically created key transmitted in enciphered form under a key encrypting key from a host system to a remote terminal. The key is deciphered at the terminal and then loaded into the working key register and used as the working key. The key exists only for the duration of the communication session and will be referred to as the system session key (KS). In private cryptographic systems which use a private protocol known to each end user but unknown to the system, a private key may be used as another type of primary communication key to provide communication security. The private key is loaded into the terminal working key register and then used as the working key. The key exists only for a time duration determined by the private protocol which may require the key to be changed for each communication, once an hour, once a week, etc. and will be referred to as the private session key (KSP).

Within the key encrypting category of cipher keys, there are two sub-categories, namely, the primary key encrypting key and the secondary key encrypting key. In the primary key encrypting key sub-category of cipher keys, the key encrypting key used in the host system to encipher other keys is a class of key called the system key. One type of this class of keys is one which is used to protect the system session keys actively used at the host and will be referred to as the host master key (KMH). In the secondary key encrypting key sub-category of cipher keys, the key encrypting key used in the terminal to protect other keys is a class of key called a secondary communication key. Two types of this class of keys are used to protect system session keys transmitted to the terminal and when system generated will be referred to as the terminal master key (KMT) and when provided as a pre-defined private key will be referred to as a private terminal master key (KMTP). The various cipher keys defined above are summarized in the following table by category, class, type and use:

CATEGORY	SECURITY CLASS	TYPE	USE
Key Encrypting Keys			
Primary	System Key	Host Master Key (KMH)	Encipher
Secondary	Secondary Communi- cations Keys	Terminal Master Key (KMT) Private Terminal Master Key (KMTP)	Other Crypto- graphic Keys
Data Encrypting Keys	Primary Communi- cation Keys	System Session Key (KS) Private Session Key (KSP)	Encipher Or Decipher Data
(Operational Keys)			

GENERATION, DISTRIBUTION, INSTALLATION AND MANAGEMENT OF CRYPTOGRAPHIC KEYS

Key generation is the process which provides for the creation of the cipher keys required by a cryptographic system. Key generation includes the specification of a system master key and primary and secondary communication keys.

The host master key is the primary key encrypting key and is the only cipher key that needs to be present in the host cryptographic facility in clear form. Since the host master key does not generally change for long periods of time, great care must be taken to select this key in a random manner. This may be accomplished by using some random experiment such as coin tossing where bit values 0 and 1 are determined by the occurrence of heads and tails of the coin or by throwing dice where bit values 0 and 1 are determined by the occurrence of even or odd rolls of the dice, with the occurrence of each group of coins or dice being converted into corresponding parity adjusted digits. By enciphering all other cipher keys stored in or passed outside the host system, overall security is enhanced and secrecy for such other cipher keys reduces to that of providing secrecy for the single host master key. Secrecy for the host master key may be accomplished by storing it in a non-volatile master key memory so that the host master key need only be installed once. Once installed, the master key is used only by the cryptographic apparatus for internally deciphering enciphered keys which may then be used as the working key in a subsequent encipher/decipher operation.

Installation of the host master key may be accomplished by a direct manual entry process using mechanical switches, dials, or a hand-held key entry device. Alternately, an indirect entry method may be used in which case the host master key may be entered from a non-volatile media such as a magnetic card or tape which is maintained in a secure location (safe, vault, etc.) accessible only to the security administrator. Another alternative indirect entry method may be to use a keyboard entry device, though this method is subject to human error. In any event, whichever indirect method is chosen, during initialization, the host master key may be read into and temporarily stored in the host memory

and then transferred to the master key memory with the host memory entry being subsequently erased so that only one copy is present and accessible only by the cryptographic facility.

The terminal master key is a secondary key encrypting key and like the system master key, is the only key encrypting key that needs to be present in clear form in the terminal cryptographic facility. Since there may be numerous terminals associated with the data communication network, it may not be practical or prudent to have these keys generated by a human user using some type of random experiment. Therefore, to relieve the system administrator from the burden of creating cryptographic keys, except for the single system master key, the cryptographic apparatus of the host system can be used as a pseudo random generator for generating the required terminal master keys used by the various terminals of the network. The manner by which such host system generated random numbers are produced is described in detail hereafter. In addition to the system generated terminal master keys, off line means may be used by end users to establish a private terminal master key. In either event, the clear form of the system of private generated terminal master key is distributed in a secure manner to the authorized terminal users. This may be accomplished by transporting the key by courier, registered mail, public telephone, etc. The likelihood of an opponent obtaining the key during transit can be lessened by transmitting different portions of the key over independent paths and then combining them at the destination. Once having properly received a valid system or private generated terminal master key in clear form, it becomes necessary to maintain its secrecy. At the terminal, this is accomplished by writing the terminal master key into a non-volatile master key memory, as in the case of the host system master key. Once installed, the terminal master key is used only by the terminal cryptographic apparatus for internally deciphering system generated primary communication keys which may then be used as the working key in a subsequent encipher/decipher operation.

Because the ciphering algorithm used is not secret, the degree of protection that can be derived from a cryptographic system ultimately depends upon the security of the cryptographic keys. Therefore, the objectives of key management are: (1) cryptographic keys should never occur in clear form outside the cryptographic device, except under secure conditions during the period when keys are originally distributed and installed or when stored in a secure place such as a safe, vault or similar location for backup or recovery and (2) no cryptographic operation, or combination thereof, using any cryptographic quantities which are routinely stored or routed through the system, or derived therefrom, should permit clear keys to be recoverable outside the cryptographic device. Therefore, in keeping with the first objective, if the system generated terminal keys are to be stored at the host system they must be protected by being enciphered under another key. One way in which this may be accomplished is to encipher the terminal master keys under the host master key by an Encipher Master Key function (EMK). However, for reasons which will be described hereafter, this results in an exposure of primary communication keys which violates the second objective of key management. Accordingly, to prevent exposing these keys in clear form, a dual master key approach is adapted, by the present invention, in which a variant (KMH1) of the

host master key (KMH0) is used to encipher the terminal master keys by an Encipher Master Key function (EMK1), which will be described in greater detail hereafter. In the embodiment of the present invention, only the host master key resides in clear form within the cryptographic device. Accordingly, when an EMK1 function is to be performed, the host master key is read out of the master key memory and by selected inversion of certain bits of the host master key the variant KMH1 is derived for use in enciphering the terminal master key. By enciphering the terminal master keys under the variant of the host master key, the enciphered terminal keys may be stored in a cryptographic data set until required for use in a cryptographic operation and the first objective of key management is obtained, namely, that no key shall occur in clear form. For reasons which will be described hereafter, the encipherment also meets the second objective of key management.

System generated primary communication keys, i.e. session keys, are time variant keys which are dynamically generated for each communication session and are used to protect communicated data. Since there may be numerous communications sessions it is impractical to have these keys generated by a human user. Therefore, the cryptographic apparatus of the host system may be used as a pseudo-random generator for generating, as each communication session is required, a pseudo-random number which, in keeping with the objective that cryptographic keys should never occur in the clear, may be defined as being a session key enciphered under the host master key.

When encipher/decipher data operations are required at the host system, a decipher key function (DECK) is first performed, described in greater detail hereafter, in which, using the host master key as the working key, the session key enciphered under the host master key is deciphered, with the resulting session key, in clear form, being retained in the host cryptographic device and replacing the host master key as the working key for encipher/decipher data operations. An encipher data function (ENC) is performed by enciphering data under the session key now available as the working key whereas a decipher data function (DEC) is performed by deciphering data enciphered under the session key by using the session key now available as the working key, both of these functions will be described in greater detail hereafter.

In order to allow the host system and a terminal to communicate with each other using the session key as a common operational key, it is necessary to communicate the session key to the terminal. This is accomplished by first performing a Re-encipher From Master Key transformation function (RFMK), which re-enciphers the session key enciphered under the host master key to the session key enciphered under the terminal master key, in a manner described in greater detail hereafter, and then communicating the session key enciphered under the terminal master key to the terminal. At the terminal, the enciphered session key is deciphered by a DECK function, using the terminal master key as the working key with the resulting session key, in clear form, being retained in the terminal cryptographic device and replacing the terminal master key as the working key for terminal encipher/decipher data functions ENC/DEC.

In order to perform the transformation function described above, it is necessary to make use of the enciphered terminal master key. Accordingly, if the terminal

master key had been stored under the host master key rather than a variant of the host master key, then the session key may be exposed in clear form when the session key enciphered under the terminal master key becomes available over the communication line by wiretap and the enciphered terminal master key may become exposed while in storage at the host system. This may be accomplished by first performing a DECK function to decipher the terminal master key enciphered under the host master key, rather than the variant of the host master key, using the host master key as the working key with the resulting terminal master key, in clear form, being retained in the host cryptographic device and replacing the host master key as the working key. Then, by performing a DEC function using the wiretapped session key enciphered under the terminal master key as data, the enciphered session key may be deciphered using the terminal master key as the working key with the resulting session key becoming available in clear form outside the cryptographic device and violating the first objective of key management namely, that cryptographic keys should never occur in clear form outside the cryptographic device. This exposure is eliminated by using the variant of the host master key to encipher the terminal master key since the DECK function always uses the host master key as the working key and any attempt to decipher the terminal key enciphered under a variant of the host master key by using the non-variant of the host master key will result in useless information. It should be noted that although the relationship between the host master key and its variant are known i.e. which bits are inverted, the cryptographic strength is not weakened because there is no way to use this information to arrive at useful key information because of the complexity of the algorithm.

Thus, by enciphering the terminal master key under a first variant of the host master key, both of the objectives of key management are obtained, namely, the terminal master key does not occur in clear form outside the cryptographic device and when used in a cryptographic function it does not permit a clear key to be recoverable outside the cryptographic device.

In some private cryptographic systems, end users may wish to use a private primary communication key but still make use of the system facilities for key generation and key management. Thus, in a single domain data communication network where an end user terminal is remote from the host system, the end users may define a mutually agreed upon private communication key i.e. a private terminal master key KMTP. At the host, the mutually agreed upon key may be loaded into host, be enciphered under a variant of the host master key to maintain the private key in a secure manner, and then stored in a crypto key data set until such time as a session is to be had with the terminal user as in the case of system generated keys. When a communication session is to be established between the host and an end user terminal, the private terminal master key is loaded into the terminal master key memory and the balance of the operation may proceed as in the case of system generated keys.

Where limited key management facilities are used with a private end user protocol, it may be necessary to write the enciphered private terminal master key to an output device, such as a printer, and store the printer output in a secure manner, e.g. in a physically protected vault, until such time as the communication session is desired. At that time, the enciphered private terminal

key is brought out and loaded back into the host system. The terminal user loads the private key into the terminal master key memory and the communication session may then be initiated.

In other private cryptographic systems, where the end users use a private protocol which is unknown to the system, key selection, management and data transfer operations are performed without system knowledge that cryptography is being performed. In such arrangements, the end users may define a private protocol using a mutually agreed upon primary communication key, i.e. a private session key. This key is loaded into the host system and the terminal as a common working key thereby allowing the host and terminal to communicate using the common private session key. With this end-to-end encryption approach, enciphered messages can be sent via networks of any type, private or public, without system knowledge that cryptography is being performed but providing communication security for such data transmissions.

While it is efficient to use variants of a host master key to provide protection for the various cryptographic keys used in the system, it is well within the skill of the art to provide separate master keys instead of variants of a single master key. This could be accomplished by providing separate master key memories each being loaded with a master which is different from each other and being accessed when needed. While this is a viable alternative, it would substantially increase the cost of the host data security device as opposed to using a single master key memory and obtaining variants as needed.

SINGLE DOMAIN COMMUNICATION NETWORKS

Modern day data communication networks may include a complex of communication terminals connected via communication lines to a single host and its associated resources such as the host programs and locally attached terminals and data files. A representative network is shown in FIG. 2 with the host and its associated resources shown in block form and a representative one of the plurality of remote communication terminals also shown in block form. The terminal and integrated data security device and the manner in which the data security performs cryptographic operations is described in detail in the co-pending application Ser. No. 857,533, filed Dec. 5, 1977 entitled "Cryptographic Communication and File Security Using Terminals" by Ehram et al. While the particular manner in which the host is implemented is not critical to the present invention, the block diagram of the host in FIG. 2 shows the data flow and control relationships of a representative host arrangement. The host includes a programmable processor 1 operationally connected to a memory 2 which provides storage for data and the programs which are utilized to control the system and a channel 3 which controls the transfer of data between input/output devices and the processor 1. Channel 3 is connected to the processor 1 and memory 2 and via a channel I/O Interface, with control units such as control unit 4 capable of controlling a cluster of input/output devices which may be display or printer type of devices, control unit 5 capable of controlling a plurality of magnetic tape units or control unit 6 capable of controlling a plurality of disk files. Communication controller 7 is a two-direction control unit that links the host to communication lines connected to remote terminals such as communica-

tion terminals 8, 9 and 10. While not shown, communication lines require a modem at each end of the line to convert binary signals to analog signals back to binary signals at the other over the communication line and for reconverting (demodulation) analog signals back to binary signals at the other end of the line.

The collection of data and control lines connected between the channel and I/O control units is commonly referred to as the channel I/O interface providing an information format and signal sequence common to all the I/O control units. The I/O interface lines generally include a data bus out which is used to transmit device addresses, commands and data from the channel 3 to the I/O control unit; a data bus in which is used to transmit device identification, data or status information from the I/O control unit to the channel 3 and tag signal lines which are used to provide signals identifying an I/O operation, the nature of information on the data bus and parity condition. Since each I/O control unit has a unique electrical interface, device adapters are generally provided to allow device connection to the common I/O interface. All I/O data transfers between the processor and the attached control units may be performed in a programmed input/output (PIO) mode on a 1 byte per I/O instruction basis.

Into this organization of a general purpose host system is integrated a data security device of the present invention. The data security device (DSD) 11 includes a crypto device 12, a master key (MK) memory 13, a DSD adapter 14 which connects to the I/O interface and a manual entry device 15 for manually loading a terminal master key into the MK memory 13. Either one of two methods can be used for writing a host master key into the MK memory 13. The first method for writing the host master key into the MK memory 13 is achieved under program control. In this method, an I/O device having a keyboard, magnetic stripe card reader or the like, may use such elements to cause the host master key to be stored in the host memory 2 as in the case of conventional data entry. Subsequently, under program control, the host master key may be read from the host memory 2 to the MK memory 13 of the DSD in a manner which will be described in greater detail hereafter. The other method of writing the host master key into the MK memory 13 consists of manually writing the host master key into the MK memory 13 by means of individual toggle or rotary switches wired to produce binary coded hex digits as will be described in greater detail hereafter. To enable master key writing into the MK memory 13 by either method, an enable write key (EW) switch is provided which is initially turned on when a write master key operation is initiated and turned off at the end of write master key operation. To prevent the key from being changed by unauthorized persons, the EW switch operation may be activated by a physical key lock arrangement.

The DSD adapter 14 serves a dual function namely, providing adapter functions for DSD connection to the I/O interface and control functions for the DSD.

The I/O interface provides the DSD adapter 14 with overall direction, gives it cipher keys to be used, presents it with data to be processed and accepts the processed results. Overall direction is achieved by use of operation commands which are decoded and subsequently provide control in properly timed sequences of signals to carry out each command. These signals are synchronized with the transfer of data in and out. The DSD adapter 14 also controls the placing of cipher keys

in the crypto device 12 and directs the crypto device in the enciphering and deciphering operations.

The MK memory 13 is a non-volatile 16×4 bit random access memory (RAM) which is battery powered to enable key retention when host power may not be present. The host master key consists of eight master key bytes (64 bits) each of which consists of seven key bits and one parity bit.

The crypto device 12 is the heart of the DSD hardware for performing enciphering and deciphering operations. The crypto device 12 performs encipher/decipher operations on a block cipher basis in which a message block of 8 data bytes (64 bits) is enciphered/deciphered under control of a 56 bit cipher working key to produce an enciphered/deciphered message block of 8 data bytes. The block cipher is a product cipher function which is accomplished through successive applications of a combination of non-linear substitutions and transpositions under control of the cipher working key. Sixteen operation defined rounds of the product cipher are executed in which the result of one round serves as the argument of the next round. This block cipher function operation is more fully described in the aforementioned U.S. Pat. No. 3,958,081. A basic encipher/decipher operation of a message block of data starts with the loading of the cipher key from the host memory 2. This key is generally stored under master key encipherment to conceal its true value. Therefore, it is received as a block of data and deciphered under the master key to obtain the enciphering/deciphering key in the clear. The clear key does not leave the crypto device 12 but is loaded back in as the working key. The message block of data to be enciphered/deciphered is then transferred to the crypto device 12 and the cipher function is performed, after which the resultant message block of enciphered/deciphered data is transferred from the crypto device 12 to the host memory 3. If subsequent encipher/decipher functions are to be performed using the same working key, there is no need to repeat the initial steps of loading and deciphering the working key as it will still be stored in the working key register.

The crypto device 12 includes duplicate crypto engines operating in synchronism to achieve checking by 100% redundancy. Referring now to FIG. 3, one of the crypto engines is shown in simplified block form with a heavy lined border signifying a secure area. The crypto engine 16 contains a 64 bit input/output buffer register 17 divided into upper and lower buffer registers 18 and 19 of 32 bits each. The buffer register 17 is used in a mutually exclusive manner for receiving input data on a serial by byte basis from the bus in, termed an input cycle, and for providing output data in a serial by byte basis to the bus out, termed an output cycle. Thus, during each input cycle a message block of eight data bytes is written into the buffer register 17 from the host memory 2 while during each output cycle a message block of eight processed data bytes is read from the buffer register 17 to the host memory 2. Serial outputs of the buffer register 17 are also applied as serial inputs to the working key register 20 and a parity check circuit 21, the latter being controlled to be effective only when a 64 bit clear cipher key is to be loaded directly into the working key register 20 from the host memory 2 via the buffer register 17. Only 56 of the 64 bits are stored in the working key register 20, the 8 parity bits being used only in the parity check circuit 21. The buffer register 17 is also provided with parallel input and output paths from and to a 64 bit data register 22 also divided into

upper and lower data registers 23 and 24 of 32 bits each. The upper and lower data registers 23 and 24 each possesses parallel outputs and two sets of parallel inputs. The parallel inputs to the lower data register 24 being from the lower buffer register 19 and the upper data register 23 while the parallel inputs to the upper data register being from the upper buffer register 18 and from the lower data register 24 after modification by the cipher function circuits 25. The 64 bit master key is inputted to the crypto engine 16 on a serial by byte basis with each byte being checked for correct parity by the parity check circuit 26. As in the case of the cipher key transfer from the buffer register 17 to the working key register 20, only 56 of the 64 bits are stored in the key register 20, the 8 parity bits being used only in the parity check circuit 26. During the loading process, the key register 20 is configured as seven 8-bit shift right registers to accommodate the eight 7-bit bytes received from the MK memory 13 (or the buffer register 16).

When the working key is used for enciphering, the key register 20 is configured as two 28 bit recirculating shift left registers and the working key is shifted left, in accordance with a predetermined shift schedule, after each round of operation of the cipher function so that no set of key bits once used to perform a cipher operation is used again in the same manner. Twenty-four parallel outputs from each of the two shift registers (48 bits) are used during each round of the encipher operation. The shift schedule provided is such that working key is restored to its initial beginning position at the end of the complete encipher operation.

When the working key is used for deciphering, the key register 20 is configured as two 28 bit recirculating shift right registers and the working key is shifted right in accordance with a predetermined shift schedule, after each round of operation of the cipher function so that again no set of key bits is used again. As in the enciphering operation, twenty-four parallel outputs from each of the two shift registers (48 bits) are used during each round of the decipher operation. The shift schedule provided in this case is also such that the working key is restored to its initial beginning position at the end of the complete decipher operation.

The cipher function circuits 24 perform a product cipher through successive application of a combination of non-linear substitutions and transpositions under control of the cipher working key. Sixteen rounds of the product cipher are executed in which the results of one round serves as the argument of the next round. Deciphering is accomplished by using the same key as for enciphering but with the shift schedule for shifting the key being altered so that the deciphering process is the reverse of the enciphering process, thus undoing in reverse order every step that was carried out during the enciphering process. During each round of the cipher function, the data contents of the upper data register 23, designated R, is enciphered under control of the working key, designated K, with the result being added modulo-2 to the contents of the lower data register 24, designated L, the operation being expressed as $L \oplus f(R, K)$. At the end of the cipher round, the contents of the upper data register 23 is parallel transferred to the lower data register 24 while the output of the cipher function circuits 25 is parallel transferred to the upper data register 23 to form the arguments for the next round of the cipher function. After a total of sixteen rounds, which completes the total cipher function, the contents of the upper data register 23 is parallel trans-

ferred to the upper buffer register 18 while the output of the cipher function circuits 25 is parallel transferred to the lower buffer register 19. The transformed data contents of the buffer register 17 is then outputted via the bus out to the host memory 2.

DSD COMMANDS AND ORDERS

Input/output operations of an I/O device are generally directed by the execution of I/O instructions. In executing an I/O instruction, the channel generally provides an address field for addressing the I/O device, a command field for designating the operation to be performed and another address field for addressing the data field in memory from which data is fetched or to which data is stored. The data security device 11 of the present invention is responsive to seven types of commands from the processor as shown in the following table including the mnemonic and bit pattern of the command:

COMMAND FORMAT									
Name	Mnemonic	0	1	2	3	Command Field			
1. Reset Adapter	RST	—	—	—	—	0	0	1	0
2. Set Basic Status	SET BS	—	—	—	—	0	1	1	0
3. Reset Basic Status	RST BS	—	—	—	—	0	1	0	0
4. Read Basic Status	RD BS	—	—	—	—	0	1	1	1
5. PIO Write Data	PIOW	—	—	—	—	1	1	0	0
6. PIO Read Data	PIOR	—	—	—	—	1	1	0	1
7. Write DSD Order	WR DSD	w	x	y	z	1	1	1	0

The following is a brief description of the function of each of the commands, the operation of which will be described in greater detail hereafter.

1. Reset Adapter (RST)—This command causes a reset signal to be created to reset all counters, flip-flops and latches in the adapter and control sections of the DSD.

2. Set Basic Status (SET BS)—This command causes those latches in a status register of the DSD that correspond to 1's in the data field to be set to 1.

3. Reset Basic Status (RST BS)—This command is similar to the SET BS command except that the status latches corresponding to 1's in the data field are set to 0.

4. Read Basic Status (RD BS)—This command causes the contents of the status latches to be applied via the data bus in to the processor.

5. PIO Data (PIOW)—This command causes the data field to be loaded into the buffer register or the bits 0, 1, 2, and 3 of the data field to be stored in the MK memory depending on the operation to be performed.

6. PIOR DATA (PIOR)—This command causes the contents of the buffer register, with correct parity, to be applied via the data bus in to the processor.

7. Write DSD Order (WR DSD)—This command uses the four high order bits of the command field to designate cipher key handling and data processing orders as shown in the following table including the mnemonic and bit pattern of the order field:

ORDER FORMAT										
5	Name	Mnemonic	Order Field				Command Field			
			W	X	Y	Z	4	5	6	7
	<u>Cipher Key Handling</u>									
1.	Write Master Key	WMK	0	0	0	0	1	1	1	0
10	2. Decipher Key	DECK	0	1	1	1	1	1	1	0
3.	Generate Random Number	GRN	1	1	1	1	1	1	1	0
4.	Encipher Master Key 0	EMK0	1	1	0	0	1	1	1	0
15	5. Encipher Master Key 1	EMK1	1	1	0	1	1	1	1	0
6.	Reencipher From Master Key	RFMK	0	1	0	1	1	1	1	0
20	<u>Data Processing</u>									
1.	Encipher	ENC	1	0	0	0	1	1	1	0
2.	Decipher	DEC	1	0	1	0	1	1	1	0

DSD FUNCTIONS

DSD cryptographic functions may be performed by combinations of the previously defined commands or by a combination of functions. These functions require an input to the cryptographic apparatus consisting of a key parameter or a data parameter. The notation used to describe these functions will be expressed as follows:

FUNCTION[KEY PARAMETER]→OUTPUT

or

FUNCTION[DATA PARAMETER]→OUTPUT

and when functions are combined, the notation used to describe the combined functions will be expressed as follows:

FUNCTION[KEY PARAMETER, DATA PARAMETER]→OUTPUT

The salient characteristics of host cryptographic functions are that (1) the key parameter, is always in enciphered form and therefore must be internally deciphered by the crypto engine before the clear key is used and that (2) no function allows keys to become available in clear form. The descriptions that follow describe what each function does and how it is performed. These functions will be described in greater detail hereafter but the general description of these functions or combination of functions are given at this point to provide a better understanding of how various security applications may be performed. The descriptions may follow along with reference to FIG. 3 at times. In the diagrams which are referenced in the following, the cryptographic facility is shown in simplified block form for ease of understanding these operations and will be shown and described in greater detail hereafter.

Before proceeding to the descriptions of the functions, a brief general description will be given of how the manual write key operation is performed. Referring now to FIG. 4, there is shown a simplified block diagram of a manual WMK operation. In the manual WMK operation, an EW switch is set on to enable writing into the MK memory 13 after which a MW switch is closed to enable manual writing and causing the current master key to be overwritten with whatever

happens to be set in the data key entry switches. Following this, 16 sets of 4 bits (64 bits) are manually written into the MK memory 13 to complete the manual WMK operation.

Referring now to FIG. 5, there is shown a simplified block diagram of a write master key (WMK) function. This function is carried out by the following sequence of commands: (1) WMK and (2) 16 PIOW's. In this operation, as in the manual WMK operation, the EW switch is previously set on to enable writing into the MK memory 13. The execution of this function causes the current master key in the master key memory 13 to be over-written with whatever happens to be present as bits 0, 1, 2 and 3 on the bus in. Thereafter, the crypto engine controls are set to allow a 64 bit master key KM to be written as a key parameter into the MK memory 13 by means of 16 successive PIOW data commands with the bits 0, 1, 2 and 3 in the data fields associated with the 16 PIOW data commands constituting the new master key. The notation $WMK[KM] \rightarrow KM$ is used to describe this operation whereby the term WMK indicates the function, the contents of the brackets indicate the key parameter input to the MK memory 13 and the arrow points to the result.

Referring now to FIG. 6, there is shown a simplified block diagram of a decipher key DECK function. This function is carried out by the following sequence of commands: (1) DECK and (2) 8 PIOW's. The execution of this function sets the crypto engine controls to first allow the master key KM in the MK memory 13 to be transferred to the crypto engine 16 as the working key. After or during the master key transfer, a 64 bit data block, defined as an operational key enciphered under the master key, is loaded as a key parameter into the crypto engine 16 by means of 8 successive PIOW data commands with the successive data fields associated with the 8 PIOW commands constituting the enciphered operational key. After the key parameter loading is completed, the crypto engine 16 performs a decipher operation to obtain the cipher key in clear form. The resultant clear cipher key does not leave the crypto engine 16 but is loaded back into the key register 20 of the crypto engine 16 replacing the master key as the working key. The notation $DECK[E_{KM}KO] \rightarrow KO$ is used to describe this operation whereby the term DECK indicates the function, the contents of the bracket indicate the key parameter which is inputted to the crypto engine 16 and the arrow points to the result.

Referring now to FIG. 7, there is shown a simplified block diagram of an encipher (ENC) function. This function is carried out by the following sequence of commands: (1) ENC (2) 8 PIOW's and (3) 8 PIOR's. The execution of this function sets the crypto engine controls to the encipher mode of operation and allows a 64 bit message block of data to be loaded as a data parameter into the crypto engine 16 by means of 8 successive PIOW data commands with the successive data fields associated with the 8 PIOW commands constituting the message block of data to be enciphered. After the data parameter loading is completed, the crypto engine 16 performs an encipher operation to encipher the data parameter under the operational key presently stored in the working key register of the crypto device 16. The 64 bit enciphered result is transferred by a series of 8 PIOR commands from the crypto engine 16 for storage in designated data fields of the host memory 2. The notation $ENC[DATA] \rightarrow E_{KO}DATA$ is used to describe this operation whereby the term ENC indi-

cates the function, the contents of the bracket indicate the data parameter input to the crypto engine 16 and the arrow points to the result. Additionally, so long as the crypto engine controls remain set in the encipher mode of operation, then a message which consists of multiple 8 byte blocks of data may be enciphered by the crypto engine 16 by means of an encipher command followed by a series of successive 8 PIOW data commands and successive 8 PIOR data commands for each block of data. This message encipherment may be expressed by the notation:

$$ENC[DATA_1, DATA_2 \text{---} DATA_N] \rightarrow E_{KO}(DATA_1, DATA_2 \text{---} DATA_N).$$

Referring now to FIG. 8, there is shown a simplified block diagram of a decipher (DEC) function. This function is carried out by the following sequence of commands: (1) DEC (2) 8 PIOW's and (3) 8 PIOR's. The execution of this function sets the crypto engine controls to a decipher mode of operation and allows a 64 bit message block of enciphered data to be loaded as a data parameter into the crypto engine 16 by means of 8 successive PIOW data commands with the successive data fields associated with the 8 PIOW commands constituting the message block of enciphered data to be deciphered. After the data parameter loading is completed, the crypto engine 16 performs a decipher operation to decipher the data parameter under control of the operational key presently stored in the working key register of the crypto engine 16. The 64 bit deciphered result is transferred by a series of 8 PIOR commands from the crypto engine 16 for storage in designated data fields of the host memory 2. The notation $DEC[E_{KO}DATA] \rightarrow DATA$ is used to describe this operation whereby the term DEC indicates the function, the contents of the bracket indicate the data parameter input to the crypto engine 16 and the arrow points to the results. Additionally, so long as the crypto engine controls remain set in the decipher mode of operation, then a message which consists of multiple blocks of enciphered data may be deciphered by the crypto engine 16 by means of a decipher command followed by a series of successive 8 PIOW data commands and successive 8 PIOR data commands for each block of enciphered data. This message decipherment may be expressed by the notation:

$$DEC[E_{KO}(DATA_1, DATA_2 \text{---} DATA_N)] \rightarrow DATA_1, DATA_2 \text{---} DATA_N.$$

Referring now to FIG. 9, there is shown a simplified block diagram of a generate random number (GRN) function. This function is carried out by the following sequence of commands (1) GRN and (2) 8 PIOR's. Accordingly, in executing this function, the crypto engine controls are set to the encipher mode of operation and a variant KM3 of the master key KM in the MK memory 13 is transferred to the crypto engine 16 as the working key, the variant KM3 being obtained by inverting predefined bits of the master key. During the transfer of the master key variant KM3 to the crypto engine 16, a 64 bit count value CT from a non-resettable RN counter is loaded as a data parameter into the crypto engine 16. After the key and the data parameter loading is completed, the RN counter is stepped by one and the crypto engine 16 performs an encipher operation to encipher the data parameter CT under control of the variant KM3 of the master key presently stored in the working key register of the crypto device 16. The 64 bit enciphered result is a pseudo random number RN

which is transferred by a series of 8 PIOR commands from the crypto engine 16 for storage in designated data fields of the host memory for use as a cryptographic key in a manner which will be described hereafter. The notation $GRN[CT] \rightarrow RN(E_{KM}CT)$ is used to describe this operation whereby the term GRN indicates the function, the contents of the bracket indicates the data parameter input to the crypto engine 16 and the arrow points to the result.

Referring now to FIGS. 10 and 11, there are shown simplified block diagrams of the encipher master key (EMK0 and EMK1) function. This function is carried out by the following sequence of commands (1) EMK0 (2) 8 PIOW's and (3) 8 PIOR's or (1) EMK1 (2) 8 PIOW's and (3) 8 PIOR's. Accordingly, in executing these functions, the crypto engine controls are set to the encipher mode of operation causing, in the case EMK0 function, the unmodified master key in the MK memory 13 to be transferred to the crypto engine 16 as the working key and, in the case in the EMK1 function, a variety KM1 of the master key KM in the MK memory 13 to be transferred to the crypto engine 16 as the working key. The variant KM1 is obtained by inverting predefined bits of the master key which are different from those used in the GRN function. After or during the master key transfer, a 64 bit data block, defined as an operational key, in the case of the EMK0 command, or as a secondary key encrypting key, in the case of the EMK1 command, is loaded as a data parameter into the crypto engine 16 by means of 8 successive PIOW data commands with successive data fields associated with the 8 PIOW commands constituting the operational key or the secondary key encrypting key. After the key and data parameter loading is completed, the crypto engine 16 performs an encipher operation to encipher the data parameter under the master key or variant of the master key stored in the working key register of the crypto device 16. The 64 bit enciphered result is transferred by a series of 8 PIOR commands from the crypto engine 16 for storage in designated data fields of the host memory. The notation $EMK0[KO] \rightarrow E_{KM}KO$ is used to describe the EMK0 operation while the notation $EMK1[KEK] \rightarrow E_{KM}KEK$ is used to describe the EMK1 operation whereby the terms EMK0 and EMK1 indicate the function, the contents of the bracket indicate the data parameter input to the crypto engine 16 and the arrow points to the results.

Referring now to FIG. 12, there is shown a simplified block diagram of an encipher data (ECPH) function. This function is a combination of the DECK function and the ENC function and is carried out by the following sequence of commands: (1) DECK (2) 8 PIOW's (3) ENC (4) 8 PIOW's and (5) 8 PIOR's. Accordingly, in executing this function, the crypto engine controls are first set to the decipher key mode of operation by the DECK command causing the master key KM in the master key memory 13 to be transferred as the working key to the working key register of the crypto engine 16. After or during the master key loading, the key parameter of the function, consisting of an operational key enciphered under the master key, is loaded into the crypto engine 16 by means of 8 successive PIOW data commands. The crypto engine 16 then performs a decipher key operation to obtain the operational key in clear form which is then loaded back in as the working key of the crypto engine 16 replacing the previously loaded master key. The crypto engine controls are then set to an encipher mode of operation by the ENC command

and the data parameter of the function, consisting of clear data, is loaded into the crypto engine 16 by means of 8 successive PIOW data commands. The crypto engine 16 then performs an encipher operation to encipher the data parameter under the present operational key. The enciphered result is then transferred by a series of 8 PIOR commands from the crypto engine 16 for storage in designated fields of the host memory 2. The notation $ECPH[E_{KM}KO, DATA] \rightarrow E_{KO}DATA$ is used to describe this operation whereby the term ECPH indicates the function, the contents of the bracket indicate the successive key parameter and data parameter inputs to the crypto engine and the arrow points to the result.

Referring now to FIG. 13, there is shown a simplified block diagram of a decipher data (DCPH) function. This function is a combination of the DECK function and the DEC function and is carried out by the following sequence of commands: (1) DECK (2) 8 PIOW's (3) DEC (4) 8 PIOW's and (5) 8 PIOR's. The first part of this function is identical to that for the encipher data function insofar as loading an operational key in clear form as the working key of the crypto engine 16. After the operational key loading is completed, the crypto engine controls are then set to a decipher mode of operation by the DEC command and the data parameter of the function, consisting of DATA enciphered under the operational key, is loaded into the crypto engine 16 by means of 8 successive PIOW data commands. The crypto engine 16 then performs the decipher operation to decipher the data parameter under control of the present operational key. The deciphered result is then transferred by a series of 8 PIOR commands from the crypto engine 16 for storage in designated fields of the host memory 2. The notation $DCPH[E_{KM}KO, E_{KO}DATA] \rightarrow DATA$ is used to describe this operation whereby the term DCPH indicates the function, the contents of the bracket indicate the successive key parameter and the data parameter inputs to the crypto engine and the arrow points to the result.

Referring now to FIG. 14, there is shown a simplified block diagram of a reencipher from master key (RFMK) function. This function is carried out by the following sequence of commands: (1) RFMK, (2) 8 PIOW's, (3) 8 PIOW's and (4) 8 PIOR's. Accordingly, in executing this function, the crypto engine controls are first set to the decipher mode of operation by the RFMK command and a variant KM1 of the master key KM in the KM memory 13 is transferred to the crypto engine 16 as the working key, the variant KM1 being obtained by inverting the same predefined bits of the master key as in the EMK1 function. During or after the transfer of the master key variant KM1 to the crypto engine 16, a 64 bit data block, defined as a key encrypting key enciphered under the same variant of the master key is loaded as a key parameter to the crypto engine 16 by means of 8 successive PIOW data commands with the successive data fields associated with the commands constituting the enciphered key encrypting key. After the key parameter loading is completed, the crypto engine 16 performs a decipher operation to obtain the key encrypting key in clear form. The resultant clear key encrypting key does not leave the crypto engine 16 but is retained, with half the resultant clear key available at the upper data registers 23 of the crypto engine 16 and the other half available at the cipher function circuits 25. With the crypto engine control still set for the decipher mode of operation, a special key operation

is now performed in which a 64 bit data block, defined as an operational key enciphered under the master key, is loaded as a data parameter into the buffer register 17 of the crypto engine 16 by means of 8 successive PIOW data commands with the successive data fields associated with the commands constituting the enciphered operational key. After the data parameter loading is completed, the contents of the buffer register 17 is transferred to the data register 22 of the crypto engine 16 while at the same time the contents of the upper data register 23 and the output of the cipher function circuits 25 are transferred to the buffer register 17 of the crypto engine 16. By this swapping action, the key encrypting key resulting from the first decipher operation now resides in the buffer register 17 of the crypto engine 16 while the enciphered operational key now resides in the data register 22 of the crypto engine 16. Because of the fact that a special key operation is being performed, the crypto engine control allows the master key KM in the master key memory 13 to now be transferred to the crypto engine 16 as the working key. After the master key loading is completed, the crypto engine 16 performs a second decipher operation to obtain the operational key in clear form. The resultant clear operational key does not leave the crypto engine 16 but is retained, with half of the resultant clear key available at the upper data register 23 of the crypto engine 16 and the other half available at the cipher function circuits 25. At this time, a special encipher operation is initiated with the crypto engine controls being set for an encipher mode of operation and the half of the clear operational key at the cipher function circuits 25 is transferred to the lower data register 24 so that the clear operational key is now fully available in data register 22. The key encrypting key resulting from the first decipher operation and presently residing in the buffer register 17 of the crypto engine 16 is now loaded as a working key into the key register 20 of the crypto engine 16. After key register loading operation is completed, the crypto engine 16 performs an encipher operation to encipher the operational key under the key encrypting key to complete the reencipherment function by which the operational key enciphered under the master key is now enciphered under the key encrypting key. The reenciphered result is transferred by a series of 8 PIOW commands from the crypto engine 16 for storage in designated data fields of the host memory. The notation $\text{RFMK} [E_{KM} \text{KEK}, E_{KM} \text{KO}] \rightarrow E_{KEK} \text{KO}$ is used to describe this operation whereby the term RFMK indicates the function, the contents of the brackets indicates the successive key parameter and data parameter inputs to the crypto engine and the arrow points to the results.

COMMUNICATION SECURITY APPLICATIONS

The previous section provides a description of the various basic function, command and order capabilities of a host having a data security device capable of performing enciphering and deciphering operations. Similarly, the aforementioned co-pending application Ser. No. 857,533, provides a description of the various basic function, command and order capabilities of a terminal having a data security device capable of performing enciphering and deciphering operations. Accordingly, the following descriptions will provide an explanation of how such a terminal and host may be used in various communication security applications. While the diagrams used to illustrate these applications are simplified block diagrams, it should be understood that the net-

works represented by these diagrams are far more complex than that shown. However, this type of representation is used merely to simplify and aid in the understanding of the applications to be described. It should be further understood that the host system contains a full complement of known programming support including an operating system, application programs, a telecommunications access method which, in the present case of single domain networks, directs the transmission of data between host application programs and terminals.

COMMUNICATION SECURITY IN SINGLE DOMAIN NETWORKS

Referring now to FIG. 15, there is shown a simplified conceptual block diagram of a single domain data communication network comprising a terminal, having a data security device, connected via a communication line to a host system also having a data security device contained therein. The data security device of the terminal and the manner in which it is used to generate and manage cipher keys and perform encipher/decipher operations is more fully described in the aforementioned co-pending application Ser. No. 857,533.

At host system initialization time, a primary key encrypting key KMH is generated in some random manner, as by coin or dice throwing, and then written into the MK memory of the host DSD. Following this, secondary communication key encrypting keys, e.g. KEK, are generated in clear from which, if system generated, are designated as terminal master keys KMT or, if privately generated, are designated as private terminal master keys KMTP. The clear system or private generated terminal key encrypting keys KEK are then distributed in a secure manner, as by courier, registered mail, public phone etc. to the authorized terminal users and retained at the host system in enciphered form by enciphering the terminal key encrypting key under a variant of the host master key $E_{KMH} \text{KEK}$. At the terminal the first step of initializing the terminal for communication sessions is to secure the terminal master key which is accomplished by loading the terminal KEK into the MK memory of the terminal's DSD by manual or terminal control means. To establish a communication session between the terminal and the host system, the next step is to generate a primary communication operational or data encrypting key as the common session key KS. This is initiated at terminal by the authorized terminal user LOGON or SIGNON procedure which causes a message to be transmitted to the host system identifying itself and the application program with which it wishes to communicate and a request to initiate a communication session. The host system, in response thereto, communicates with the identified application program to determine whether it is available for a communication session with the requesting terminal. If available, the host system causes a pseudo random number to be generated which is defined as being the system session key enciphered under the system master key $E_{KMH} \text{KS}$. This is in keeping with the rule that no key shall ever appear in the clear. The enciphered session key is retained at the host system for encipher/decipher operations during the communication session. Additionally, in order to distribute the session key to the requesting terminal the host system, using the enciphered terminal key encrypting key $E_{KMH} \text{KEK}$ and the enciphered session key $E_{KMH} \text{KS}$, performs an RFMK transformation function which reenciphers the session key from encipherment under

the system master key to encipherment under the terminal master key i.e. from $E_{KMHO}KS$ to $E_{KEK}KS$ where KEK may be a system generated terminal master key KMT or a private generated terminal master key $KMTP$. Since the session key is now enciphered under the terminal key encrypting key i.e. $E_{KEK}KS$, it may be transmitted over the communication line to bind the requesting terminal to the requested application program in host system for a communication session.

Now, the requesting terminal can communicate with the application program in host system to perform the following encipher data $ECPH$ function: $ECPH[E_{KEK}KS, DATA_T] \rightarrow E_{KS} DATA_T$. In executing this function, a decipher key operation $DECK(E_{KEK}KS) \rightarrow KS$ is first performed to obtain the session key in clear form as the working key, after which an encipher operation $ENC(DATA_T) \rightarrow E_{KS} DATA_T$ is performed on the data to be transmitted over the communication line to the application program in host system.

At the host system, the enciphered terminal data is deciphered by performing the following $DCPH$ function: $DCPH(E_{KMHO}KS, E_{KS} DATA_T) \rightarrow DATA_T$. In executing this function, a decipher key operation $DECK(E_{KMHO}KS) \rightarrow KS$ is first performed to obtain the session key in clear form for use as the working key, after which the enciphered data received from the terminal is deciphered by a decipher operation $DEC(E_{KS} DATA_T) \rightarrow DATA_T$ to obtain the terminal data in clear form. Alternatively, host data may be enciphered under the session key at the host system by performing the $ECPH$ function $ECPH(E_{KMHO}KS, DATA_H) \rightarrow E_{KS} DATA_H$ for transmission over the communication line to the terminal. In this case, the terminal performs the ($DCPH$) function to obtain the host data in clear form: $DCPH[E_{KEK}KS, E_{KS} DATA_H] \rightarrow DATA_H$.

It should be noted that when the communication session is terminated, the terminal must reinitiate a new request to the host system for a new communication session and cause the host system to generate a new session key enciphered under the terminal master key for establishing a new common operational key for the new communication session. This procedure provides increased security for the system since the primary communication keys are time variant and dynamically generated for each new communication session. Thus, it should be apparent that there will be frequent operational key changes for subsequent communication sessions thereby providing increased security for the system.

COMMUNICATION SECURITY IN SINGLE DOMAIN NETWORKS USING A SYSTEM KEY

Referring now to FIG. 16, there is shown in block diagram form, a logical view of session level communication security in a single domain network. In order to properly control data transmissions throughout a data communication network, it is necessary to define a communication architecture for the network. The architecture establishes the logical structure, formats, protocols, and operational sequences for the orderly movement of information throughout the network. There are many possible communication architectures which can be extended to include cryptography support. One such type of architecture is the system network architecture described in varying detail in the following publications: "Systems Network Architecture—General Information" No. GA27-3102, IBM Corporation, Armonk,

N.Y. 1975; "Advanced Function for Communications System Summary" No. GA27-3099, IBM Corporation, Armonk, N.Y., Second Edition, 1975; "System Network Architecture" IBM Systems Journal, Vol. 15, No. 1, 1976, Pages 4-80. Further details of the formats and protocols of such architecture are described in "Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic" No. SC30-3112, IBM Corporation, Armonk, N.Y., 1976. Also, one type of access method implementation of this architecture for controlling the transmission of data between elements in a data communication network is described in detail in the publication, "Advanced Communications Function for VTAM (ACF/VTAM)—Concepts and Planning" No. GC380282-1, IBM Corporation, Armonk, N.Y., Second Edition, August 1977. While the details of the architecture described in these publications are not critical to the present invention, a brief discussion of the commands for session initiation and the network elements between which they flow will be given in the following to provide a better understanding of the environment in which the invention may be applied.

In data communication networks, application programs and terminals are considered as logical units. Before data may be communicated between such logical units, a logical relationship called a session must be established between the respective logical units. In the communication session between an application program of a host system and a remote terminal of the system, the application program acts as the primary logical unit (PLU) for establishing and terminating the communication session and the terminal acts as the secondary logical unit (SLU). In order to allow a session to proceed, it is necessary to establish a connection between the two logical units. Typically, the connection may be initiated at the terminal or by the application program causing an Initiate (INIT) request to be passed to the System Services Control Point (SSCP) of the host system along with request parameters identifying the SLU in the session. The SSCP is responsible for managing the network and has available to it a complete description of the network. When the INIT request is accepted, a positive response is returned to the requesting LU. The SSCP then causes a Control Initiate (CINIT) request to be passed to the application program that it should attempt to establish (BIND) a communication session between the application program and the remote terminal. Included with the CINIT request is a Bind image which contains the session parameters that establish the characteristics of the session to be established. Upon receipt of the CINIT request, the application program has the option to accept or reject the request to go into session with the remote terminal. When the CINIT request is accepted, a positive response is returned to the SSCP. The application program then causes a BIND request, based on the Bind image, to be passed to the remote terminal requesting that a communication session be established. Included with the BIND request is the session parameters which define all of the protocols which must be observed during this session. Upon receipt of the BIND request, the remote terminal has the option to accept or reject the request to go into session with the application program. When the BIND request is accepted, a positive response is returned to the application program and the session is now estab-

lished allowing data to be communicated between the application program and the remote terminal.

The descriptions which now follow in connection with FIG. 16 through FIG. 19 are keyed to numbered notations in the figures in order to aid in understanding the sequence of operations performed in carrying out the application shown in each figure.

Accordingly, referring now to FIG. 16, at host initialization time, (1) a host master key (K_{MH0}) is selected and loaded into the MK memory by a manual WMK function or by requesting the execution of a WMK function under host control, (2) the host system then requests a series of GRN functions to be executed to define a series of terminal master keys ($K_{MT1}-K_{MTn}$) for each of the terminals associated with the host system. (3) These keys are then distributed to an authorized terminal users in a secure manner, as by courier, registered mail, public telephone etc. (4) The host system next requests a series of EMK1 functions to be performed to encipher each of the generated terminal master keys under a variant of the host master key ($E_{K_{MH1}}K_{MT1}-E_{K_{MH1}}K_{MTn}$) which are then (4) written to a cryptographic key data set (CKDS) along with terminal ID's for subsequent retrieval when cryptographic operations are to be performed. The authorized terminal user having received the terminal master key in a secure manner now loads the master key into the MK memory of the terminal by a (6) manual WMK function or by requesting the execution of a WMK function under host control.

The session initiation process begins with either the terminal or an application program initiating (7) an INIT request to the SSCP of the host system along with request parameters identifying the terminal in the session for which connection is being sought. When the INIT request is accepted, a positive response is returned to the requesting LU. The SSCP must now obtain a session key and arrange for its distribution to the participating network elements. Accordingly, the SSCP requests a (8) GRN function to be performed to generate a random number which is defined as the session key enciphered under the host master key i.e. $RN=E_{K_{MH0}}KS$, in keeping with the objective that no key shall occur in clear form, with the enciphered session key being retained in the host memory for subsequent encipher/decipher data operations. In order to distribute the session key in a form useable by the terminal, the SSCP next requests a (9) privileged RFMK transformation function to be performed. This is accomplished by accessing the CKDS for the enciphered terminal master key $E_{K_{MH1}}K_{MTi}$ as the key parameter and accessing the host memory for the enciphered session key $E_{K_{MH0}}KS$ as the data parameter to perform the RFMK function, whereby the session key enciphered under the host master key is re-enciphered to the session key enciphered under the terminal master key $E_{K_{MTi}}KS$. Having derived these quantities i.e. $E_{K_{MTi}}KS$ and $E_{K_{MH0}}KS$, they are included in the session parameters of the CINIT request. (10) The SSCP then causes the CINIT request to be passed to the application program indicating that there is a request for a session to be established with the terminal. If the application program accepts the CINIT request, a positive response is returned to the SSCP and the enciphered session key $E_{K_{MH0}}KS$ is extracted and saved for subsequent encipher/decipher data operations during the session. (11) The application program then generates a BIND request which contains among other things the enci-

phered session key $E_{K_{MTi}}KS$, which is passed to the terminal. If the terminal accepts the BIND request, a positive response is returned to the application program and the enciphered session key $E_{K_{MTi}}KS$ is extracted and saved for subsequent encipher/decipher data operations during the session. The net result of this is to establish a communication session between two participating LU's of the network with each being provided with a common operational key in a form suitable for use with their respective cryptographic apparatus. Thus, the terminal can now request that an (12) ECPH function be performed to encipher terminal data, using the session key enciphered under the terminal master key, to obtain enciphered terminal data $E_{KS}DATA$ for transfer to the application program and the application program can request a (13) DCPH function be performed to decipher the enciphered data received from the terminal using the same session key but enciphered under the host master key to obtain the terminal data $DATA_7$ in clear form. Alternatively, the application program can request an (14) ECPH function to be performed, using $E_{K_{MH0}}KS$, to encipher host data and the terminal can request a (15) DCPH function to be performed, using $E_{K_{MTi}}KS$, to decipher enciphered host data received from the application program.

COMMUNICATION SECURITY IN SINGLE DOMAIN NETWORKS USING A PRIVATE KEY

Referring now to FIG. 17, there is shown in block diagram form, a logical view of session level communication security in a single domain network using a private key. There are many situations where it is desired to provide data transmissions through a data communication network using a private secondary communication key i.e. a private terminal master key K_{MTP} , which is not system generated but is mutually agreed upon by the end users. In this case, the end users use the system for generating the session key and key management for performing the transformation function but the encipher/decipher data operations may be invoked by the system or the application program depending upon the protocol established. Therefore, in this case, at host initialization time (1) a host master key (K_{MH0}) is again selected and loaded into or may already reside in the host MK memory. (2) The end users decide upon and define, in a secure manner, the private terminal master key (K_{MTP}) to be used in their communication session. (3) This value is then loaded into the host memory and the host requests an EMK1 function to be performed to encipher the private key under a variant of the host master key $E_{K_{MH1}}K_{MTP}$ which is then (4) written out to the CKDS along with a terminal ID for retrieval in subsequent cryptographic operations. The balance of the operation to establish a communication session between an application program and the terminal used for the communication is identical to that described above in connection with the system generated key system of FIG. 16 except, depending upon the protocol established, either the system or the application program may request the encipher/decipher data operations to be performed.

COMMUNICATION SECURITY IN SINGLE DOMAIN NETWORKS USING A PRIVATE KEY AND PRIVATE END USER PROTOCOL

Referring now to FIG. 18, there is shown in block diagram form, a logical view of communication in a single domain network using a private key and a private

end user protocol. In some situations, a private level of communication security can be established using a protocol whereby key selection and distribution are the user's responsibility and requests for cryptographic service are explicitly expressed by the end user. Therefore, in this case, as in the last example, at host initialization time (1) a host master key (KMH0) is selected and loaded into or may already reside in the host MK memory. (2) The end users again decide upon and privately define, in a secure manner, the private terminal master key (KMTP) to be used in their communication session. (3) This value is loaded into the host memory and (4) the host requests that an EMK1 function be performed to encipher the private key under a variant of the host master key $E_{KMH1}KMTP$. However, in this instance, since cryptographic services are explicitly expressed by the end user rather than the system, the resultant value is not written out to a CKDS but rather (5) to an output device e.g. a printer, where both a copy of the defined private key and its enciphered version is (6) stored in a secure manner e.g. a vault, until such time as a communication session is to be established. At that time, the copies are taken out of the vault and the private key is (7) written into the terminal MK memory and (8) the enciphered version is loaded into the host memory for subsequent use when cryptographic services are requested. As in the previously described applications, the request to establish a connection may be initiated at the terminal or by the application program causing an (9) INIT request to be passed to the SSCP of the host system. When the INIT request is accepted, a positive response is returned to the requesting LU. In this case, since the private end user protocol has established that requests for cryptographic services are to be expressed by the application program, the SSCP makes no request for a session key but merely causes a (10) CINIT request to be passed to the application program that it should attempt to BIND a communication session between the application program and the terminal. If the application program accepts the CINIT request, a positive response is returned to the SSCP and the application program then requests the (11) GRN function to be performed to obtain a random number defined as the enciphered session key i.e. $RNE_{KMH0}KS$ and the (12) RFMK function to transform the session key enciphered under the host master key $E_{KMH0}KS$ to the session key enciphered under the private terminal master key $E_{KMTP}KS$ for transmittal to the terminal. The balance of the operation is identical to that described above in connection with FIG. 17 and once the common session key is established at both ends, the application program will control all requests for encipher (ECPH) or decipher (DCPH) data operations at the host system.

COMMUNICATION SECURITY IN SINGLE DOMAIN NETWORKS USING A PRIVATE KEY AND A TOTALLY PRIVATE PROTOCOL

Referring now to FIG. 19, there is shown in block diagram form a logical view of communication security in a single domain network using a private key and a private protocol which is totally private and therefore unknown to the system. In totally private systems, key selection, key management and data transfer is accomplished without system knowledge that cryptography is being performed. Whatever cryptography is performed is known only to an application program. Therefore, in this case, at host initialization time, (1) a host master key

(KMH0) is selected and loaded into or already resides in the host MK memory. (2) The end users again decide upon and privately define, in a secure manner, a private primary communication key i.e. a private session key KSP, to be used as the common operational key. (3) This value is then loaded into the host memory and the application program request an (4) EMK0 function to be performed in order to encipher the private session key under the host master key $E_{KMH0}KS$. The resulting enciphered value is not written out to a CKDS but rather to an output printer device and both a copy of the defined private session key and its enciphered version are (6) stored in a secure manner e.g. a vault, until such time as a communication session is to be established. At that time, the copies are taken out of the vault and the private session key is (7) written directly into the key registers of terminal crypto engine as a working key and (8) the enciphered version is loaded into the host memory for subsequent use when cryptographic services are requested. Since a totally private protocol is being used in this application, the steps (9) INIT request (10) CINIT request and (11) BIND request proceed in a straight forward manner to establish the communication session without the system being aware that any cryptographic operation is to be performed. Following the establishment of the session, the terminal can perform an (12) ENC function to encipher terminal data using the private session key KSP as the operational key to obtain enciphered terminal data $E_{KSP}DATA_T$ for transfer to the application program. At the host system, upon receipt of the enciphered terminal data, the application program requests a (13) decipher DCPH function to be performed to decipher the enciphered terminal data, using the enciphered private session key, to obtain the terminal data $DATA_T$ in clear form. Alternatively, the application program can request an (14) encipher ECPH function to be performed on host data, using the enciphered private session key, to obtain enciphered host data $E_{KSP}DATA_H$ for communication to the terminal. At the terminal, upon receipt of the enciphered host data, the terminal requests a (15) decipher DEC function to be performed to decipher the enciphered host data, using the private session key as the working key, to obtain the host data $DATA_H$ in clear form.

DETAILED DESCRIPTION--HOST DATA SECURITY DEVICE

Data Security Device Clock

Referring now to FIG. 20, there is shown the logic details of a clock pulse generator 100 used in the DSD of the present invention. The primary input is a square wave oscillator whose nominal repetition rate is 4MHz, having approximately a 50% duty cycle. The oscillator 102 effectively drives a ring counter made up of two D-type flip-flops 108 and 110 which are used for controlling other logic circuits within the clock 100. The clock 100 produces a clock signal — C derived from the flip-flop 110 and additionally produces four basic clock pulses from a ring counter and the oscillator pulses on the phase 1, —phase 1, —phase 1 late, phase 3 late and phase 4 lines, each being nominally 125ns in duration and having the relationships shown in FIG. 21.

More specifically, the flip-flops 108 and 110 are initially in an off state with the flip-flop 110 applying a positive signal to one input of the AND circuit 130 and to condition the flip-flop 108 for being turned on. The leading edge of a pulse from the oscillator 102 is applied

via inverters 104 and 106 to turn on the flip-flop 108 which, in being turned on, applies a positive signal to a second input of the AND circuit 130 and to condition the flip-flop 110 for being turned on. At the trailing edge of the first oscillator pulse, a positive signal is applied from the inverter 104 to render the AND circuit 130 effective to apply a positive pulse on the 03L line having a 125ns duration. The leading edge of the next oscillator pulse is applied via the inverters 104 and 106 to turn on the conditioned flip-flop 110 which, in being turned on, applies a positive signal to condition the AND invert circuit 134 and to turn on the 04 latch 132. The latch 132, in being turned on, applies a positive signal to render the AND invert circuit 134 effective to apply a negative pulse on the —04 line and, via inverter 136, a positive pulse on the 04 line, both pulses being of 125ns duration. The flip-flop 110 in being turned on also applies a negative signal to condition the flip-flop 108 for being turned off and to render the AND invert circuit 120 effective to apply a positive signal to the —C line. The leading edge of the next oscillator pulse is effective via the inverters 104 and 106 to turn off the flip-flop 108 which, in being turned off, applies a positive signal to condition the AND invert circuit 124, to turn on the 01 latch 122 and to one input of the AND invert circuit 128 and also applied a negative signal to condition the flip-flop 110 for being turned off. The latch 122 in being turned on applies a positive signal to render the AND invert circuit 124 effective to apply a negative pulse to the 01 line and, via the inverter 126, a positive pulse to the 01 line, both being of 125ns duration. The flip-flop 110 still being on applies a positive signal to a second input of the AND invert circuit 128. Accordingly, at the trailing edge of the third oscillator pulse, a positive signal is applied from inverter 104 to render the AND invert circuit 128 effective to apply a negative pulse on the 01L line having a duration of 125ns. The trailing edge of the third oscillator pulse is also effective via the inverter 106 to apply a negative pulse to reset the latch 122. The leading edge of the fourth oscillator pulse is effective, via the inverters 104 and 106, to reset the flip-flop 110 which returns the ring counter back to its initial condition. The flip-flop 110 in being reset applies a positive signal to one input of the AND invert circuit 120 and after a delay provided by the inverters 112, 114, 116 and 118 to render the AND invert circuit 120 effective to apply a negative signal on the —C line. At the end of the fourth oscillator cycle, the clock 100 is back at the initial condition to repeat the generation of the various clock pulses in successive phase times as shown in FIG. 21.

MANUAL WRITE MASTER KEY (WMK) OPERATION

The write master key operation consists of manually writing 16 half-bytes (4 bits) constituting the master key into the master key (MK) memory via 4 bit lines. Enable write (EW) and manual write (MW) switches are provided to initialize and control the 16 cycles needed for loading the individual half-bytes into the MK memory. Bit switches are also provided for producing the binary coded numbers 0 through F with all outputs being low for 0 and high for F. The master key is pre-generated, in a random manner, as 16 hexadecimal numbers to be written into the 16 locations of the MK memory. The following is a generalized step-by-step procedure of manually writing the master key into the MK memory.

Step 1: Set the EW switch to the on or enable write master key (EWMK) position.

Step 2: Press the MW switch once to reset the MK memory address counter to 0 and to overwrite the master key presently stored in the MK memory.

Step 3: Set the bit switches to the half-byte to be written into the MK memory location 0.

Step 4: Press the MW switch once.

Step 5: Set the bit switches to the next half-byte to be written into the next succeeding location of the MK memory.

Step 6: Press the MW push button once.

Steps 7-34: Repeat Steps 5 and 6 in succession until the last half-byte has been written into the last location of the MK memory.

Step 35: Set the EW switch to the off position.

At any time during the execution of this procedure, as when there is uncertainty that it has been correctly done, a restart can be accomplished by doing Step 35 and beginning again with Step 1.

Referring now to FIG. 22c1 and the timing diagram of FIG. 23, a more detailed description of the manual WMK operation will be given in the following. To initiate this operation, the Enable Write (EW) switch, which may be a SPDT switch activated by a physical key lock to prevent the key from being changed by unauthorized persons, is set to the ON position. Following this, the Manual Write (MW) switch, which may be a push-button switch, may be pressed to the MWNO position causing a negative pulse to be applied to turn on the MW latch 138. The latch 138 in being turned on applies a negative signal via the —MW line to turn on the MK BUS SELECT latch 140 and the manual write half byte (MWHB) control latch 154. The latch 140 in being turned on applies a positive signal to condition the AND circuits 164 in FIG. 22d1 for passing a half byte (4 bits) from the bit switches SW0-SW3. When the MW switch is released, it returns to the MWNC position causing a negative signal to be applied to reset the MW latch 138. The MW latch 138 in being reset applies a positive signal on the —MW line which together with the positive signal from the latch 140 renders the AND invert circuit 142 effective to apply a negative signal to turn on the ENABLE MAN RST latch 144. At 01 time of the next clock cycle, a 01 clock pulse together with the positive signal now on the —MW line and a positive signal from the latch 154 render the AND invert circuit 156 effective to apply a negative signal to the inverter 160 where it is inverted to a positive signal on the MWHB line. The positive signal on the MWHB line is applied to condition the AND invert circuits 152 and 158. The AND invert circuit 158 is effective to maintain the positive signal on the MWHB line until the next 01 time when a —01 clock pulse is applied to decondition the AND invert circuit 158 causing the positive signal on the MWHB line to be terminated thereby providing a 1 microsecond positive signal on the MWHB line. The AND invert circuit 152 is rendered effective by a 04 clock pulse in the present clock cycle for resetting the MWHB CTRL latch 154.

Referring now to FIG. 22c2, the positive signal on the MWHB line is inverted to a negative signal by inverter 162 to decondition the AND circuit 380 causing a negative signal to be applied to the —W ENABLE line and to decondition the AND inverter 376 which, in turn, applies a positive signal to the inverter 378 where it is inverted to a negative signal on the —M ENABLE line.

Signals on the $\overline{M}$ ENABLE and $\overline{W}$ ENABLE lines are used to enable the MK memory for writing and reading operations. The MK memory 700 shown in block form in FIGS. 22e1 and 22e2 is a 16 word by 4 bit CMOS random access memory (RAM) which is used for storing the master key. The MK memory 700 is addressed by a 4-bit value on the address lines $\overline{ADR1}$, $\overline{ADR2}$, $\overline{ADR3}$ and $\overline{ADR4}$ from the setting of the address counter 390 in FIG. 22d2. When negative signals are applied to both the $\overline{W}$ ENABLE and $\overline{M}$ ENABLE lines, the information present on the 4 bit input lines 0, 1, 2 and 3 is written into the MK memory 700 at the designated address. A transistor switch 139 is provided in series with the $\overline{W}$ ENABLE line to control writing into the MK memory 700. The potential at the base of this switch is controlled by the setting of the EW switch. Accordingly, when the EW switch is set on and a negative signal is applied to the $\overline{W}$ ENABLE line, the transistor 139 is turned on to produce a negative signal on the $\overline{W}$ ENABLE line to enable writing into the MK memory 700 whereas when the EW switch is set OFF the transistor switch 139 is biased off causing a positive signal to be maintained on the $\overline{W}$ ENABLE line to prevent writing into the MK memory 700. Addressing of the MK memory 700 for reading is accomplished in the same manner as that for writing. When a positive signal is applied to the $\overline{W}$ ENABLE line and a negative signal is applied to the $\overline{M}$ ENABLE line, the information which was written into the designated address of the MK memory 700 is read out in inverted form to the 4 bit output lines of the MK memory 700 and applied to a buffer register consisting of the 4 shift registers 702.

Referring now to FIGS. 22c1 and 22c2, during 03 time, a positive 03L clock pulse together with positive signals from the latches 144 and 146 render the AND invert circuit 148 effective to apply a negative signal to turn on the MAN RST latch 150 which remains set until the next clock cycle when a $\overline{01L}$ clock pulse is applied to reset latch 150 thereby providing a negative signal on the $\overline{MAN RST}$ line from 03L time to 01L time. The MAN RST latch 150 in being turned on applies a negative signal via the $\overline{MAN RST}$ line to reset the latch 146, to decondition the AND circuit 382, and to turn on the master key overwrite (MK OVW) latch 276 and the KEY INVALID latch 278 in FIG. 22c3. The AND circuit 382 in being deconditioned is effective to apply a negative signal to the reset inputs of the address counter 390 resetting the counter to an address of 0. The latch 276 in being set applies a negative signal on the $\overline{MK OVW}$ line to decondition the AND circuit 380 to maintain a negative signal on the $\overline{W}$ ENABLE line during the entire period of the master key overwrite operation. The negative signal on the $\overline{MK OVW}$ line is also applied to decondition the AND invert circuit 368 which, in turn, applies a positive signal to condition the AND invert circuits 370 and 374 during the entire period of the MK overwrite operation. Referring now to FIG. 22c1, at 01 time of the next clock cycle, a $\overline{01}$ clock pulse is applied to decondition the AND invert circuit 158 and apply a positive signal to the inverter 160 where it is inverted to a negative signal on the MWHB line which is maintained thereon for the balance of the overwrite operation. The negative signal is inverted to a positive signal and applied to one input of the AND invert circuit 376. However, at this time, namely, 01 time, positive signals are maintained at the inputs to the AND invert circuit 374 which is therefore

effective to apply a negative signal to the other input of the AND invert circuit 376 to maintain the AND invert circuit 376 deconditioned despite the signal change on the MWHB line. As a result, the AND invert circuit 376 maintains a positive signal output therefrom until 01L time when the $\overline{01L}$ clock pulse is applied to decondition the AND invert circuit 374 causing a positive signal to be applied to the AND invert circuit 376. Therefore, at this 01 time, the AND invert circuit 376 is rendered effective to apply a negative signal to the STEP CTR line and to the inverter 278 where it is inverted to a positive signal on the $\overline{M}$ ENABLE line.

It should be apparent that from the time the address counter 390 is reset to address 0, namely, at 03L time, until the present 01L time negative signals are maintained on both the $\overline{W}$ ENABLE and $\overline{M}$ ENABLE lines to allow a 4 bit value to be written into the MK Memory 700 at address 0. Referring now to FIG. 22d1, whatever the bit switches SW0 to SW3 happen to be set at are applied as a half byte value via the conditioned AND circuits 164 and OR invert circuits 168 to the bit inputs of the MK memory 700. For example, if the bit switch SW0 is set to the 1 position, a positive signal is applied to render the AND circuit 164a effective to apply a positive signal to the OR invert circuit 168a which, in turn, applies a negative signal as a 1 bit input to the MK memory 700. If the bit switch SW0 is set to the 0 position then a positive signal is applied as a 0 bit input to the MK memory 700.

Returning now to FIGS. 22c2 and 22d2, the negative signal applied to the $\overline{STEP CTR}$ line, at 01L time, is inverted by inverter 388 to a positive signal and applied via the STEP CTR line to step the address counter to an address count of 1 in preparation for writing the half byte value setting of switches SW0 to SW3 into the next location of the MK memory 700. AND invert circuits 374 and 376 are connected in a latching arrangement such that the negative signal output of the AND invert circuit 376 is effective to maintain the AND invert circuit 374 deconditioned after termination of the $\overline{01L}$ clock pulse and thereby maintain a positive signal input to the AND invert circuit 376 which together with the positive signal from the inverter 162 (due to the negative signal now maintained on the MWHB line) maintain the AND invert circuit 376 effective to maintain a negative signal output thereof (and a positive signal on the $\overline{M}$ ENABLE line). This condition will be maintained until 03L time, when a 03L clock pulse is applied to render the AND invert circuit 370 effective to apply a negative signal to now decondition the AND invert circuit 376. The AND invert circuit 376 in being deconditioned applies a positive signal to the inverter 378 where it is inverted to a negative signal on the $\overline{M}$ ENABLE line. The positive signal output of the AND invert circuit 376 will be operative in the latching arrangement of AND invert circuits 374 and 376 to maintain this signal output until 01L time of the next clock cycle when the $\overline{01L}$ clock pulse is applied to decondition the AND invert circuit 374. Accordingly, a negative signal will be maintained on the $\overline{M}$ ENABLE line from 03L time of the present clock cycle which together with the negative signal maintained on the $\overline{W}$ ENABLE line, due to the AND circuit 380 being maintained deconditioned by the MK OVW latch 276, allows writing of the half byte value setting of the switches SW0 to SW3 into the MK Memory at address 1.

In a similar manner, each succeeding 01L clock pulse will be effective to control stepping of the address counter 290 to the next address of the MK memory 700 and each succeeding 03L clock pulse will be effective to control writing the half byte value setting of the switches SW0 to SW3 into the MK memory 700 at the next address. After 16 such operations, the master key previously stored in the MK memory 700 will have been overwritten. Disclosure of the master key through unauthorized writing of trial half bytes into the MK memory 700 is thwarted by this overwriting operation of the previously stored master key when the MW switch is first pressed.

Referring now to FIG. 22d2, when the address counter 390 steps to a count of 8 (the 9th location in MK memory 700) a negative signal from the -C8 output is applied to set the 16 STEP latch 404 which, in being set, applies a positive signal to condition the AND circuit 406. After the 16th half byte is written into the MK memory 700, the address counter 390 is again stepped, at 01L time, back to an address count of 0 and a positive signal is applied via the -C8 output to render the AND circuit 406 effective to apply a positive signal to the inverter 408 where it is inverted to a negative signal on the -16 STEP line. The negative signal on the -16 STEP line is applied to reset the MK OVW latch 276 in FIG. 22c2 which, in being reset, applies a positive signal via the -MK OVW line to render the AND circuit 380 effective to apply a positive signal to the -W ENABLE line thereby inhibiting further writing into the MK memory 700. The positive signal on the -MK OVW line is also applied to render the AND invert circuit 368 effective to apply a negative signal to decondition the AND invert circuits 370 and 374 so that the -01L and 03L clock pulses will have no further effect. The jointly deconditioned AND invert circuits 370 and 374 will jointly apply a positive conditioning signal to one input of the AND invert circuit 376.

This completes the master key overwrite operation and the host operator may now proceed to load the new master key into the MK memory 700 a half byte at a time, for 16 times, in order to completely load the 64 bit master key into the MK memory 700. Referring to FIGS. 22c1 and 22d1 the host operator sets the switches SW0 to SW3 according to the first half byte of the master key to be loaded. Following this, the MW switch set to the MWNO position causing a negative pulse to be applied to turn on the MW latch 138. The MW latch 138 in being turned on applies a negative signal via the -MW line to set the MWHB CTRL latch 154 which, in being set, applies a positive signal to one input of the AND invert circuit 156. When the MW switch is released to the MWNC position, a negative signal is applied to reset the MW latch 138 which, in being reset, applies a positive signal to a second input of the AND invert circuit 156. Therefore, at 01 time of the next clock cycle, a 01 clock pulse is applied to render the AND invert circuit 156 effective to apply a negative signal to the inverter 160 where it is inverted to a positive signal on the MWHB line. The positive signal on the MWHB line is applied to the inverter 162 in FIG. 22c2 where it is inverted to a negative signal and applied to decondition the AND circuit 380 which, in turn, applies a negative signal to the -W ENABLE line. The negative signal from the inverter 162 is also applied to decondition the AND invert circuit 376 which, in turn, applies a positive signal to the inverter 378 where it is inverted to a negative signal on the -M ENABLE line.

The combination of negative signals on the -W ENABLE and -M ENABLE lines permits the first half byte of the new master key to be passed via the AND circuits 164 in FIG. 22d1 and the OR invert circuits 168 to be loaded into the MK memory 700 at location 0. Referring now to FIG. 22c1, at 04 time, a 04 clock pulse in combination with the positive signal on the MWHB line renders the AND invert circuit 152 effective to apply a negative signal to reset the MWHB CTRL latch 154 which, in being reset, applies a negative signal to decondition the AND invert circuit 156. At 01 time of the next clock cycle, a -01 clock pulse is applied to decondition the AND invert circuit 158 which, in turn, applies a positive signal to the inverter 160 where it is inverted to a negative signal on the MWHB line. The negative signal on the MWHB line is applied to the inverter 162 in FIG. 22c2 where it is inverted to a positive signal to render the AND circuit 380 effective to apply a positive signal to the -W ENABLE line to terminate the writing operation into the MK memory 700. The positive signal from the inverter 162 is also applied to render the AND invert circuit 376, conditioned by the positive signal output from the AND invert circuits 370 and 374, effective to apply a negative signal via the -STEP CTRL line to the inverter 378 where it is inverted to a positive signal on the -M ENABLE line. The negative signal on the -STEP CTRL line is also inverted by inverter 388 in FIG. 22d2 to a positive signal to step the address counter 390 to an address count of 1 in preparation for writing into the next location of the MK memory 700. Referring now to FIG. 22d1, the bit switches SW0 to SW3 are now set in accordance with the second half byte of the master key for loading into the MK memory 700. The MW switch is again set and the circuitry operates in the same manner as described above with respect to writing the first half byte for writing the next half byte of the new master key and stepping the address counter 390 to the next address. This operation is repeated for a total of 16 times in order to write the 16 half bytes of the master key into the MK memory 700.

After the last half byte of the new master key is loaded into the MK memory 700, the EW switch in FIG. 22c1 is switched off to terminate the manual write operation. The EW switch in being turned off applies a negative signal to reset the MK BUS SELECT latch 140 and to reset the ENABLE MAN RESET latch 144 which, in being reset, applies a negative signal to set the MAN RST CTRL latch 146 in preparation for the next time a manual write master key operation is to be performed.

ADDRESS DECODING AND SELECTION

Referring now to FIGS. 22a1 and 22a2, when an IO operation is to be performed, a negative signal is applied to the -IO tag line. The convention to be used in the following descriptions are that all lines are down level active i.e. the active state is the presence of a negative signal and, in the case of data, a 1 bit is represented as a negative signal and a 0 bit as a positive signal. Information is received by the DSD on a -DATA BUS OUT and may include address information, command information or data to be processed. Tag signals are used as control signals to identify the nature of the information being provided on the Data Bus. Thus, when an address is placed on the -DATA BUS OUT, a -TA signal is provided on the -TA tag line to identify the information as being address information, when a command is

placed on the bus, a -TC signal is provided on the -TC tag line to identify the information as being a command and when data is placed on the bus, a -TD, signal is provided on the -TD tag line to identify the information as being data. The -IO signal is inverted to a positive signal by the inverter 182 and applied to one input of the AND invert circuit 190. At TA time, address information is received on the -DATA BUS OUT and a -TA signal is applied to the inverter 184 where it is inverted to a positive signal and applied as a second input to the AND invert circuit 190.

The data security device can be personalized to be responsive to any one of 40 possible addresses. This is accomplished by jumpering each of the 3 pins, J5, J6 and J7 to either ground or +5v, and by jumpering one pin JU to any one of five others J0, J1, J2, J3 or J4. In the example shown, the wiring is such that the DSD responds to the address 1xxxx010. The 8 bit address is passed via the inverters 170 to the parity generator 178 which generates a parity bit which is compared with the parity bit received with the address. If the generated parity bit is equal to the received parity bit a positive signal is applied via the PARITY GOOD line to a third input of the AND invert circuit 190. Additionally, the personalized bits from the jumpers J5, J6 and J7 are compared with the inverted incoming bits on lines 5, 6 and 7 by the exclusive OR and inverter combinations 172 and 174 which produce positive signal inputs to the AND circuit 176 if a match is found. The personalized bit on the JU jumper is applied as the remaining positive input to render the AND circuit 176 effective for applying a positive signal to the remaining input of the AND invert circuit 190. Accordingly, if the personalized address having good parity has been detected, then the AND invert circuit 190 is rendered effective to apply a negative signal to set the SEL latch 192 and to decondition the AND circuit 216 in FIG. 22b1 which, in turn, produces a -VALID B signal indicating a valid address byte presentation. The SEL latch 192 remains set throughout the I/O operation unless reset subsequently by the occasion of a command error which will be described hereafter. The SEL latch 192, in being set, applies a positive signal via the SEL line to condition the AND invert circuits 204, 206 and 208. Referring now to FIG. 22a1, at the end of TA time, a positive signal is applied to the -TA tag line which is inverted to a negative signal by inverter 184 to decondition the AND invert circuit 190. Accordingly, AND invert circuit 190 applies a positive signal to render AND circuit 216 effective to terminate the negative signal on the -VALID B line.

COMMAND DECODING

At TC time, command information is received on the -DATA BUS OUT and a -TC signal is provided to indicate this condition. The low order command bit (bit 7) specifies the direction of the data transfer, i.e., whether the I/O operation is a read (bit 7=1) or a write (bit 7=0) operation. Referring now to FIG. 22a2, the I/O command byte is passed via the inverters 170 to the AND invert circuits 222 and to the parity generator 178 where a parity bit is generated and compared with the parity provided with the command byte by the exclusive OR 180. If the parity bit generated by the parity generator 178 is equal to the parity bit associated with the command byte then the exclusive OR 180 provides a positive signal on the PARITY GOOD line as a second input to the AND invert circuit 206. The -TC

signal is inverted by the inverter 188 to a positive TC signal and applied to the remaining inputs of the AND invert circuits 206 and 209. The AND invert circuit 206 is rendered effective to apply a negative signal via -TC SEL line to the inverter 214 and to decondition the AND circuit 216. The AND circuit 216 in being deconditioned applies a -VALID B signal to indicate that a valid command byte has been received. The inverter 214 inverts the negative signal to a positive signal on the TC SEL line which is applied to procedural error circuitry, which will be described hereafter, and to the other inputs of the AND invert circuits 222 in FIG. 22a2 to allow the I/O command byte to be loaded into the command register 224. The positive signal on the TC line in combination with the positive signal on the SEL line render the AND invert circuit 208, in FIG. 22b1, effective to apply a negative signal to set the TC END latch 210 which in being set, applies a positive signal to condition the AND circuit 218.

Referring now to FIGS. 22b2 and 22b3, the command and order codes of the command byte stored in the command register 224 during TC time are decoded by a series of AND invert circuits. Bits 4, 5, 6, and 7 are decoded to produce one of the seven defined commands described in the section DSD COMMANDS AND ORDERS. Thus, the AND invert circuit 226 decodes the PIOW data command (PIOW), the AND invert circuit 232 decodes the set basic status command (SET BS), the AND invert circuit 238 decodes the reset basic status command (RST BS), the AND invert circuit 242 decodes the read basic status command (RD BS), the AND invert circuit 250 decodes the reset adapter command (RST), the AND invert circuit 262 decodes the PIOR data command (PIOR) and the AND invert circuit 266 decodes the WR DSD order command (WR DSD). Detailed description of the operation of these commands will be provided hereafter.

In addition to the command code provided by bits 4, 5, 6 and 7 an order code WXYZ is provided by the other four bits, namely, bits 0, 1, 2 and 3 if the command is a WR DSD command. Thus, bits 0, 1, 2 and 3 of the order code are decoded to produce one of the five previously defined cipher handling orders or one of the two previously defined data processing orders. Accordingly, the AND invert circuits 280 and 302 decode a portion of the cipher key handling and data processing orders for (WMK) and (ENC or DEC), respectively, the AND invert circuits 288, 314, 340 and 341 decode the cipher key handling orders (DECK), (GRN), (RFMK), (EMK0) and (EMK1), respectively. Detailed decryption of the operation of these orders will be provided hereafter.

Referring now to FIG. 22a1, at the end of TC time, a positive signal is applied to the -TC tag line which is inverted to a negative signal by the inverter 188 and applied via the TC line to decondition the AND invert circuits 206 and 208. Accordingly, deconditioned AND invert circuit 206 applies a positive signal to render AND circuit 216 effective to terminate the negative signal on the -VALID B line. The positive signal from deconditioned AND invert circuit 206 is also applied to inverter 214 where it is inverted to a negative signal on the TC SEL line and applied to the procedural error circuitry and to decondition the AND invert circuits 222 associated with the command register 224 in FIG. 22a2. The deconditioned AND invert circuit 208 applies a positive signal to render the AND circuit 218, conditioned by the positive signal output of the TC End

latch 210, effective to apply a positive signal on the TC END line. If bit 7 of the decoded command code is a 1, indicating a read operation, then positive signals on the bit 7 line and the TC END line are applied to render the AND invert circuit 220 effective to produce a —P Valid signal to indicate that the parity of the data byte to be subsequently presented to the —DATA BUS IN is valid. This is so because the DSD always provides correct parity for data bytes it applies to the —DATA BUS IN for read type commands. The positive signal on the TC END line is also applied, in FIG. 22b2, to the inverter 244, AND circuit 254, inverter 258 to control the operation of the READ BS, RST and PIOR commands, respectively, and to AND invert circuit 356 in FIG. 22c4 to control the command error detection, all of which will be described in greater detail hereafter.

COMMAND ERROR DETECTION

Referring now to FIGS. 22b3 and 22c4 if one of the legal commands has been decoded, then a negative signal is applied to decondition either AND circuit 350 or AND invert circuit 352 to apply a positive signal to the LEGAL CMD line. The positive signal on the LEGAL CMD line is inverted by inverter 354 to a negative signal which is applied via the NO LEGAL CMD line to decondition the AND invert circuit 356. The AND invert circuit 356 in being deconditioned applies a positive signal which has no effect on the CMD ERR latch 358. On the other hand, if none of the legal commands are decoded, then the AND invert 352 is rendered effective to apply a negative signal to the inverter 354 where it is inverted to a positive signal and applied via the NO LEGAL CMD line to condition the AND invert circuit 356. At the end of TC time, the positive signal on the TC END line is applied to render the AND invert circuit 356 effective to apply a negative signal to set the CMD ERR latch 358 which is being set, applies a negative signal via the —CMD ERR line to reset the SEL latch 192 in FIG. 22a1 thereby deselecting the DSD due to the command error. Referring now to FIG. 22i2, the negative signal on the —CMD ERR line is also applied to set the machine check bit latch 954 E (bit 5) of the status register 952.

SYNC TD

At TD time, a —TD signal is provided to indicate that a data byte is present on the —DATA BUS OUT or that a data byte is on the —DATA BUS IN depending upon whether a write or read operation is to be performed. Additionally, because the clock 100 may run asynchronously with respect to the processor, it is necessary to provide a special timing signal for use during certain operations, this signal being called the SYNC TD signal. This signal begins at 01 time of a clock cycle coinciding with or following the beginning of a TD time and lasts until 01 time of the next clock cycle. It then remains inoperative until the next occurring TD time.

Referring now to FIG. 22a1, at TD time, the —TD signal is applied to the inverter 186 where it is inverted to a positive TD signal and applied in combination with a positive signal from the SYNCH latch 196 to condition the AND invert circuit 198. At 01 time, a 01 clock pulse is applied to render the AND invert circuit 198 effective to apply a negative signal to the inverter 202 where it is inverted to a positive signal on the SYNCH TD line. At 04 time, a 04 clock pulse in combination with the positive signal on the SYNCH TD line render

the AND invert circuit 194 effective to apply a negative signal to reset the SYNCH latch 196. At 01 time of the next clock cycle, a —01 signal is applied to decondition the AND invert circuit 200 causing a positive signal to be applied to the inverter 202 to terminate the positive signal on the SYNCH TD line, the positive signal having been present for a 1 usec clock cycle period. The positive signal on the SYNCH TD line is used to synchronize the PIOW data and WR DSD commands as will be described in greater detail hereafter.

Referring now to FIGS. 22a1 and 22b1, if the SEL latch 192 has not been reset by a command error, then positive signals on the SEL and TD line are applied to render the AND invert circuit 204 effective to apply a negative signal via the —TD SEL line to the inverter 212 and to decondition the AND circuit 216 causing a —VALID B signal to be produced indicating that the DSD was selected and a legal command was decoded. The inverter 212 inverts the negative signal to a positive signal on the TD SEL line which is used to determine whether there was a crypto engine data error during the execution of a PIOR Data command which will be described in greater detail hereafter and for controlling write error detection which will be described in the next section.

Referring now to FIG. 22a1, at the end of TD time, a positive signal is applied to the —TD tag line which is inverted to a negative signal by the inverter 186 and applied via the TD line to decondition the AND invert circuit 204. The AND invert circuit 204 in being deconditioned causes a positive signal to be applied to the —TD SEL line which, in turn, is applied to the inverter 212 and to render the AND circuit effective to terminate the negative signal on the —VALID B line. The inverter 212 inverts the positive signal to a negative signal on the TD SEL line which is applied to decondition the engine error circuitry in FIG. 22b3, to control circuitry in FIG. 22b2 for terminating the operation of the SET BS or RST BS commands and to decondition the write error circuitry in FIG. 22b3.

Following the end of TD time, the IO operation ends and a positive signal is applied via the —IO tag line to the inverter 182 where it is inverted to a negative signal to reset the SEL latch 192 and the WR ERR latch 364 in FIG. 22c4. The SEL latch 192 in being reset applies a negative signal to reset the command register 224 in FIG. 22a2 to reset the TC END latch 210 which, in being reset, applies a negative signal to decondition the AND circuit 218 thereby terminating the positive signal on the TC END line. The deconditioned AND circuit 218 causes a negative signal to be applied via the TC END line to decondition the AND invert circuit 220 thereby terminating the negative signal on the —P Valid line. The command register 224 in being reset deconditions all of the decoder circuitry in FIGS. 22b2 and 22b3.

WRITE ERROR DETECTION

Referring now to FIGS. 22b3 and 22c4, if a legal command has been decoded, indicated by a positive signal on the LEGAL CMD line, and the command is of the write type, indicated by a positive signal on the —7 line, and if the data byte on the BUS IN has bad parity, indicated by a positive signal on the PARITY BAD line, then, at TD time, the positive signal on the TD SEL line is applied to render the AND invert circuit 362 effective to apply a negative signal to set the WR ERR latch 364. This latch will remain set for the

duration of the IO operation or until the end of TD time for a RST command. The WR ERR latch 364 in being set applies a positive signal to set the status bit 3 latch 954D in the status register 952 in FIG. 22i2 to record the fact that a write error was detected.

ILLEGAL ORDER

If the DSD has been properly addressed and selected and if the command byte specifies an order code not recognized by the DSD, then this condition will be detected and the status bits 0 and 2 of the status register set to indicate this illegal order condition. More specifically, referring to FIG. 22b2, if a WR DSD ORDER command is decoded by the AND invert circuit 266, a negative signal is applied to the inverter 268 where it is inverted to a positive signal and applied via the WR DSD ORDER line to condition the AND circuit 270. At TD time, the positive signal on the SYNCH TD line is applied to render the AND circuit 270 effective to apply a positive signal via the WR ORD TIME line to one input of the AND invert circuit 348 in FIG. 22b3. The other inputs to the AND invert circuit 348 are the legal order codes recognized by the DSD. If none of these order codes occur, then positive signals are applied to the remaining inputs of the AND invert circuit 348 rendering it effective to apply a negative signal via the minus ILG ORD line to set the status bit 0 and 2 latches 954a and 954c of the status register 952 in FIG. 22i2.

WRITE MASTER KEY ORDER OPERATION

A general description of this operation will first be given followed by a more detailed description. Provided that the EW switch has been previously set to the on position, three latches are set when this order is decoded, namely, the WMK latch 274 in FIG. 22c3, the key invalid latch 278 and the master key overwrite latch (MW OVW) 276 in FIG. 22c2. The master key overwriting function, which is provided to destroy the previously stored contents of the MK memory 700, is accomplished by activating the write enable line, pulsing the memory enable line and stepping the address counter 390 in FIG. 2b2. Whatever happens to be present as bits 0, 1, 2 and 3 on the BUS IN will be written into the MK memory in all locations. The MK OVW latch 276 remains set for 16 microseconds and is reset after the 16th MK memory location has been overwritten. Thereafter, the actual master key is written with bits 0, 1, 2 and 3 from the data fields in a series of 16 PIOW data commands with one microsecond write enable and memory enable signals being provided for each SYNCH TD time. The address counter 390 is stepped at the conclusion of each pulse. There is no automatic termination of the write master key order. After the 16th half byte has been written into the MK memory 700, a RST command must be issued to reset the WMK latch 274 and regardless of whether the operation is under terminal control or manual control the EW switch must be set to the off position. The key invalid latch 278 is left set and no data can be processed until after a valid key is installed in the crypto engines by a DECK order. If the WMK order is issued while the EW switch is set in the off position, there is no action other than recording a procedural error. The WMK order is performed infrequently and is done only under physically secure conditions, as the master key appears in clear form in the machine at this time.

A more detailed description of the write key order operation will now be given and should be followed in conjunction with the timing diagram of FIG. 24. After address selection at TA time and loading of the command register 224 at TC time, the command code is decoded by the AND inverter circuit 266 in FIG. 22b2 to produce a negative signal which is inverted to a positive signal by the inverter 268 on the WR DSD ORDER line thereby indicating the presence of a WR DSD order command. The positive signal on the WR DSD ORDER line is applied to condition the AND circuit 270. At the same time, a portion of the order code is decoded by the AND invert circuit 280 to apply a negative signal via the -WMK DEC line to the inverter 282 where it is inverted to a positive signal and applied via the WMK line to one input of the AND invert circuit 272. A positive signal on the -Y line personalizes this order as a WMK order and is applied to a second input of the AND invert circuit 272. Referring now to FIG. 22c1, the EW switch will have previously been set to the on position, thereby permitting a positive signal from the +5V source to be applied as a third input to the AND invert circuit 272 in FIG. 22b2. At TD time, a positive signal is applied via the SYNCH TD line to render the conditioned AND circuit 270 effective to apply a positive signal via the WR ORD TIME line to the remaining input of the AND invert circuit 272. Accordingly, the AND invert circuit 272 is rendered effective to apply a negative signal via the -SET WMK line to set the WMK latch 274 in FIG. 22c3 and to set the MK OVW 276 in FIG. 22c2. The MK OVW latch 276 in being set applies a negative signal via the -MK OVW line to decondition the AND circuit 380 and the AND invert circuit 368. The deconditioned AND circuit 380 applies a negative signal to the -W ENABLE line to prepare the MK memory 700 for a writing operation. The AND invert circuit 368 in being deconditioned applies a positive signal to condition the AND invert circuit 370 and 374, in a manner as previously described in the manual WMK operation, for producing the successive signals on the -M ENABLE line during the memory overwrite operation. The WMK latch 274 remains set for the remainder of this operation and applies a positive signal to the WMK line and a negative signal to the -WMK line. The positive signal on the WMK line is applied to condition the AND invert circuit 366 in FIG. 22c2 in preparation for writing the new master key into the MK memory 700. The negative signal on the -WMK line is applied to set the KEY INVALID latch 278 which remains set for the remainder of this operation and will be reset only after a valid key is installed in the crypto engines by either a LKD or DECK order, either of which will cause a reset of this latch. The negative signal on the -WMK line is also applied to decondition the AND invert circuit 298 in FIG. 22c4 causing a positive signal to be applied to the K ORD line and via inverter 300 a negative signal to the -K ORD indicating that a key order operation is being performed.

Referring now to FIG. 22c2, at 03L time, a 03L clock pulse is applied to render the AND invert circuit 370 effective to apply a negative signal to decondition the AND invert circuit 376 which, in turn, applies a positive signal which is inverted by the inverter 378 to a negative signal on the -M ENABLE line. Accordingly, the presence of negative signals on the -W ENABLE and -M ENABLE lines enables the MK memory 700 for a write operation. Referring now to FIG.

22c1, since the MW switch has not operated, the MW latch 138 remains reset and likewise the MK BUS SELECT latch 140. The MK BUS SELECT latch 140 in being in a reset state applies a positive signal to condition the AND circuits 166 and a negative signal to decondition the AND circuits 164 in FIG. 22d1. In this case, the half byte value is not taken from the manual switches SW0 to SW3 but rather from whatever happens to be present on the bits 0, 1, 2 and 3 line of the BUS IN which will now be written into location 0 of the MK memory 700. Referring now to FIG. 22c2, the positive signal produced by the AND invert circuit 376 is applied to the AND invert circuit 374 the other inputs of which have positive signals maintained thereon at this time causing a negative signal to be applied to the AND invert circuit 376 to maintain the positive signal output thereof until 01L time of the next clock cycle. At that time, a -01L clock pulse is applied to decondition the AND invert circuit 374 which, in turn, applies a positive signal to render the AND circuit 376 effective to apply a negative signal to the -STEP CTR line and to the inverter 378 where it is inverted into a positive signal on the -M ENABLE line. The negative signal on the -STEP CTR line is inverted by the inverter 388 in FIG. 22d2 to a positive signal which is applied via the -STEP CTR line to step the address counter 390 to an address count of 1 indicating the next location of the MK memory 700. In a similar manner each successive 03L clock pulse is effective to control the application of a negative signal on the -M ENABLE line to permit half byte value on the BUS IN to be written into and overwrite the previous master key half byte at that location and each succeeding -01L clock pulse is effective to control the termination of the negative signal on the -M ENABLE line and to step the address counter 390 to the next location as previously described in connection with the manual write master key operation. Similarly, when a count of 16 is reached and the address counter 390 returns to an address count of 0, the negative signal on the -16 STEP line is applied to reset the MK OVW latch 276 to thereby terminate the MK overwrite operation.

Following the end of the MK overwrite operation, the first of 16 PIOW data commands is provided to the DSD. After address selection during the TA time and loading of the command byte in the command register during TC time, in a manner previously described, the AND invert circuit 226 in FIG. 22b2 decodes this command and applies a negative signal via the -PIOW DATA DEC line to one input of the OR invert circuit 230. At TD time, a positive signal on the SYNCH TD line is inverted by the inverter 228 to a negative signal to the other input of the OR invert circuit 230 which, in turn, applies a positive signal to the PIOW DATA line. The positive signal on the PIOW DATA line is applied to the AND invert circuit 366 in FIG. 22c2 which in combination with the positive signal on the MK line renders the AND invert circuit 366 effective to apply a negative signal to decondition the AND circuit 380 and the AND invert 376 for the period of the SYNC TD pulse. The AND circuit 380 in being deconditioned applies a negative signal to the -W ENABLE line. The AND invert circuit 376 in being deconditioned applies a positive signal which is inverted by inverter 378 to a negative signal on the -M ENABLE line. The combination of negative signals on the -W ENABLE and -M ENABLE lines permit the bits 0, 1, 2 and 3 of the data field associated with the PIOW command, which is

the first half byte of the new master key, to be written into location 0 of the MK memory 700. At the end of SYNC TD time, a negative signal is applied to the SYNC TD line which is inverted by inverter 228 in FIG. 22b2 to a positive signal which renders the AND invert circuit 230 effective to apply a negative signal via the PIOW DATA line to decondition the AND invert circuit 366 in FIG. 22c2. Accordingly, AND invert circuit 366, in being deconditioned, applies a positive signal to condition the AND circuit 380 and the AND invert circuit 376. The AND circuit 380 in being conditioned applies a positive signal on the -W ENABLE line while the AND invert circuit 376 in being conditioned applies a negative signal to the -STEP CTR line and is inverted by the inverter 378 to a positive signal on the -M ENABLE line. The positive signals on the -W ENABLE AND -M ENABLE lines inhibit further writing operations into the MK memory 700. The negative signal on the -STEP CTR line is inverted by inverter 388 in FIG. 22d2 to a positive signal on the STEP CTR line to step the address counter 390 to an address count of 1 representing the next address for the MK memory 700. In a similar manner, succeeding negative signals on the -W ENABLE and -M ENABLE lines are provided for succeeding SYNC TD times to write the succeeding half bytes of the new master key into the MK memory 700 with the address counter 390 being stepped at the conclusion of each succeeding SYNC TD signal.

After the sixteenth half-byte value has been written into the MK memory 700, the WMK order operation is completed by setting the EW switch in FIG. 22c1 to the off position which, in turn, causes a negative signal to be applied to decondition the AND invert circuit 272 in FIG. 22b2 and inhibit the performance of any subsequent WMK order operation so long as the EW switch remains off. This concludes the description of the WMK order operation. However, it should be noted that the MK latch 274 in FIG. 22c3 remains set until such time as a RST command is issued to reset this latch and that the KEY INVALID latch 278 also remains set and no data can be processed until after a valid key is installed in the crypto engine by a DECK order as will be described in greater detail hereafter.

RESET ADAPTER COMMAND OPERATION

The execution of this command causes a RST signal to be created from the end of TC time until the end of I/O operation. This signal is used to reset all counters, flip-flops and latches in the adapter and control section. Nothing in the crypto engines are reset and the data field associated with this command is ignored. The same reset signal can also be created by a discrete reset signal on the -RESET line from the I/O interface.

A more detailed description of the reset adapter command operation will now be given in conjunction with the timing diagram in FIG. 24. After the address selection is performed during TA time and the command byte is loaded into the command register during the TC time, as previously described, the AND invert circuit 250 in FIG. 22b2 decodes the RST command code and produces a negative signal which is applied to the inverter 252 where it is inverted to a positive signal and applied to one input of the AND circuit 254. At TC time, a positive signal on the TC END line is applied to render the AND circuit 254 effective to apply a positive signal to the OR invert circuit 256 which, in turn, applies a negative signal on the RST line. A similar opera-

tion may be initiated by a discrete negative signal on the —RESEt line from the I/O interface in FIG. 22a2 which is inverted by the inverter 248 to apply a positive signal to the OR invert circuit 256 which, in turn, applies a negative signal to the —RST line. As mentioned above, this signal is used to reset all counters, flip-flops and latches in the adapter and control sections that are not automatically reset by the clock 100 or tag signals. If this command is issued after a WMK order command, then the negative signal on the —RST line is applied to reset the WMK latch 274 which, in being reset, applies a positive signal in the —WMK line to render the AND invert circuit 298 in FIG. 22c5 effective to apply a negative signal on the K ORD line and via the inverter 300 a positive signal on the —K ORD line.

INPUT/OUTPUT MANAGEMENT AND CONTROLS

Before proceeding to various order commands which involve the use of the crypto engine, a description will be given of the I/O management technique used in the DSD as well as some of the major controls used in such management. Referring now to FIGS. 22/1 and 22g1, one of the crypto engines is shown in block form and includes a 64-bit input/output buffer register divided into an upper buffer register UBR 100 and a lower buffer register LBR 150 of 32 bits each. The buffer register is used for both input and output operations in a mutually exclusive manner for receiving an input block of data by a series of 8 PIOW DATA commands, termed an input cycle or for producing an output block of data by a series of 8 PIOR data commands, termed an output cycle. During each input cycle, an 8 byte block of input data is written into the buffer register on a serial-by-byte basis from the terminal memory and during each output cycle an 8 byte block of output data is read from the buffer register on a serial-by-byte basis to the terminal memory. During the input cycle, each received byte is parity checked for odd parity over nine bits and during the output cycle to each byte is appended a parity bit to achieve odd parity over nine bits. Principal input/output controls which are used for the I/O management include: (1) an input cycle latch 454 in FIG. 22e3 which is set by a PIOW data command, except during the execution of a WMK order command, and remains set until after 8 PIOW data commands have been counted by a byte counter 448 in FIG. 22d4; (2) an output cycle latch 464 in FIG. 22e3 which is set by a PIOR data command, by the conclusion of the input cycle during the LKD order operation or by the conclusion of the deciphering process during the execution of the DECK order operation, and remains set until after the 8 PIOR data commands have been counted or until after 8 buffer to key register shifts have been counted by the byte counter; (3) a byte counter 448 which counts the number of shifts of the buffer register as it is being loaded or unloaded by PIOW or PIOR data commands, respectively, or as a cipher key is being transferred from the buffer register to the key register; and (4) a block counter 414 in FIG. 22d3 which is set at the end of every input cycle and is reset at the end of every output cycle.

CRYPTO ENGINE CONTROLS

The crypto engine used in the present invention is similar in detail to that shown and described in the aforementioned U.S. Pat. No. 3,598,081. One difference between the engine shown in the aforementioned patent

and that in the present invention is that in the aforementioned patent the crypto engine is provided with separate input and output buffer registers whereas in the crypto engine of the present invention a single input/output buffer register is provided and used, in a mutually exclusive manner, for input/output operations. However, while there is a difference in design detail between the previous and the present crypto engine, the algorithm performed by both is identical. Additionally, the crypto engine of the aforementioned patent discloses how the basic encipher/decipher operations are performed with the cipher key being loaded directly into the key register as a working key whereas, in the present invention, in addition to being loaded directly into the key register from the MK memory 700, it is also loaded as a working key into the key register via the input/output buffer register when the cipher key is provided from the host memory during a DECK operation. The details of these modifications of the prior crypto engine are shown in FIG. 25a to FIG. 25c and correspond to FIGS. 3a to 3d of the aforementioned patent with the notations used being identical for both except for the lines labeled ER and LBR which correspond to lines labeled LB and IBT in the aforementioned patent. The various control signals used in the crypto engine and their function will be generally described in the following and the operation of the modified crypto engine will be described in conjunction with the detailed descriptions of the various command operations which will be described hereafter.

Load Input Buffer (LIB)—This signal is used for loading and unloading the buffer registers UBR 100 and LBR 150. During an input cycle, this signal causes a data byte presently on the BUS IN to be latched in and simultaneously shifted in the buffer registers. After eight such actions, the loading operation is complete. During an output cycle, a data byte is outputted, after which this signal causes the buffer registers UBR 100 and LBR 150 to be shifted in preparation for outputting the next data byte. After eight such actions, the unloading operation is complete.

Load Key Register From Buffer (LKB)—This signal is essentially identical to the LIB signal and is produced during the output cycle of LKD or DECK operations causing the buffer register output to be latched into the key registers UKR 350 and LKR 400.

Load Data Register (LDR) and End of Last Round (ELR)—These signals are simultaneously produced from the same source with LDR causing the content of the buffer register UBR 100 and LBR 150 to be transferred to the data registers UDR 200 and LDR 250 and ELR causing the contents of the data registers UDR 200 and LDR 250 (via the cipher function circuits) to be transferred to the buffer registers UBR 100 and LBR 150, the simultaneous action constituting a swap of the contents of the buffer and data registers.

Engine Busy (EB)—This control signal is produced during actual data ciphering operations and occurs from the end of the input cycle to the end of the last of the 16 rounds of the cipher function.

End of Round (ER)—This signal is used to latch up the intermediate results of each round in the data registers UDR 200 and LDR 250.

End of Round 16 (ER16)—This signal is used to latch up the final result output of the cipher function circuits to the lower data register LDR 250.

Load Master Key (LDK)—This signal causes the contents of the MK memory buffer 702 to be latched into the key registers UKR 350 and LKR 400.

Shift Right (SR), Shift Right and Recirculate (SRR) and Shift Left (SL)—The SR signal is used to shift the key registers UKR and LKR 400 to the right when a cipher key is being loaded from either the MK memory 700 or the buffer registers UBR 100 and LBR 150. The SRR signal configures the key register UKR 350 and LKR 400 into two recirculating right shifting registers. During the decipher process, the SR and SRR control signals cause the key registers to be shifted to the right. During the encipher operation, the SL control signal configures the key registers UKR 350 and LKR 400 into two recirculating left shifting registers which are shifted to the left.

DECIPHER KEY ORDER OPERATION

The function of this operation is to decipher an enciphered operational key and then load the operational key in clear form as the working key in the key registers of the crypto engines for subsequent data processing operations.

When the order code specifying this order is decoded, a decipher key (DECK) latch is set, a load master key (LMK) latch is set, the key invalid latch is reset (having been set and remain set by a previous WMK order command if that command preceded the present one) to permit data to be subsequently processed since a new working key is to be written into the key registers of the crypto engines by the present operation and an encipher (ENC) latch is reset so that the processing mode is set for a decipher operation. With the LMK latch set, the contents of the MK memory is caused to be read out and transferred, a byte at a time, to the crypto engines. The master key is parity checked, a byte at a time, and loaded as a working key directly into the key registers of the crypto engines. Concurrently with (or after) loading the master key into the key registers, a series of 8 PIOW commands are received with the data fields associated with the commands, constituting the enciphered operational key to be deciphered under control of the master key, being loaded into the buffer registers of the crypto engines. The first such command initiates an input cycle and a byte counter counts each such command received. After the 8 PIOW commands have been received and the 8th byte written into the buffer registers, then, at the 8th count, the input cycle ends, the enciphered operational key is transferred from the buffer registers to the data registers of the crypto engines, a block counter is set and the crypto engines start a decipher operation which is indicated by the generation of an engine busy signal. At the end of the decipher operation, the operational key, now in clear form, is loaded into the buffer registers of the crypto engines and an output cycle is started. During the output cycle, the buffer registers and the key registers are shifted in synchronism, once for each clock cycle, causing the operational key presently in the buffer registers to be shifted into the key registers. During this transfer, the byte counter counts the clock cycles and after the 8th count, the output cycle ends, the block counter is reset and the DECK latch is reset to end the operation. Any attempt to read the contents of the buffer registers while the operational key is present in clear form will be detected and cause a procedural error as will be described in greater detail hereafter.

A more detailed description of the decipher key operation will now be given in conjunction with the timing diagrams of FIGS. 26a—26c. After address selection at TA time and loading the command byte into the command register at TC time, the command code is decoded by AND invert circuit 266 in FIG. 22b2 to produce a negative signal which is inverted by inverter 268 to a positive signal on the WR DSD ORDER line thereby indicating the presence of a WR DSD order command. At the same time, the order code is decoded by the AND invert circuit 288 to apply a negative signal via the —DECK DEC line to the inverter 290 where it is inverted to a positive signal and applied to one input of the AND invert circuit 292. At TD time, a positive signal is applied via the SYNCH TD line to render the AND circuit 270, conditioned by the positive signal on the WR DSD ORDER line, effective to provide a positive signal on the WR ORD TIME line which is applied to the remaining input of the AND invert circuit 292 to render it effective to produce a negative signal on the —SET DECK line. The negative signal on the —SET DECK line is applied to set the DECK latch 296 in FIG. 22c3, to reset the key invalid latch 278, to set the LMK latch 566 in FIG. 22g4 and to decondition the AND invert circuit 368 in FIG. 22c2. The AND invert circuit 368 in being deconditioned applies a positive signal to condition the AND invert circuits 370 and 374 which will be used for controlling a MK memory read-out as will be described hereafter. The LMK latch 566 in being set applies a negative signal via the —LMK via line, in FIG. 22c2, to maintain the AND invert circuit 368 deconditioned and thereby maintain the AND invert circuits 370 and 374 conditioned while the LMK latch remains set i.e. during the MK memory read out time. Referring now to FIGS. 22c3, 22c4 and 22d5, the DECK latch 296 in being set applies a negative signal via the —DECK line to decondition the AND invert circuit 298 which, in turn, applies a positive signal on the K ORD line and via inverter 300 a negative signal on the —K ORD line thereby providing indications that this is a key order operation. The negative signal on the —K ORD line is applied to reset the ENC latch 312. Since DECK latch 296 is set, a positive DECK signal is applied to OR invert circuit 492, resetting SPEC ENC latch 494. The ENC latch 312, and SPEC ENC latch 494, being reset, apply a negative signal via OR circuit 522 to the ENC line which, in FIG. 22g3 is inverted to a positive signal by the inverter 546 to provide a positive signal on the DEC line indicating a decipher mode of operation.

Referring now to FIG. 22c2, negative signals are applied to the inputs of the AND invert circuit 366 and a negative signal is applied to the inverter 162 both of which cause a positive signal to be applied to one input of the AND circuit 380 and to condition the AND invert circuit 376. Additionally, the MK OVW latch 276, presently in a reset state, causes a positive signal to be applied via the —MK OVW line to the other input of the AND circuit 380 rendering it effective to apply and maintain a positive signal on the —W ENABLE line. At 03L time, 03L clock pulse is applied to render the AND invert circuit 370 effective to apply a negative pulse to decondition the AND invert circuit 376 which, in turn, applies a positive signal to the inverter 378 where it is inverted to a negative signal on the —M ENABLE line. The positive signal on the —W ENABLE line together with the now negative signal on the —M ENABLE line are effective to cause the first

half byte at location 0 of the MK MEMORY 700 to be read out. at 01 time of the next clock cycle, a 01 clock pulse is effective to shift the half byte into the shift registers 702 in FIG. 22e1. Referring now to FIG. 22c2, at 01L time, a -01L clock pulse is applied to decondition the AND invert circuit 374 which, in turn, applies a positive signal to render the AND invert circuit 376 effective to apply a negative signal to the -STEP CTR line and to the inverter 378 to apply a positive signal on the -M ENABLE line. The negative signal on the -STEP CTR line is applied to the inverter 388 where it is inverted to a positive signal to step the address counter 390 to an address count of 1 and cause a positive signal to be provided on the CI line. At 03L time, a 03L clock pulse is again applied to render the AND invert circuit 370 effective to initiate production of a negative signal, via the AND invert circuit 376 and the inverter 378, on the -M ENABLE line. The positive signal on the -W ENABLE line in combination with the negative signal on the -M ENABLE line is again effective to cause the next half byte at location 1 of the MK memory 700 to be read out. At 01 time of the next clock cycle, a 01 clock pulse is effective to shift the next half byte into the first stages of the shift register 702 and to shift the previous half byte read out of the MK memory 700 to the second stages of the shift registers 702. As a result of this action, the first full byte of the cipher key is now stored in the shift registers 702.

Referring now to the AND invert circuit 568 in FIG. 22b4, a 01 DEL clock pulse in combination with positive signals on the CL, -STEP CTR and LMK lines are applied to render the AND invert circuit 568 effective to apply a negative signal to set the LDK latch 570 which, in being set, applies a negative signal via the -LDK line to decondition the AND circuit 572 and to one input of the OR invert circuit 576. The deconditioned AND circuit 572 causes a negative signal to be applied via the -SR line to one input of the OR invert circuit 574.

Referring to the AND invert circuit 374 in FIG. 22c2, at 01L time, a -01L clock pulse is applied to decondition the AND invert circuit 374 causing a positive signal to be applied to render the AND invert circuit 376 effective to apply a negative signal to the -STEP CTR line and via the inverter 378 to a positive signal on the -M ENABLE line. The negative signal on the -STEP CTR line is inverted by the inverter 388 to a positive signal to step the address counter to an address count of 2 and causing a negative signal to now be applied to the CI line.

Referring now to the OR invert circuits 574 and 576 in FIG. 22g4, at 02 time, a -C clock pulse is applied to the other inputs of the OR circuits 574 and 576 causing them to apply positive signals via the SR and LDK lines respectively, to the control signal cable connected to the crypto engines. The positive signal on the SR line is also applied to the OR invert circuit 606 in FIG. 22h4 causing a negative signal, delayed by delay circuit 608, to be applied via LDK line to the control signal cable.

Referring now to the crypto engines in FIG. 22g1, the positive signal on the LDK line is applied to condition the AND circuit 807 to permit a parity check to be made of the first byte of the cipher key stored in the shift registers 702 to be checked for a parity error. The positive signals on the SR, LDK and LDK lines are applied as control signal inputs to the key registers UKR 350 and LKR 400 to shift the key register and

allow the first byte of the cipher key, passed via the P box 300, to be latched into the key registers.

Referring now to FIG. 22c2, at 03L time, a 03L clock pulse is again applied to render the AND invert circuit 370 effective to initiate production of a negative signal on the -M ENABLE line to permit the third half byte to be read out of the MK memory 700 from location 2. Referring now to FIG. 22g4, at 01 time of the next clock cycle, a -01 clock pulse is applied to reset the LDK latch 570 to inhibit production of the control signals for the crypto engine during this clock cycle in order to permit the next half byte to be read out of the MK memory 700 and shifted into the shift registers 702 in FIG. 22e1. Accordingly, referring to FIG. 22e1, at the same time that the LDK latch 570 is reset, a 01 clock pulse is applied to shift the next half byte from the MK memory 700 into the shift registers 702.

In a similar manner, during each succeeding clock cycle, a half byte of the cipher key is read out of the MK memory 700 and shifted into the shift registers 720 and the address counter 390 stepped to the next address count. After each second clock cycle, when a full byte of the cipher key is loaded into the shift registers 720, control signals are provided on the LDK, SR and LDK lines to parity check the cipher key byte and to simultaneously shift the previously loaded byte one position to the right and to latch up the newly entered byte in the key registers in the crypto engine.

Referring now to FIG. 22d2, when the address counter 390 steps to an address count of 8 (the 9th address location), a negative signal is produced on the -C8 line to set the 16 STEP latch 404 which, in being set, applies a positive signal to one input of the AND circuit 406. After the 8th byte is loaded into the key registers, the address counter 390 steps from an address count of 15 back to an address count of 0 (count of 16) causing a positive signal to be produced on the -C8 line which is applied to condition the AND invert circuit 402 and to the other input of the AND circuit 406. The AND circuit 406 is rendered effective to produce a positive signal which is inverted by inverter 408 to a negative signal on the -16 STEP line to reset the LMK latch 566 in FIG. 22g4. The LMK latch 566 in being reset applies a negative signal via the LMK to decondition the AND invert circuit 568 and inhibit further setting of the LDK latch 570 and further production of crypto engine control signals on the LDK, SR and LDK lines. Referring to FIG. 22d2, at 04 time of the 16th clock cycle, a 04 clock pulse is applied to reset the 16 STEP latch 404.

After loading the master key into the key registers of the crypto engines the first of a series of 8 PIOW data commands is now received by the DSD and after address selection at TA time and command loading into the command register at TC time, the AND invert circuit 226 in FIG. 22b2 decodes this command causing a negative signal to be applied to one input of the OR invert circuit 230. At TD time, a positive signal on the SYNCH TD line is inverted by inverter 228 to a negative signal to the other input of the OR invert circuit 230 which, in turn, applies a positive signal to the PIOW data line. The positive signal on the PIOW data line is applied to the AND invert circuit 426 in FIG. 22d3 which is presently conditioned by a positive signal on the -WMK line. Accordingly, the AND invert circuit 426 is rendered effective to apply a negative signal to one input of the OR invert circuit 430. At this time, positive signals are maintained at the input of the AND

invert circuit 428 causing a negative signal to be applied to the other input of the OR invert circuit 430. The negative signal inputs to the OR invert circuit 430 causes a positive signal to be applied via the PIOW line to condition the AND invert circuit 431, to condition the AND invert circuit 444, in FIG. 22d4, and to be applied to the inverter 596 in FIG. 22g3 where it is inverted to a negative signal to decondition the AND circuit 600 which, in turn, applies a negative signal on the —LIB line to one input of the OR invert circuit 602. At —C time, a —C clock pulse is applied to the other input of the OR invert circuit 602. The negative signal inputs to the OR invert circuit 602 causes a positive signal to be applied via the LIB line and the control line but to the crypto engines and to the OR invert circuit 648 in FIG. 22h4. The OR invert circuit 648 is rendered effective to apply a negative signal to the delay circuit 650, which provides a 250ns time delay, and via the LIB line and the control line bus to the crypto engines. Referring now to FIGS. 22f1 and 22g1 the combination of signals on the LIB and LIB lines are effective to permit the data field associated with the first PIOW data command to be loaded from the BUS IN via the P box 50 into the buffer registers UBR 100 and LBR 150 in each crypto engine.

Referring now to FIG. 22e3, at 03L time of the clock cycle, a 03L clock pulse is applied to render the conditioned AND invert circuit 431 effective to apply a negative signal to set the INPUT CYCLE latch 454 to start the input cycle operation. The INPUT CYCLE latch 454 in being set applies a negative signal via the —IN CYCLE line to set the START IN CYCLE END latch 530 which, in being set, applies a positive signal to one input of the AND invert circuit 532. Referring now to FIG. 22d4, at 04 time, a 04 clock pulse is applied to render the conditioned AND invert circuit 444 effective to apply a negative pulse to the STEP BYTE CTR line, the positive trailing edge of which is effective to step the byte counter 448 to a count of one.

In a similar manner, succeeding ones of the data fields associated with the series of 8 PIOW data commands are loaded into the buffer registers UBR 100 and LBR 150 with the previous byte being simultaneously shifted and the byte counter 448 counting each such byte received. After the 8th byte is written into the buffer registers, the byte counter 448 steps from a count of 7 back to a count of 0 causing a negative signal to be produced to set the COUNT 8 latch 450 which, in turn, applies a negative signal to the —CT8 line. The negative signal on the —CT8 line is applied to reset the INPUT CYCLE latch 454 in FIG. 22e3 thereby ending the input cycle. The INPUT CYCLE latch 454 in being reset applies a positive signal via the —IN CYCLE line to the AND invert circuit 410 in FIG. 22d3. The combination of positive signals on —IN CYCLE and —OUT CYCLE lines are applied to render the AND invert circuit 410 effective to apply a negative signal to reset the COUNT 8 latch 450 in FIG. 22d4 and is inverted by inverter 412 to a positive signal to set the BLOCK COUNT flip flop 414 producing a positive signal on the —BLK0 line and a negative signal on the —BLK1 line.

Referring now to FIGS. 22e3 and 22f3, positive signals on the —IN CYCLE line and from the START IN CYCLE END latch 530 are applied to condition the AND invert circuit 532. At the next 01 time, the AND invert circuit 524 is rendered effective to apply a negative pulse, from 01 time to 01L time, on the —01/L line to inverter 526 where it is inverted to a positive pulse

which is applied via the 01 DEL line to render the now conditioned AND invert circuit 532 effective to apply a negative pulse to set the IN CYCLE END latch 534 which, in being set, applies a positive signal to the IN CYCLE END line.

Referring now to FIG. 22f4, the positive signal on the IN CYCLE END line is applied to the inverter 622 where it is inverted to a negative signal and applied to decondition the AND circuit 626 causing a negative signal to be applied to set the START EB latch 628 and to the inverter 638 in FIG. 22g4 where it is inverted to a positive signal and applied to the OR invert circuit 640 which produces negative signals on the —ELR and —LDR lines. The negative signal on the —ELR line is applied to one input of the OR invert circuit 642 and, in FIG. 22c2 to decondition the AND circuit 382 causing a negative signal to be applied to reset the counter 390 in FIG. 22d2 in preparation for this counter to operate as a round counter for the 16 rounds of operation of the cipher engines. The negative signal on the —LDR line is applied to one input of the OR invert circuit 644. At 02 time, a —C clock pulse is applied to the other inputs of the OR invert circuit 642 and 644 causing positive signals to be applied via the ELR and LDR lines, respectively, to the control signal cable connected to the crypto engines. The positive signal on the ELR line is also applied to the OR invert circuit 648 causing a negative signal, delayed by the 250ns time delay circuit 650, to be applied via the LIB line to the control signal cable. The positive signal on the LDR line is applied to the OR invert circuit 652 causing a negative signal, delayed by the 250ns time delay circuit 654 to be applied via the LDR line to the control signal cable.

Referring now to the crypto engines in FIG. 22g1, the control signals LDR and LDR are effective for parallel transferring the contents of the buffer registers UBR 100 and LBR 150 to the data registers UDR 200 and LDR 250. The control signals ELR and LIB are effective for causing the contents of the upper data register UDR 200 and the lower data register LDR 250 (via the cipher function circuits) to be transferred to the upper buffer register UBR 100 and the lower buffer register LBR 150, the transfer to the buffer registers being of no consequence at this time but will be of consequence at the end of the 16th round of operation of the crypto engines. At this time, with the enciphered operational key presently stored in the data registers and the cipher key stored in the key registers, the crypto engines are now effective to perform a decipher function in a manner described in detail in the aforementioned U.S. Pat. No. 3,958,081. Reference may be made to the aforementioned patent for a more detailed description of the decipher function.

A description of the manner in which the crypto engine control signals are produced will now be given and can be followed in conjunction with the timing diagram in FIG. 26. Referring now to FIG. 22f3, at 01/L time, a —01/L clock pulse is applied to reset the IN CYCLE END latch 534 which, in being reset, applies a negative signal to inverter 622 in FIG. 22f4, where it is inverted to a positive signal to be applied to render the AND circuit 626 effective and together with the positive signal from the set START EB latch 628 renders the AND invert circuit 630 effective to apply a negative signal to set the EB latch 632 indicating the start of the crypto operation. The EB latch 632 in being set applies a positive signal to the EB line and a negative signal to the —EB line. The positive signal on the EB

line is applied to one input of the AND invert circuit 398 in FIG. 22d2 and to condition the ER flip flop 384 in FIG. 22c2 while the negative signal on the —EB line is applied to set the START EB END latch 612.

The cipher function is performed by repeating a product cipher function 16 times, termed 16 rounds, with each round being carried out in two clock cycles for a total of 32 clock cycles per cipher function. During each round, the data contents of the upper data register UDR 200 is ciphered (in the present case deciphered) under control of the contents of the key registers UKR 350 and LKR 400 with the results being added to the contents of the lower data register LDR 250 by modulo-2 adders 650-664. At the end of each round, the outputs of the modulo-2 adders are parallel transferred to the upper data registers UDR 200 while the contents of the upper data registers UOR 200 are parallel transferred to the lower data register LDR 250 to form the arguments for the next round.

Referring now to FIG. 22d2, during the cipher function operation the counter 390 functions as a round counter. The round counter 390 is stepped every 2 clock cycles from a count value of 0 to a count value of 15 providing a total count of 16 for the 16 rounds. Stepping of the round counter 390 is accomplished under control the ER flip flop 384 after being enabled by the positive signal on the EB line. Thus, at 01 time following the conditioning of the ER flip flop 384, a 01 clock pulse is applied to set the flip flop 384 and at 01 time of the succeeding clock cycle, a 01 clock pulse is again applied to reset the flip flop 384 which in being reset applies a negative signal to inverter 386 where it is inverted to a positive signal and applied to step the round counter 390. Therefore, it should be apparent, that the round counter 390 is stepped to the next count every 2 clock cycles. Additionally, during the first clock cycle of each round, ER flip flop 384 being in a reset state, applies a positive signal via the —ER FF line to one input of the AND invert circuit 400. The other input to the AND invert circuit 400 is connected to a round count decoder consisting of AND invert circuits 392, 394, 396 and 398 which is effective, while a positive signal is maintained on the EB line, to produce a positive signal at the output of the AND invert circuit 398 when the round count is 0, 7, 14 or 15 and a negative signal at all other times. Thus, during the first clock cycle of rounds 0, 7, 14 and 15, the combination of positive signals on the —ER FF line and the output of the AND invert circuit 398 will render AND invert circuit 400 effective to apply a negative signal on the CT 0, 7, 14, 15 line whereas during the first clock cycle of all other rounds the negative signal output of the AND invert circuit 398 deconditions the AND invert circuit 400 causing a positive signal to be applied to the CT 0, 7, 14, 15 line. During the second clock cycle of every round, the ER flip flop 384 is in a set state causing a negative signal to be applied to decondition the AND invert circuit 400, which, in turn, applies a positive signal to the CT 0, 7, 14, 15 line. Thus, it should be apparent, that a positive signal is maintained on the CT 0, 7, 14, 15 line during every round count except during the first clock cycle of round count 0, 7, 14 and 15 with one exception, namely, during the second cycle of the round count 15 (16th round). This is so because of the fact that the EB latch 632 in FIG. 22f4 is reset at the end of the first clock cycle of the 16th round to terminate the positive signal on the EB line and thereby inhibit production of a positive signal on the CT 0, 7, 14, 15 line

during the second clock cycle. Therefore, a positive signal is maintained on the CT 0, 7, 14, 15 line from the beginning of the second clock cycle of round count 0 to the end of the second clock cycle of round count 6, then from the beginning of the second clock cycle of round count 7 to the end of the second clock cycle of round count 13 and during the second clock cycle of round count 14.

Referring now to the AND invert circuit 548 in FIG. 22g3, during the time that the positive signal is maintained on the CT 0, 7, 14, 15 line, that positive signal in combination with the positive signal on the DEC line are applied to render the AND invert circuit 548 effective for applying a negative signal via the —SRR line to one input of the OR invert circuit 550 and to decondition the AND circuit 572 in FIG. 22g4. The AND circuit 572 in being deconditioned causes a negative signal to be applied via the —SR line to one input of the OR invert circuit 574. Thus, negative signals are maintained on the —SRR and —SR line during times corresponding to the positive signal maintained on the CT 0, 7, 14, 15 line. During each succeeding —C time, while such negative signals are maintained on the —SRR and —SR lines, —C clock pulses are applied to the other input of the OR invert circuit 550 and 574 causing positive signals to be applied via the SRR and SR lines, respectively, to the control signal cable connected to the crypto engines. The positive signals on the SR lines are also applied to the OR invert circuit 606 causing negative signal delayed by delay circuit 608 to be applied via the LDK line to the control signal cable. Therefore, a total of 27 positive signals are produced on the SRR, SR and LDK lines during 15 rounds of the cipher function. Referring now to the crypto engines in FIG. 22g1, each combination of positive signals on the SR, SRR and LDK lines are effective for shifting the key register right one position. Thus, with this key shifting schedule arrangement the key registers are shifted twice each round except during round counts 0, 7 and 14 when the key registers are shifted once and during round count 15 where the key registers are not shifted at all as shown in the timing diagram of FIG. 26.

Referring now to the ER flip flop 384 in FIG. 22c2, since the ER flip flop 384 is switched every clock cycle, a negative signal is applied to the —ER FF line during every second clock cycle of each round except the last round. This is so because of the fact that the EB latch 632 in FIG. 22f4 is reset at the end of the first clock cycle of the round count 15 (16th round) to terminate the positive signal EB line and thereby inhibit ER flip flop 384 in FIG. 22c2 from being set during the second clock cycle of the round count 15. The successive negative signals on the —ER FF line are applied to one input of the OR invert circuit 542. Accordingly, during every second clock cycle of a round, a —C clock pulse is applied to the other input of the OR invert circuit 542 causing positive signals to be applied on the ER line to the control signal cable connected to the crypto engines. The positive signals on the ER line are also applied to render the OR invert circuit 652 in FIG. 22h4 effective to apply negative signals, delayed by a 250ns delay circuit 654, via the LDR line to the control signal cable. Referring now to the crypto engine in FIG. 22g1, the positive signals on the ER and LDR line are applied to the upper and lower data registers UDR 200 and LDR 250 at the end of each round and are effective to cause the intermediate result of the cipher function to be transferred from the output of the modulo-2 adders

650-664 to the upper data register UDR 200 while the output of the upper data register UDR 200 are transferred to the lower data register LDR 250 in preparation for the next round of the cipher function.

Referring now to the AND invert circuit 624 in FIG. 22/4, at 04 time of the first clock cycle of the round count 15, a 04 clock pulse in combination with positive signals on the C1 and 14, 15 line render the AND invert circuit effective to apply a negative signal to reset START EB and EB latches 628 and 632, respectively. The EB latch 632 in being reset applies a negative signal on the EB line to decondition the ER flip flop 384 in FIG. 22c2 and a positive signal on the -EB line which together with a positive signal from the START EB END latch 612 condition the AND invert circuit 614. At 01 time of the second clock cycle of round count 15, a 01 DEL clock pulse is applied to render the AND invert circuit 614 effective to apply a negative signal to set the EB END latch 616 producing a positive signal on the EB END line and a negative signal on the -EB END line. The positive signal on the EB END line is applied to condition the AND invert circuit 610 in FIG. 22c4 and together with the positive signal on the DECK line to condition the AND invert circuit 618 and to render the AND circuit 636 in FIG. 22g4 effective to apply a positive signal to the OR invert circuit 640 causing negative signals to be applied via the -ELR and -LDR line to one input of the OR invert circuits 642 and 644, respectively. The negative signal on the -EB END line is applied to decondition the AND circuit 382 in FIG. 22c2, causing a negative signal to be applied to reset the round counter 390 in FIG. 22d2 back to a count of 0.

Referring now to FIG. 22g4, at 02 time of the second clock cycle of round 16, a -C clock pulse is applied to the other input of the OR invert circuit 642 and 644 causing positive signals to be applied via ELR and LDR lines to the control signal cable connected to the crypto engines. The positive signals on the ELR and LDR lines are also applied to the OR invert circuits 648 and 652, respectively, causing negative signals, delayed by delay circuits 650 and 654, to be applied via the LIB and LDR lines to the control signal cable. Referring now to the crypto engine in FIG. 22g1, the signals on the ELR and LIB lines and on the LDR and LDR lines cause a swapping action between the data registers and the buffer registers as previously described. However, the significance at this time is to transfer the contents of the upper data register UDR 200 to the upper buffer register UBR 100 and to transfer the outputs of the modulo-2 adders 650-664 to the lower buffer register LBR 150 so that the result of the cipher function, namely, the operational key in clear form is now stored in the buffer registers.

Referring now to FIG. 22e4, at 04 time of the second clock cycle of the 16th round, a 04 clock pulse is applied to render the AND invert circuit 610 effective to apply a negative signal to reset the START EB END latch 612 in FIG. 22/4. At the same time, the 04 clock pulse is also applied to render the AND invert circuit 618 in FIG. 22e4 effective to apply a negative signal to the OR invert circuit 620 in FIG. 22/4 where it is inverted to a positive signal on EB END L line. The positive signal on the EB END L line is applied to the AND invert circuit 619 the other inputs of which have positive signals maintained thereon so as to render the AND invert circuit 619 effective to maintain a negative signal input to the OR invert 620 thereby latching the positive signal

on the EB END L line until a negative signal is subsequently applied to the -OUT CYCLE START line. The positive signal on the EB END L line is also applied to condition the AND invert circuit 458 in FIG. 22e3. At 01 time of the next clock cycle, a 01 clock pulse is applied to render the AND invert circuit 458 effective to apply a negative signal to set the OUTPUT CYCLE latch 464 producing a positive signal on OUT CYCLE line and a negative signal on the -OUT CYCLE line thereby initiating an output cycle with the negative signal on the -OUT CYCLE line being applied to set the START OUT CYCLE END latch 580. Referring now to FIG. 22g4, the positive signal on the OUT CYCLE line together with a positive signal on the K ORD line render the AND invert circuit 598 effective to apply a negative signal to decondition the AND circuit 600, to decondition the AND circuit 572 and via the -LKB line to one input of the OR invert circuit 604. The deconditioned AND circuit 600 applies a negative signal via the -LIB line to one input of the OR invert circuit 602 while the deconditioned AND circuit 572 applies a negative signal via the -SR line to one input of the OR invert circuit 574. Referring now to FIG. 22/4, at 01/L time, a -01/L clock pulse is applied to reset the EB END latch 616. Referring now to FIG. 22g4, at 02 time, a -C clock pulse is applied to the other input of the OR invert circuits 602, 604 and 574 causing them to be deconditioned and apply positive signals via the LIB, LKB and SR lines, respectively, to the control signal cable connected to the crypto engines. The positive signals on the SR line is also applied to the OR invert circuit 606 in FIG. 22h4 causing a negative signal, delayed by delay circuit 608, to be applied via the LDK line to the control signal cable.

Referring now to the crypto engines in FIG. 22g1, these signals are effective to cause the buffer and key registers to shift in synchronism with a data byte being transferred from the buffer registers UBR 100 and LBR 150 to the key registers UKR 350 and LKR 400. Referring now to FIG. 22d4, at 04 time, a 04 clock pulse in combination with positive signals on the OUT CYCLE and K ORD lines are applied to render the AND invert circuit 442 effective to apply a negative pulse to the STEP BYTE CTR line, at the trailing edge of which a positive signal is effective to step the byte counter to a count of 1. In a similar manner to that described above, the buffer registers and the key registers of the crypto engine are shifted in synchronism, once for each clock cycle, causing successive bytes of the operational key in clear form to be transferred from the buffer registers to the key registers.

The byte counter 448 counts the clock cycles and when the count steps from a count of 7 back to a count of 0, a negative signal is applied to set the COUNT 8 latch 450 which, in being set, applies a negative signal via the -CT8 line to reset the OUTPUT CYCLE latch 464 in FIG. 22e3. The OUTPUT CYCLE latch 464, in being reset, applies a positive signal on the -OUT CYCLE line and a negative signal on the OUT CYCLE line. Referring now to FIG. 22d3, the combination of positive signals on the -OUT CYCLE line and the -IN CYCLE line render the AND invert circuit 410 effective to apply a negative signal to reset the COUNT 8 latch 450 in FIG. 22d4, and is inverted by the inverter 412 to a positive signal to reset the BLOCK COUNT flip flop 414 producing a negative signal on the -BLK0 line and a positive signal on the -BLK1 line. At the same time, the negative signal on the OUT CYCLE line

is applied to decondition the AND invert circuit 598 in FIG. 22g4 causing a positive signal to be applied via -LKB line to the OR invert circuit 604 and to render the AND circuits 600 and 572 effective to apply positive signals via the -LIB and -SR line to the OR invert circuits 602 and 574. As a result, negative signals are now maintained on the LIB, LKB and SR line to terminate further shifting of the buffer and key registers in the crypto engines.

Referring now to FIG. 22/3, at 01 time of the next clock cycle, a 01 DEL clock pulse in combination with the positive signal on the -OUT CYCLE line and the positive signal output of the START OUT CYCLE END latch 580 are applied to render the AND invert circuit 582 effective to produce a negative signal to set the OUT CYCLE END latch 584. The OUT CYCLE END latch 584, in being set, applies a positive signal on the OUT CYCLE END line to condition the AND invert circuit 578 in FIG. 22e3 and a negative signal on the -OUT CYCLE END line to reset the DECK latch 296 in FIG. 22c3. The DECK latch 296 in being reset applies a positive signal to render the AND invert circuit 298 in FIG. 22c4 effective to apply a negative signal on the K ORD line and via the inverter 300 a positive signal on the -K ORD line indicating the end of the key order operation. Referring now to FIGS. 22e3 and 22/3, at 04 time, a 04 clock pulse is applied to render the AND invert circuit 578 effective to apply a negative signal to reset the START OUT CYCLE END latch 580. At 01 time of the next clock cycle, a -01/L clock pulse is applied to reset the OUT CYCLE END latch 584 and thereby end the decipher key order operation with the operational key presently stored in the key registers in preparation for a subsequent data processing operation.

ENCIPHER ORDER OPERATION

The function of this operation is to encipher a message, which may consist of one or more 8 byte blocks of plaintext, into a corresponding message of ciphertext. After a valid operational key is installed in the crypto engines there is no need to issue any further key handling orders for successive blocks of plaintext so long as that same operational key is used. A valid operational key is loaded in the key registers of the crypto engine by performing a DECK operation, as previously described.

When the order code specifying the encipher order is decoded, a ENC latch is set to signal the encipher mode of operation. Following the ENC order command, a first series of 8 PIOW data commands is issued, with the data fields associated with the commands, being loaded into the buffer registers of the crypto engines as the first message block of plaintext to be enciphered. The first such command initiates an input cycle and a byte counter counts each such command received. After the 8 PIOW commands have been received and the 8th byte of the message block written into the buffer registers, then at the 8th count, the input cycle ends, a block counter is set and the crypto engines start an encipher function which is indicated by the generation of an engine busy signal. At the end of the encipher operation, half of the ciphertext block of data is present in the upper data register and the other half is present at the outputs of the cipher function circuits. Following the encipher operation, a series of 8 PIOR data commands are issued for reading the enciphered message block of ciphertext. The first such command initiates an output

cycle and the byte counter counts each such command received. During the execution of the first PIOR data command, while the block count is at a count of 1, the message block of ciphertext is parallel transferred from the upper data register and the outputs of the cipher function circuits to the buffer registers where it is now available for reading, a byte at a time. At the end of the execution of each PIOR command, the buffer registers are shifted one position to present the next byte of the message block of ciphertext for reading. At the 8th count of the byte counter, the output cycle ends, the block counter is reset and the ENC latch remains set to end the encipher order operation. The ENC latch in remaining set permits one or more succeeding message blocks of plaintext to be enciphered in a similar manner as that described above.

A more detailed description of the encipher order operation will now be given in conjunction with the timing diagrams of FIGS. 27a-27d. After address selection at TA time and loading the command byte into the command register at TC time, the command code is decoded by AND invert circuit 266 in FIG. 22b2 to produce a negative signal which is inverted by inverter 268 to a positive signal on the WR DSD ORDER line thereby indicating the presence of a WR DSD ORDER command. At the same time, a data processing order code is decoded by the AND invert circuit 302 to apply a negative signal via the -DP DEC line to the inverter 304 where it is inverted to a positive signal and applied to one input of the AND invert circuit 306. At TD time, a positive signal is applied via the SYNCH TD line to render the AND circuit 270, conditioned by the positive signal on the WR DSD ORDER line, effective to produce a positive signal on the WR ORD TIME line which is applied to the remaining input of the AND invert circuit 306 to render it effective to produce a negative signal which is applied via the -RST ENC line to reset the ENC latch 312 in FIG. 22c4 and to the inverter 308 where it is inverted to a positive signal and applied to one input of the AND invert circuit 310. A positive signal on the -Y line from the command register 224 personalizes the present order as an ENC order and is applied to the other input of the AND invert circuit 310 to render it effective to apply a negative signal via the -SET ENC line to set the ENC latch 312. The ENC latch 312 in being set applies a positive signal via the ENC line to FIG. 22g3 where it is effective via OR gate 522 to condition the AND circuit 536 and is inverted to a negative signal by the inverter 546 to apply a negative signal on the DEC line to decondition the AND invert circuits 548 and 560.

The series of 8 PIOW data commands is now received and processed in a similar manner to that described in the DECK order operation i.e. an input cycle is initiated, the byte counter 448 is conditioned to count each PIOW data command received and the message block of plaintext is loaded, a byte at a time, per PIOW data command, into the buffer registers UBR 100 and LBR 150. After the 8th byte has been written into the buffer registers, then, at the 8th count, the input cycle ends, the block count flip flop 414, in FIG. 22d3, is set and the IN CYCLE END latch 534 in FIG. 22/3 is set. The IN CYCLE END latch 534 in being set initiates the swapping action between the buffer registers and the data registers of the crypto engines which, in this case, causes the message block of plaintext to be transferred from the buffer registers UBR 100 and LBR 150 to the data registers UDR 200 and LDR 250 preparatory to

performing the encipher operation. At the same time, referring to the AND circuit 538 in FIG. 22g3, positive signals on the IN CYCLE END and ENC lines render the AND circuit 538 effective to apply a positive signal to the OR invert circuit 540 causing a negative signal to be applied via the -SL line to one input of the OR invert circuit 544. At -C time, a -C clock pulse is applied to the other input of the OR invert circuit 544 causing it to apply a positive signal via the SL line to the control signal cable and to one input of the OR invert circuit 606 in FIG. 22h4. The OR invert circuit 606 is rendered effective to apply a negative signal, delayed by the delay circuit 608, via the LDK line to the control signal cable connected to the crypto engines. Referring now to the crypto engines in FIG. 22g1, the signals on the SL and LDK line are applied to the key registers causing the contents thereof to be shifted one position to the left as a pre-shift operation prior to the encipher operation.

The encipher operation is similar to the decipher operation previously described in connection with DECK order operation except that in this case the key register is shifted to the left under control of SL control signals rather than the SRR and SR control signals as can be better seen by referring to the timing diagram of FIG. 27. Referring to FIG. 22g3, this is so because the signals on the CT 0, 7, 14, 15 line are used with the AND circuit 536 conditioned by the positive signal on the ENC line and inhibited from being used with the AND circuit 548 deconditioned by the negative signal on the DEC line. As a result of the single pre-shift signal on the SL line and the 27 additional signals on the SL line during the encipher operation, the key registers shift left exactly 28 times to return the operational key back to the initial condition in the key registers in preparation for enciphering the next block of a multi-block plaintext message. At the end of the cipher function, half of the ciphertext block of data is available at the output of the upper data register UDR 200 and the other half is available at the outputs of the cipher function circuits.

Referring now to FIG. 22b2, the first of a series of 8 PIOR data commands is now received and after address selection at TA time and command loading into the command register at TC time, the AND invert circuit 262 decodes this command and applies a negative signal to one input of the OR invert circuit 260 and to the inverter 264 where it is inverted to a positive signal on the PIOR EARLY line. Referring now to FIG. 22d3, the positive signal on the PIOR EARLY line is applied to the inverter 422 where it is inverted to a negative signal and applied to one input of the OR invert circuit 424. At this time, positive signals are maintained at the input of the AND invert circuit 416 causing a negative signal to be applied to the other input of the OR invert circuit 424 which therefore produces a positive signal on the PIOR line. The positive signal on the PIOR line is applied to the OR invert circuit 456 in FIG. 22e3 where it is inverted to a negative signal to set the OUT-PUT CYCLE latch 464 producing a positive signal on the OUT CYCLE line and a negative signal on the -OUT CYCLE line to initiate an output cycle. The positive signal on the PIOR line is also applied to the inverter 462 where it is inverted to a negative signal and applied via the -PIOR line to set the START PIOR END latch 588 in FIG. 22/3. Referring now to FIGS. 22e3 and 22/3, the negative signal on the -OUT CYCLE line is applied to set the START OUT

CYCLE END latch 580 while the positive signal on the OUT CYCLE line in combination with the positive signal output of the START OUT CYCLE START latch 554 in FIG. 22/3 are applied to condition the AND invert circuit 556. At 01 time of the next clock cycle, a 01 DEL clock pulse is applied to render the AND invert circuit 556 effective to apply a negative signal to set the OUT CYCLE START latch 558 which, in being set, applies a positive signal to the OUT CYCLE START line and a negative signal to the -OUT CYCLE START line. The positive signal on the OUT CYCLE START line is applied to condition the AND invert circuit 552 in FIG. 22e3 and is also applied to the AND circuit 634 in FIG. 22g4. Since this is not a key order operation and the block count is at a count of one, positive signals are maintained on the other inputs to the AND circuit 634 which, therefore, is rendered effective to apply a positive signal to the OR invert circuit 640 which, in turn, initiates production of the ELR and LIB control signals, in a manner previously described, to the crypto engines where they are effective to cause the enciphered block of data to be transferred from the outputs of the upper data register UDR 200 and the outputs of the modulo-2 adder 650-664 to the upper buffer register 100 and the lower buffer register 150, respectively, in preparation for reading the now enciphered block of ciphertext. Referring now to FIGS. 22e3 and 22/3, at 04 time, a 04 clock pulse is applied to render the AND invert circuit 552 effective to apply a negative signal to reset the START OUT CYCLE START latch 554. At 01/L time, a -01/L clock pulse is applied to reset the OUT CYCLE START latch 558.

Referring now to FIG. 22b2, at TC END time, a positive signal on the TC END line is applied to the inverter 258 where it is inverted to a negative signal to decondition the OR invert circuit 260 causing a positive signal to be applied to the PIOR DATA line. Referring now to the AND circuit 902 in FIG. 22h3, assuming there has been no procedural error, the positive signal on the PIOR DATA line is applied to render the AND circuit 902 effective to apply a positive signal to condition an array of exclusive OR circuits 906 in FIG. 22i1. The function of this array is to compare corresponding data bytes from the two crypto engines for equality. Exclusive OR circuit 906A is representative of this array and will be described in detail. Byte outputs from the crypto engine are applied to the AND invert circuits 908, 910 and 912 with a positive signal on the bit line representing a bit 1 and a negative signal on the bit line representing a bit 0. If the output bits are both equal to 1, then positive signals are applied to render the AND invert circuit 908 effective to apply a negative signal to decondition both the AND invert circuits 910 and 912 causing a positive signal to be produced from the joint outputs thereof. Similarly, if the output bits are both equal to 0, then negative signals are applied to decondition the AND invert circuits 910 and 912 causing a positive signal to also be produced from the joint outputs thereof. On the other hand, if the output bits from the crypto engines are not equal, then the AND invert circuit 908 is deconditioned to apply a positive signal to condition the AND invert circuits 910 and 912, one of which will have a positive signal applied thereto from one of the crypto engines to render that AND invert circuit effective to apply a negative signal from the joint outputs thereof. Accordingly, it should be apparent that if the outputs of one crypto engine equal

the outputs of the other crypto engine, then positive signals will be applied from the array of exclusive OR circuit 906 to render the AND invert circuit 916 effective to produce a negative signal to decondition the engine error detect AND invert circuit 918. On the other hand, if any bit of the cipher engines does not compare, then, a negative signal output from the exclusive OR circuit corresponding to the error bit will be applied to decondition the AND invert circuit 916 causing a positive signal to be applied to condition the engine error detect AND invert circuit 918.

During TC END time, while a positive signal is maintained on the PIOR DATA line, and assuming there is no engine error, the byte output of the crypto engines is taken from the output of the AND invert circuits, such as AND invert circuit 908, of the array of exclusive OR circuits 906 and applied to the -DATA BUS IN. At the same time, parity generator circuit 914, which is responsive to the data byte output of the array of exclusive OR circuits 906, generates a parity bit for the data byte which is applied to the -P line of the -DATA BUS IN.

At TD time, a positive signal is applied via the TD SEL line to render the AND invert circuit 918 effective or not depending on whether an engine error has been detected. If an engine error is detected, the AND invert circuit 918 is rendered effective to apply a negative signal via the ENGINE ERR line to set the bit 1 latch 954B of the status register 952 to indicate the fact that an engine error was detected.

At the end of this IO operation, the command register 224 in FIG. 22a2 is reset to decondition the command decoder AND invert circuit 262 thereby causing a positive signal to be applied to the OR invert circuit 260 and the inverter 264 which, in turn, cause negative signals to now be applied to the PIOR DATA and PIOR EARLY lines, respectively. The negative signal on the PIOR EARLY line is applied to the inverter 422 in FIG. 22d3 where it is inverted to a positive signal to render the OR invert circuit 424 effective to apply a negative signal on the PIOR line. The negative signal on the PIOR line is applied to the inverter 446, in FIG. 22d4, where it is inverted to a positive signal on the STEP BYTE CTR line to step the Byte Counter 448 to a count of 1. The negative signal on the PIOR line is also applied to the inverter 462 in FIG. 22e3 where it is inverted to a positive signal and applied together with a positive signal from the START PIOR END latch 588 in FIG. 22f3 to condition the AND invert circuit 590. At 01 time of the next clock cycle, a 01 DEL clock pulse is applied to render the AND invert circuit 590 effective to produce a negative signal to set the PIOR END latch 592 causing a positive signal to be produced on the PIOR END line to condition the AND invert circuit 586 in FIG. 22e4 and a negative signal on the -PIOR END line which is applied to decondition the AND circuit 600 in FIG. 22g4. The AND circuit 600 is being deconditioned initiates the production of a LIB and LIB control signals, in a manner as previously described, via the control signal cable to the crypto engines to shift the buffer registers one position in preparation for outputting the next byte of ciphertext of the enciphered message block of data. Referring now to the AND invert circuit 586 in FIG. 22e4, at 04 time, a 04 clock pulse is applied to render the AND invert circuit 586 effective to reset the START PIOR END latch 588. At 01/L time of the next clock cycle, a -01/L clock pulse is applied to reset the PIOR END latch 592.

In a similar manner, during each of the succeeding ones of the series of 8 PIOR data commands, the next data byte of cipher text is passed with an appended parity bit to the -DATA BUS IN, the data byte is checked for an engine error, the byte counter is stepped to the next count and the buffer registers of the crypto engines are shifted one position to provide the next succeeding data byte of ciphertext for processing.

After the 8th byte is read to the -DATA BUS IN, the byte counter 448 in FIG. 22d4 steps from a count of 7 back to a count of 0 causing a negative signal to be produced to set the COUNT 8 latch 450 which, in turn, applies a negative signal to the -CT 8 line. The negative signal on the -CT 8 line is applied to reset the OUTPUT CYCLE latch 464 in FIG. 22e3 thereby ending the output cycle. The OUTPUT CYCLE latch 464 in being reset applied a positive signal on the -OUT CYCLE line and a negative signal on the OUT CYCLE line.

Referring now to FIG. 22d3, the combination of the positive signals on the -OUT CYCLE line and the -IN CYCLE line render the AND invert circuit 410 effective to apply a negative signal to reset the COUNT 8 latch 450 in FIG. 22d4 and is inverted by inverter 412 to a positive signal to reset the BLOCK COUNT flip flop 414. The negative signal on the OUT CYCLE line is applied to set the START OUT CYCLE START latch 554 in FIG. 22f3. At the end of this IO operation, the command register is reset to effectively cause a positive signal to be applied on the -PIOR line, as in a manner previously described, which in combination with the positive signal output of the START PIOR END latch 588 are applied to condition the AND invert circuit 590 in FIG. 22f3. Accordingly, at 01 time of the next clock cycle, a 01 DEL clock pulse is applied to render the AND invert circuit 590 effective to apply a negative signal to set the PIOR END latch 592 which, in being set, applies a positive signal to the PIOR END line and a negative signal to the -PIOR END line. The negative signal on the -PIOR END line is applied to decondition the AND circuit 600 in FIG. 22g4 which initiates production of the LIB and LIB control signals, in a manner previously described, via the control cable to the crypto engines. Referring now to the crypto engine in FIG. 22g1, the LIB and LIB control signals are applied to shift the buffer register one more position to effectively clear the content thereof in preparation for receiving the next block of plaintext of a multi-block message for encipherment. Referring now to FIG. 22e4, at 04 time, a 04 clock pulse in combination with the positive signal on the PIOR END line are applied to render the AND invert circuit 586 effective to apply a negative signal to reset the START PIOR END latch 588 in FIG. 22f4. At 01/L time of the next clock cycle, a -01/L clock pulse is applied to reset the PIOR END latch 592 to terminate the encipher order operation.

DECIPHER ORDER OPERATION

The function of this operation is to decipher a message, which may consist of one or more 8 byte blocks of ciphertext, into a corresponding message of plaintext. After a valid operational key is installed in the crypto engine by a DECK order operation there is no need to issue any further key handling orders for successive blocks of ciphertext so long as the same operational key is used.

When the order code specifying a decipher order is decoded, the ENC latch is reset to signal the decipher

mode of operation. Following the DEC order command, a series of 8 PIOW data commands is issued, with the data fields associated with the commands, constituting the message block of ciphertext, being loaded into the buffer registers of the crypto engines. The first such command initiates an input cycle and a byte counter counts each such command received. After the 8 PIOW commands have been received and the 8th byte written into the buffer registers, then, at the 8th count, the input cycle ends, the block of ciphertext is transferred from the buffer registers to the data registers of the crypto engines, a block counter is set and the crypto engines start a decipher function which is indicated by the generation of an engine busy signal. At the end of the decipher operation, half of the cleartext block of data is present in the upper data register and the other half is present at the outputs of the cipher function circuits. Following the decipher operation, a series of 8 PIOR data commands are issued for reading the deciphered message block of cleartext. The first such command initiates an output cycle and the byte counter counts each such command received. During the execution of the first PIOR data command, while the block count is at a count of 1, the message block of cleartext is parallel transferred from the upper data register and the outputs of the cipher function circuits to the buffer registers where it is now available for reading, a byte at a time. At the end of the execution of each PIOR data command, the buffer registers are shifted one position to present the next byte of the message block of cleartext for reading. At the 8th count of the byte counter, the output cycle ends, the block counter is reset and the ENC latch remains reset to end the decipher operation. The ENC latch in remaining reset permits one or more succeeding message blocks of ciphertext to be deciphered in a similar manner as that described above.

The decipher operation is similar to the encipher operation in that an order code is decoded, a series of 8 PIOW data commands are issued to proceed into an input cycle for loading a data parameter into the crypto engines, a cipher function is performed on the data parameter under control of an operational key and a series of 8 PIOR data commands are issued to proceed into an output cycle for reading the results of the cipher function. The similarity between these two operations can be seen from the timing diagrams of FIGS. 27a-27d. The basic difference between these two operations is in the specification of the decipher order rather than an encipher order, which sets the device for the decipher mode of operation, and the key shifting schedule provided for the key registers during the decipher function performed by the crypto engines. It will be remembered that for an encipher operation the key registers are shifted to the left by one pre-shift SL control signal followed by 27 additional SL control signals during the 16 rounds of the encipher operation for a total of 28 SL control signals to restore the cipher key back to its initial home position in preparation for enciphering the next block of cleartext. In the decipher operation, the key registers, instead of being shifted to the left, as in the encipher operation, are shifted to the right by 27 SRR and SR control signals during the 16 rounds of the decipher function, as described in detailed in the DECK order operation, followed by one post-shift SRR and SR control signals at the beginning of the output cycle for a total of 28 SRR and SR control signals to restore the cipher key back to its initial home position in preparation for deciphering the next block of ciphertext. It

should be apparent that with this symmetry, the decipher rounds are performed in the reverse order of the encipher rounds i.e. the set of cipher key bytes used in the last round of an encipher operation is the set of cipher key bytes used in the first round of the decipher operation so that each round of the decipher operation undoes each round of the encipher operation, in reverse order.

Since the basic cipher operation has been described in detail in the previous section and the generation of the 27 control signals SRR and SR for a decipher function has been described in connection with the detailed description of DECK order operation, the following detailed description will be restricted to a description of how the device is set for the decipher mode of operation and how the 28th postshift SRR and SR control pulses are provided at the beginning of the output cycle of the decipher order operation.

After address selection at TA time and loading the command byte into the command register at TC time, the command code is decoded by the AND invert circuit 266 in FIG. 22b2 to produce a negative signal which is inverted by inverter 268 to a positive signal on the WR DSD ORDER line thereby indicating the presence of a WR DSD order command. At the same time, the order code for data processing operation is decoded by the AND invert circuit 302 in FIG. 22b3 to produce a negative signal on the -DP DEC line where it is inverted to a positive signal by inverter 304 and applied to one input of the AND invert circuit 306. At TD time, a positive signal is applied via the SYNCH TD line to render the AND circuit 270, conditioned by the positive signal on the WR DSD ORDER line, effective to produce a positive signal on the WR ORD TIME line which is applied to the remaining input of the AND invert circuit 306 to render it effective to produce a negative signal which is applied via the -RST ENC line to reset the ENC latch 312 in FIG. 22c4 and to the inverter 308 where it is inverted to a positive signal and applied to one input of the AND invert circuit 310. A negative signal on the -Y line from the command register 224 personalizes this data processor order as a DEC order and is applied to decondition the AND invert circuit 310, which in being deconditioned, maintains a positive signal on the -SET ENC line so that the ENC latch 312 remains in a reset condition. SPEC ENC latch 494 is also held reset by the inverted WR ORD TIME signal. The ENC latch 312, and SPEC ENC latch 494, being in a reset condition, apply a negative signal via OR circuit 522 to the inverter 546 in FIG. 22g3 where it is inverted to a positive signal on the DEC line to condition the AND invert circuits 548 and 560 each of which is effective for controlling the generation of the SRR and SR control signals used during the decipher operation.

After the decipher function has been completed and the key registers have been shifted 27 times under control of the 27 SRR and SR control signals, the first of a series of 8 PIOR data commands is issued to initiate an output cycle causing the OUTPUT CYCLE latch 464 in FIG. 22e3 to be set which, in being set, applies a positive signal to the OUT CYCLE line. The positive signal on the OUT CYCLE line in combination with a positive signal from the START OUT CYCLE START latch 554 in FIG. 22/3 are applied to condition the AND invert circuit 556. At the next 01 time, a 01 DEL clock pulse is applied to render the AND invert circuit 556 effective to apply a negative signal to set

OUT CYCLE START latch 558. The OUT CYCLE START latch 558, in being set, applies a positive signal to the AND invert circuit 560 in FIG. 22g3 which, at this time, has positive signals maintained on the other inputs thereto thereby rendering the AND invert circuit 560 effective to apply a negative signal on the —SRR and via the AND circuit 572 in FIG. 22g4 a negative signal on the —SR line to initiate the generation of the post-shift SRR and SR control signals which are used to shift the key register the 28th time to restore the cipher key back to its initial home position in preparation for deciphering the next block of ciphertext. The remainder of the DEC order operation, namely, to read the 8 bytes of the block of cleartext is performed in a similar manner as that described in detail for the encipher order operation.

GENERATE RANDOM NUMBER ORDER OPERATION

The function of this operation is to generate a random number by enciphering a pseudo random number under a variant of the host master key which, in the applications previously described, is used as a secondary key (or multiple secondary keys if multiple operations are performed) or is used as an enciphered operational key.

During command time of this operation, when the order code specifying a generate random number (GRN) order is decoded, a load master key (LMK) latch and a key variant 3 latch are set. With the LMK latch set, the contents of the MK memory is caused to be read out and with the key variant 3 latch set, each byte of the master key read out is modified to provide a variant thereof for transfer to the crypto engines. The variant of the master key is parity checked, a byte at a time, and loaded as a working key into the key registers of the crypto engines. During synch TD time of this operation, a GRN latch and a special encipher latch are set, the latter causing the processing mode to be set for an encipher operation. After half of the variant of the master key is loaded into the key registers of the crypto engine and while the remaining half is being loaded, an input cycle is initiated during which the contents of a non-resettable 64 bit random counter is transferred, a byte at a time each clock cycle, to the buffer registers of the crypto engine. During this transfer, a byte counter counts the clock cycles and after the 8th byte of the random number has been loaded into the buffer registers, then, at the 8th count, the input cycle ends, the LMK latch is reset to terminate further MK memory read out, the random number is transferred from the buffer registers to the data registers of the crypto engine and a block counter is set. During this transfer, the last byte of the variant of the master key is loaded into the key registers, the crypto engines initiate an encipher operation, indicated by an engine busy signal, the key variant latch is reset and the random number counter is stepped to the next count value. During the encipher operation, the random number count value in the data registers of the crypto engines is enciphered under control of the variant of the master key in the key registers of the crypto engines. At the end of the encipher operation, half of the enciphered random number is present in the upper data register and the other half is present at the outputs of the cipher function circuits. Following the encipher operation, a series of 8 PIOR data compounds is received for reading the enciphered random number. The first such command initiates an output cycle and a byte counter counts each such command

received. During the execution of the first PIOR data command, while the block count is at a count of 1, the enciphered random number is parallel transferred from the upper data register and the outputs of the cipher function circuits to the buffer registers where it is then available for reading, a byte at a time, and the GRN latch is reset. At the end of the execution of each PIOR command, the buffer registers are shifted one position to present the next byte of the enciphered random number of reading. At the 8th count of the byte counter, the output cycle ends and the block counter is reset to end the operation.

A more detailed description of the generate random number order operation will now be given in conjunction with the timing diagrams of FIGS. 28a-28c. After address selection at TA time and loading the command byte into the command register at TC time, the command code is decoded by AND invert circuit 266 in FIG. 22b2 to produce a negative signal which is inverted by inverter 268 to a positive signal on the WR DSD ORDER line thereby indicating the presence of a WR DSD order command. At the same time, the order code is decoded by the AND invert circuit 314 to apply a negative signal via the —GRN DEC line to the inverter 316 where it is inverted to a positive signal and applied to one input of the AND invert circuit 318. Referring now to the inverter 476 in FIG. 22d5, the negative signal on the —GRN DEC line is inverted to a positive signal and passed via the OR circuit 484 to the SET LMK line. Referring now to the OR invert circuit 564 in FIG. 22g4, the positive signal on the SET LMK line is applied to render the OR invert circuit 564 effective to apply a negative signal to set the LMK latch 566 producing a positive signal on the LMK line and a negative signal on the —LMK line. Referring now to the AND invert circuit 368 in FIG. 22c2, the negative signal on the —LMK line is applied to decondition the AND invert circuit 368 which, in turn, maintains a positive signal at one input of the AND invert circuits 370 and 374 so long as the LMK latch 566 remains set i.e. while the MK memory is being read out.

Referring now to the KEY VAR 3 CTRL latch 515 in FIG. 22e5, the negative signal on the —GRN DEC line is applied to set the KEY VAR 3 CTRL latch 515 which, in being set, applies a positive signal to the VARIANT 3 line and via the OR circuit 518 to the VARIANT 1 line. Referring now to FIG. 22e1, the positive signals on the VARIANT 1 and VARIANT 3 lines are applied to the exclusive OR circuits 704A and 704D which are used to invert bits 0 and 6 of each byte read out of the MK memory 700 thereby providing a variant of the master key for transfer to the crypto engines.

Referring now to FIG. 22c2, negative signals are maintained at the inputs of the AND invert circuit 366 and a negative signal is maintained at the input to the inverter 162 both of which cause a positive signal to be applied to one input of the AND circuit 380 and to condition the AND invert circuit 376. Additionally, the MK OVW latch 276, presently in a reset state, causes a positive signal to be applied via the —MK OVW line to the other input of the AND circuit 380 thereby rendering it effective to apply and maintain a positive signal on the —W ENABLE line. Thereafter, and in a manner which is described in detail for the DECK order operation, the AND invert circuits 370 and 374 are alternately rendered effective by 03L and —01L clock pulses, respectively; the AND invert circuit 370 con-

trolling the AND invert circuit 376 and inverter 378 to produce successive negative signals on the -M ENABLE Line which in combination with the positive signal on the -W ENABLE line allow successive reading of the MK memory 700 while the AND invert circuit 374 controlling the AND invert circuit 376 and inverter 388 in FIG. 22d2 to produce successive positive signals on the STEP CTR line for successively stepping the address counter 390 to address successive locations of the MK memory 700. Successive pairs of half bytes read out of the MK memory 700 in FIG. 22e1 are shifted into the shift registers 702 to provide successive bytes of the master key for the crypto engines, with bits 0 and 6 of each byte being inverted by the exclusive OR circuits 704A and 704D to effectively provide a variant of the master key for transfer to the crypto engines.

Referring now to the AND invert circuit 568 in FIG. 22g4, after each byte of the master key are loaded into the shift register 702 in FIG. 22e1, a 01 DEL clock pulse in combination with positive signals on the C1, -STEP CTR and LMK lines are applied to render the AND invert circuit 568 effective to produce a negative signal to set the LDK latch 570 which, in being set, initiates production of positive signals on the SR, LDK and LDK control lines for the crypto engines, in a manner as previously described in detail in connection with DECK order operation. Referring now to the crypto engine in FIG. 22g1, the positive signal on the LDK line is applied to condition the AND circuit 807 to permit a parity check to be made of each variant byte of the master key for parity errors. The successive positive signals on the SR, LDK and LDK lines are applied as control inputs to the key registers UKR 350 and LKR 400 to shift the key registers and allow successive variant bytes of the master key to be loaded into the key registers.

Referring now to FIG. 22b2, at TD time, while the variant of the master key is being loaded into the key registers, a positive signal is applied via the SYNCH TD line to render the AND circuit 270, conditioned by the positive signal on the WR DSD ORDER line, effective to provide a positive signal on the WR ORD TIME line. Referring now to FIG. 22b2', the positive signal on the WR ORDER TIME line is applied to the inverter 322 where it is inverted to a negative signal on the -WR ORD TIME line to reset the GRN latch 320 in FIG. 22c3' and the SPEC ENC latch 494 in FIG. 22d5. Referring now to FIG. 22b2, the positive signal on the WR ORD TIME line is applied to the remaining input of the AND invert circuit 318 to render it effective to produce a signal on the -SET GRN line which is applied to set the GRN latch 320 in FIG. 22c3' producing a positive signal on the GRN line and a negative signal on the -GRN line. Referring now to FIG. 22e4 the positive signal on the GRN line is applied to one input of each of the AND circuits in units 472A-472H and to condition the AND circuits 475 in FIG. 22f1 while the negative signal on the -GRN line is applied to decondition the AND circuits 473. Accordingly, information on the BUS IN is inhibited from passing via the deconditioned AND circuits 473 while information from the random number (RN) counter 470 in FIG. 22e4 is passed via the conditioned AND circuits 475 and the OR circuit 476 to the crypto engines. Referring now to FIG. 22d5, the positive signal on the GRN line is also applied to the OR invert circuit 490 where it is inverted to a negative signal to set the SPEC ENC latch 494

causing a positive signal to be applied to the SP ENC line and a negative signal to the -SP ENC line. Referring now to FIG. 22e3, the positive signal on the SP ENC line is applied via the OR circuit 522 to condition the AND circuits 536 and 538 in FIG. 22g3 and via the inverter 546 to apply a negative signal to the DEC line to decondition the AND invert circuits 548 and 560. Referring to FIG. 22f3, the negative signal on the -SP ENC line is applied to decondition the AND invert circuit 621 causing a positive signal to be applied to one input of the AND circuit 626.

Referring now to FIG. 23d4, while the variant of the master key is being loaded into the key registers and when the address counter 390 in FIG. 23d2 is stepped to a count of 8 by a -01L clock pulse, a negative signal on the -C8 line is applied to set the 16 STEP latch 404 causing a positive signal to be applied to condition the AND circuit 406 and to set the CT OF 8 latch 441 in FIG. 22d4 causing a positive signal to be applied to the CT 8 line. The positive signal on the CT 8 line in combination with the positive signals on the GRN and LMK lines render the AND invert circuit 443 effective to apply a negative signal on the -GRNW line. The negative signal on the -GRNW line is applied to decondition the AND circuit 600 in FIG. 22g4 which, in being deconditioned, applies a negative signal via the -LIB line to one input of the OR invert circuit 602. At 02 time, a -C clock pulse is applied to the other input of the OR invert circuit 602 thereby deconditioning it and causing a positive signal to be applied via the LIB line to the control signal cable connected to the crypto engines and to the OR invert circuit 648 in FIG. 22h4 causing a negative signal, delayed by delay circuit 650, to be applied via the LIB line to the control signal cable connection to the crypto engines.

Referring to FIGS. 22d4 and 22e4 the RN counter 470 is a 64 stage nonresettable binary counter which is battery powered so that it may retain its contents independent of system power. Each of the 8 output bytes of the RN counter 470 is connected to a corresponding set of AND circuits 472A to 472H conditioned by the positive signal on the GRN line and controlled by the settings of the byte counter 448. At this time, the byte counter 448 is at a count of 0 which condition is decoded by the decoder 466 producing a positive signal on the BC 0 line to render effective the set of AND circuits 472A for passing the first byte of the count value in the RN counter 470 via the OR circuits 474 to the AND circuits 475. The AND circuits 475 being conditioned by the positive signal on the GRN line passes the random number byte via the OR circuit 476 and the P box 50 to the buffer registers UBR 100 and LBR 150. Accordingly, the now received combination of signals on the LIB and LIB line are effective to permit the random number byte to be loaded into the buffer registers in each crypto engine.

Referring now to FIG. 22e3, at 03L time, a 03L clock pulse together with positive signals on the GRNW and GRN lines render the AND invert circuit 435 effective to apply a negative signal to set the INPUT CYCLE latch 454 to start an input cycle operation during which successive bytes of the random number count value of the RN counter are loaded into the buffer registers. The INPUT CYCLE latch 454 in being set applies a negative signal via the -IN CYCLE line to set the START IN CYCLE END latch 530 in FIG. 22f3. Referring now to FIG. 22d4, at 04 time, a 04 clock pulse in combination with positive signals on the GRN, LMK and CT

8 lines are applied to render the AND invert circuit 440 effective to apply a negative pulse to the STEP BYTE CTR line, the positive trailing edge of which is effective to step the byte counter 448 to a count of 1.

In a similar manner, succeeding ones of the random number count value bytes are gated, under control of the byte counter 448, and loaded into the buffer registers UBR 100 and LBR 150, with the previous byte being simultaneously shifted and the byte counter 448 being stepped at 04 time of each clock cycle.

After the 8th random number count value byte is written into the buffer registers, then at 04 time of that clock cycle, the byte counter 448 steps from a count of 7 back to a count of 0 causing a negative signal to be produced to set the COUNT 8 latch 450 which, in being set applies a negative signal to the -CT 8 line. The negative signal on the -CT 8 line is applied to reset the INPUT CYCLE latch 454 in FIG. 22e3 thereby ending the input cycle. Referring now to FIG. 22d3, the INPUT CYCLE latch 454, in being reset, applies a positive signal which, in combination with the positive signal on the -OUT CYCLE line, renders the AND invert circuit 410 effective to apply a negative signal to reset the COUNT 8 latch 450 in FIG. 22d4 and is inverted by inverter 412 to a positive signal to set the BLOCK COUNT flip flop 414 producing a positive signal on the -BLK 0 line and a negative signal on the -BLK 1 line.

Referring now to FIG. 22f3, at 01 time of the next clock cycle, a 01 DEL clock pulse in combination with positive signals on the -IN CYCLE line and from the START IN CYCLE END latch 530 render the AND invert circuit 532 effective to apply a negative signal to set the IN CYCLE END latch 534 which, in being set, applies a positive signal to the IN CYCLE END line. Referring now to FIG. 22f4, the positive signal on the IN CYCLE END line is applied to the inverter 622 where it is inverted to a negative signal and applied to decondition the AND circuit 626 causing a negative signal to be applied to set the START EB latch 628 and to the inverter 638 in FIG. 22g4 where it is inverted to a positive signal and applied to render the OR invert circuit 640 effective to apply negative signals via the -ELR and -LDR lines to one input of the OR invert circuits 642 and 644. Referring now to FIG. 22c2, the negative signal on the -ELR line is applied to decondition the AND circuit 382 which, in turn, resets the address counter 390 in FIG. 22d2 from a count of 15 back to a count of 0 causing a positive signal to be applied to the -C 8 line. The positive signal on the -C 8 line is applied to render the AND circuit 406, conditioned by the positive signal from the 16 STEP latch 404, effective to apply a positive signal to the inverter 408 where it is inverted to a negative signal on the -16 STEP line which is applied to reset the CT OF 8 latch 441 in FIG. 22d4 and to reset the LMK latch 566 in 22g4. LMK latch 566 in being reset applies a negative signal to the LMK line and a positive signal to the -LMK line. The negative signal on the LMK line deconditions the AND invert circuit 568 to inhibit further production of the shifting control signals SR, LDK and LDK for the key registers of the crypto engines. Referring now to FIG. 22c2, the positive signal on the -LMK line is applied to render the AND invert circuit 368 effective to apply a negative signal to decondition the AND invert circuits 370 and 374 to inhibit further reading of the MK memory 700 and stepping of the address counter 390.

Referring now to FIG. 22g3, the positive signal on the IN CYCLE END line in combination with the positive signal on the ENC line are applied to render the AND circuit 538 effective to apply a positive signal to the OR invert circuit 540 which, in turn, applies a negative signal via the -SL line to one input of the OR invert circuit 544. Referring now to FIGS. 22g3 and 22g4, at 02 time, a -C clock pulse is applied to the other input of the OR invert circuits 544, 642 and 644 to decondition them causing positive signals to be applied via the SL, ELR and LDR lines, respectively, to the control signal cable connected to the crypto engines. Referring to FIG. 22h4, the positive signal on the SL line is applied to the OR invert 606 causing a negative signal, delayed by delay circuit 608, to be applied via the LDK line to the control signal cable. The positive signal on the LDR line is applied to the OR invert circuit 652 causing a negative signal, delayed by delay circuit 654, to be applied via the LDR line to the control signal cable. Referring now to the crypto engine in FIG. 22g1, the control signals LDR and LDR are effective for causing the random number stored in the buffer registers UBR 100 and LBR 150 to be transferred and loaded into the data registers UDR 200 and LDR 250 in preparation for the encipher function. The control signals on the SL and LDK lines are applied to the key registers causing the contents thereof, namely, the variant of the master key, to be shifted one position to the left as a pre-shift operation prior to the encipher operation.

Referring now to FIGS. 22e3 and 22f3, at 04 time, a 04 clock pulse in combination with the positive signal on the IN CYCLE END line are applied to render the AND invert circuit 528 effective to apply a negative signal to reset the START IN CYCLE END latch 530. At 01/L time of the next clock cycle, a -01/L clock pulse is applied to reset the IN CYCLE END latch 534 causing a negative signal to be produced on the IN CYCLE END line. Referring now to FIG. 22f4, the negative signal on the IN CYCLE END line is applied to inverter 622 where it is inverted to a positive signal to be applied to render the AND circuit 626 effective to apply a positive signal to render the AND invert circuit 630, conditioned by the positive signal from the START EB latch 628, effective to apply a negative signal to set the EB latch 632 indicating the start of the crypto operation. The EB latch 632, in being set, applies a positive signal to the EB line and a negative signal to the -EB line. Referring to FIG. 22d4, the positive signal on the EB line in combination with the positive signal on the GRN line are applied to render the AND circuit 468 effective to apply a positive signal to step the RN COUNTER 470 to the next count. Referring to FIGS. 22c2 and 22d2, the positive signal on the EB line is also applied to condition the address decoder AND invert circuit 398 and to condition the ER flip flop 384 to permit stepping of the round counter 390. Referring to FIG. 22f4, the negative signal on the -EB line is applied to set the START EB END latch 612 and referring to FIG. 22e5, to reset the KEY VAR 3 CTRL latch 515.

The encipher function operation is similar to that previously described in detail in connection with the encipher order operation and can generally be followed by referring to the timing diagram of FIG. 28. Generally, the encipher function is performed by repeating a product cipher function for 16 rounds. During each round, the contents of the upper data register UDR 200 is enciphered under control of the contents of the key

registers UKR 350 and LKR 400 with the results being added to the contents of the lower data register LDR 250 by the modulo-2 adders 650-664. At the end of each round, the outputs of the modulo-2 adders are parallel transferred to the upper data register UDR 200 while the contents of the upper data register UDR 200 are parallel transferred to the lower data register LDR 250 to form the arguments for the next round and the key registers are shifted by the control signal on the SL line in accordance with key shift schedule shown. As a result of the single pre-shift signal on the SL line and the 27 additional signals on the SL line during the encipher operation, the key registers shift left exactly 28 times to return the variant of the master key back to the initial home position in the key registers. At the end of encipher function, half of the enciphered random number is available at the outputs at the upper data register UDR 200 and the other half is available at the outputs of the cipher function circuits.

Following the encipher operation, a series of 8 PIOR data commands are issued for reading the enciphered random number. The first such command initiates an output cycle which is performed in a similar manner to that described in detail in connection with the encipher order operation. In general terms, during the execution of the PIOR data command, while the block count is at a count of 1, the enciphered random number is parallel transferred from the upper data register and the outputs of the cipher function circuits to the buffer registers where it is then available for reading, a byte at a time. At the beginning of the execution of the first PIOR data command, a positive signal is applied on the OUT CYCLE START line to reset the GRN latch 320 in FIG. 22c3' and at the end of the execution of each PIOR command, the buffer registers are shifted one position to present the next byte of the enciphered random number for reading. At the 8th count of the byte counter, the output cycle ends and the block counter is reset to end the operation, with the enciphered random number now available for use as a secondary key or an enciphered operational key. While a 64 bit RN counter is used in this operation to provide a pseudo random number, it should be apparent that it is well within the skill of the art to use a truly random number generator for generating a random value e.g. a noise generator.

ENCIPHER MASTER KEY ORDER OPERATION

The function of the encipher master key $EMK\phi$ operation is to encipher an operational key under the host master key while the function of the encipher master key $EMK1$ operation is to encipher a secondary key under a variant of the host master key.

When the order codes specifying either of these orders is decoded, a load master key (LMK) latch is set and, in the case of the $EMK1$ order, a key variant 1 latch is additionally set. With the LMK latch set for either order, the contents of the MK memory is caused to be read out and in the case of the $EMK\phi$ order operation, is transferred, a byte at a time, to the crypto engines while in the case of the $EMK1$ order operation each byte of the master key read out of the MK memory is modified to provide a variant of the master key to the crypto engines. The master key or the variant of the master key, depending upon which order is being performed, is parity checked in the crypto engines, a byte at a time, and loaded as a working key into the key registers of the crypto engines. During synch TD time of either operation, an EMK latch and a special enci-

pher SPEC ENC latch are set, the latter causing the processing mode to be set for an encipher operation. After loading the master key or the variant of the master key into the key registers, a series of 8 PIOW commands are received with the data field associated with the commands, constituting the operational key or secondary key, depending upon which order is being performed, to be enciphered, being loaded into the buffer registers of the crypto engines. The first such command initiates an input cycle and a byte counter counts each such command received. After the 8 PIOW commands have been received and the 8th byte written into the buffer registers, then, at the 8th count, the input cycle ends, the operational or secondary key is transferred from the buffer registers to the data registers of the crypto engines, a block counter is set, the crypto engines start an encipher operation, indicated by the generation of an engine busy signal, and the key variant 1 latch is reset. During the encipher operation, the operational or secondary key, depending upon which order operation is being performed, in the data registers of the crypto engines is enciphered under control of the master key or variant of the master key, respectively, in the key registers of the crypto engines. At the end of the encipher operation, half of the enciphered operational or secondary key is present in the upper data register and the other half is present at the outputs of the cipher function circuits. Following the encipher operation, a series of 8 PIOR data commands is received for reading the enciphered operational or secondary key. The first such command initiates an output cycle and the byte counter counts each such command received. During the execution of the first PIOR data command, while the block count is at a count of 1, the enciphered operational or secondary key is parallel transferred from the upper data register and the outputs of the cipher function circuits to the buffer registers where it is then available for reading, a byte at a time, and the EMK latch is reset. At the end of the execution of each PIOR command, the buffer registers are shifted one position to present the next byte of the enciphered operational or secondary key for reading. At the 8th count of the byte counter, the output cycle ends and the block counter is reset to end the operation.

A more detailed description of the encipher master key order operation will now be given in conjunction with the timing diagrams of FIGS. 29a-29c. After address selection at TA time and loading the command byte into the command register at TC time, the command code is decoded by the AND invert circuit 266 in FIG. 22b2 to produce a negative signal which is inverted by inverter 268 to a positive signal on the WR DSD ORDER line thereby indicating the presence of a WR DSD ORDER command. At the same time, if the order code specifies an $EMK\phi$ order, then that order code is decoded by the AND invert circuit 340 to apply a negative signal via the $-EMK\phi$ DEC line to the inverter 342 where it is inverted to a positive signal and applied to one input of the AND invert circuit 344 whereas, if the order code specifies a $EMK1$ order, the order code is decoded by the AND invert circuit 341 to apply a negative signal via the $-EMK1$ DEC line to the inverter 343 where it is inverted to a positive signal and applied to one input of the AND invert circuit 345. Referring now to the inverter circuits 479 and 481 in FIG. 22d5, negative signals on either of the $-EMK\phi$ DEC or $-EMK1$ DEC lines are inverted, respectively, to positive signals and passed via the OR circuit 484 to

the SET LMK line. Referring now to the OR invert circuit 564 in FIG. 22g4, the positive signal on the SET LMK line is applied to render the OR invert circuit 564 effective to apply a negative signal to set the LMK latch 566 producing a positive signal on the LMK line and a negative signal on the —LMK line. Referring now to the AND invert circuit 368 in FIG. 22c2, the negative signal on the —LMK line is applied to decondition the AND invert circuit 368 which, in turn, maintains a positive signal at one input of the AND invert circuits 370 and 374 so long as the LMK latch 566 remains set i.e. while the MK memory is being read out.

Referring now to the KEY VAR 1 CTRL latch 513 in FIG. 22e5, if the order code is a EMK1 order code, then the negative signal on the —EMK1 DEC line is applied via the OR circuits 511 to set the KEY VAR 1 CTRL latch 513 which, in being set applies a positive signal to the VARIANT 1 line and via the OR circuit 518 to the VARIANT 1 line. Referring now to FIG. 22e1, the positive signals on the VARIANT 1 and VARIANT 1 lines are applied to the exclusive OR circuit 704A and 704B which are used to invert bits 0 and 2 of each byte read out of MK memory 700 thereby providing a variant of the master key for transfer to the crypto engines.

Referring now to FIG. 22c2, positive signals are maintained at the inputs of the AND circuit 380 to thereby render it effective to apply and maintain a positive signal on the —W ENABLE line. The AND invert circuit 370 and 374 are alternately rendered effective by 03L and —01L clock pulses, respectively; the AND invert circuit 370 controlling the AND invert circuit 376 and inverter 378 to produce successive negative signals on the —M ENABLE line which in combination with the positive signal on the —W ENABLE line allows successive reading of the MK memory 700 while the AND invert circuit 374 controlling the AND invert circuit 376 and inverter 388 in FIG. 22d2 to produce successive positive signals on the STEP CTR line for successively stepping the address counter 390 to address successive locations on the MK memory 700. Successive pairs of half bytes read out of the MK memory 700 in FIG. 22e1 are shifted into the shift registers 702 to provide successive bytes of the master key for the crypto engines. If the encipher master key order being performed is EMK0, the successive bytes of the master key are transferred in unmodified form to the crypto engines whereas if the encipher master key order being performed is EMK1, then bits 0 and 2 of each byte are inverted by the exclusive OR circuits 704A and 704B to effectively provide a variant of the master key for transfer to the crypto engines.

Referring now to the AND invert circuit 568 in FIG. 22g4 a 01 DEL clock pulse in combination with positive signals on the C1, —STEP CTR and LMK lines are applied to render the AND invert circuit 568 effective to produce a negative signal to set the LDK latch 570 which, in being set, initiates production of the positive signals on the SR, LDK and LDK control lines for the crypto engines, in a manner previously described in detail in connection with the DECK order operation. Referring now to the crypto engine in FIG. 22g1, the successive positive signals on the LDK line are applied to successively condition the AND circuit 807 to permit a parity check to be made of each byte loaded into the key registers for parity errors. The successive positive signals on the SR, LDK and LDK lines are applied as control inputs to the key registers UKR 350 and LKR

400 to shift the key registers and allow successive bytes to be loaded into the key registers.

Referring now to FIG. 22b2, at TD time, while the key registers are being loaded, a positive signal is applied via the SYNCH TD line to render the AND circuit 270, conditioned by the positive signal on the WR DSD order line, effective to provide a positive signal on the WR ORD TIME line. Referring now to FIG. 22b2', the positive signal on the WR ORD TIME line is applied to the inverter 322 where it is inverted to a negative signal on the —WR ORD TIME line and applied to reset the EMK latch 346 in FIG. 22c3' and the SPEC ENC latch 494 in FIG. 22d5. Referring now to FIG. 22b2', the positive signal on the WR ORD TIME line is applied to the remaining input of the AND invert circuits 344 and 345 to render one of them effective, depending upon whether the EMK0 or EMK1 order operation is being performed, to produce a signal on the —SET EMK0 line or the —SET EMK1 line, respectively, to decondition the AND circuit 345 causing a negative signal to be applied to set the EMK latch 346 which, in being set, applies a positive signal to the EMK line. Referring now to FIG. 22d5, the positive signal on the EMK line is applied to the OR invert circuit 490 where it is inverted to a negative signal to set the SPEC ENC latch 494 which, in being set, applies a positive signal to the SP ENC line and a negative signal to the —SP ENC line. Referring now to FIG. 22e3, the positive signal on the SP ENC line is applied via the OR circuit 522 to condition the AND circuit 536 and 538 in FIG. 22g3 and via the inverter 546 to apply a negative signal to the DEC line to decondition the AND invert circuits 548 and 560.

Referring now to FIG. 22d2, after the 8th byte is loaded into the key registers, the address counter 390 steps from an address count of 15 back to an address count of 0 (count of 16) causing a positive signal to be produced on the —C8 line which is applied to condition the AND invert circuit 402 and to render the AND circuit 406, conditioned by the positive signal output by the 16 STEP latch 404, effective to produce a positive signal which is inverted by inverter 408 to a negative signal on the —16 STEP line. Referring now to FIG. 22g4, the negative signal on the —16 STEP line is applied to reset the LMK latch 566 which, in being reset, applies a negative signal to the LMK line and a positive signal to the —LMK line. The negative signal on the LMK line deconditions the AND invert circuit 568 to inhibit further production of the shifting control signals SR, LDK and LDK for the key registers of the crypto engines. Referring now to FIG. 22c2, the positive signal on the —LMK line is applied to render the AND invert circuit 368 effective to apply a negative signal to decondition the AND invert circuits 370 and 374 to inhibit further reading of the MK memory 700 and stepping of the address counter 390.

After loading the key registers of the crypto engines, a series of 8 PIOW commands are received with the data fields associated with the commands constituting the operational key or the secondary key to be enciphered, being written into the buffer registers of the crypto engines. The writing operation of the operational key or the secondary key into the buffer registers of the crypto engines by a series of 8 PIOW commands is similar to the writing operation described in detail in DEC order operation i.e. an input cycle is initiated, the byte counter 448 is conditioned to count each PIOW data command received and the operational key or

secondary key is written, a byte at a time, per PIOW data command, into the buffer registers UBR 100 and LBR 150. After the 8th byte of the operational key or the secondary key has been written into the buffer registers, then, 04 time of that clock cycle, the byte counter 448 steps from a count of 7 back to a count of 0 causing a negative signal to be produced to set the COUNT 8 latch 450 which, in being set applies a negative signal to the -CT8 line. The negative signal on the -CT8 line is applied to reset the INPUT CYCLE latch 454 in FIG. 22e3 thereby ending the input cycle. Referring now to FIG. 22d3, the INPUT CYCLE latch 454, in being reset, applies a positive signal on the -IN CYCLE line which, in combination with the positive signal on the -OUT CYCLE line, renders the AND invert circuit 410 effective to apply a negative signal to reset the COUNT 8 latch 450 in FIG. 22d4 and is inverted by inverter 412 to a positive signal to set the BLOCK COUNT flip flop 414 producing a positive signal on the -BLK0 line and a negative signal on the -BLK1 line.

Referring now to FIG. 22/3, at 01 time of the next clock cycle, a 01 DEL clock pulse in combination with positive signals on the -IN CYCLE line and from the START IN CYCLE END latch 530 render the AND invert circuit 532 effective to apply a negative signal to set the IN CYCLE END latch 534, which, in being set, applies a positive signal to the IN CYCLE END line. Referring now to FIG. 22/4, the positive signal on the IN CYCLE END line is applied to the inverter 622 where it is inverted to a negative signal to decondition the AND circuit 626 which, in turn, causes a negative signal to be applied to set the START EB latch 628 and to the AND inverter 638 in FIG. 22g4 where it is inverted to a positive signal and applied to render the OR invert circuit 640 effective to apply negative signals via the -ELR and -LDR lines to one input of the OR invert circuits 642 and 644.

Referring now to FIG. 22g3, the positive signal on the IN CYCLE END line in combination with the positive signal on the ENC line are applied to render the AND circuit 538 effective to apply a positive signal to the OR invert circuit 540 which, in turn, applies a negative signal via the -SL line to one input of the OR invert circuit 544. Referring now to FIGS. 22g3 and 22g4, at 02 time, a -C clock pulse is applied to the other inputs of the OR invert circuits 544, 642 and 644 to decondition them causing positive signals to be applied via the SL, ELR and LDR lines, respectively, to the control signal cable connected to the crypto engines. The positive signal on the SL line initiates production of the LDK control signal and the positive signal on the LDR line is applied to initiate production of the LDR control signal both of which are applied via the control signal cable to the crypto engines. Referring now to the crypto engine in FIG. 22g1, the control signal LDR and LDR are effective for causing the operational key or the secondary key stored in the buffer registers UBR 100 and LBR 150 to be transferred and loaded into the data registers UDR 200 and LDR 250 in preparation for the encipher function. The control signals on the SL and LDK lines are applied to the key registers causing the contents thereof to be shifted one position to the left as a pre-shift operation prior to the encipher operation.

Referring now to FIGS. 22e3 and 22/3, at 04 time a 04 clock pulse in combination with the positive signal on the IN CYCLE END line are applied to render the AND invert circuit 528 effective to apply a negative

signal to reset the START IN CYCLE END latch 530. At 01/L time of the next clock cycle, a -01/L clock pulse is applied to reset IN CYCLE END latch 534 causing a negative signal to be produced on the IN CYCLE END line. Referring now to FIG. 22/4, the negative signal on the IN CYCLE END line is applied to the inverter 622 where it is inverted to a positive signal and applied to render the AND circuit 626 effective to produce a positive signal which, in turn, renders the AND invert circuit 630, conditioned by the positive signal from the START EB latch 628, effective to apply a negative signal to set the EB latch 632 indicating the start of the crypto operation. The EB latch 632, in being set, applies a positive signal to the EB line and a negative signal to the -EB line. Referring to FIGS. 22d2 and 22c2, a positive signal on the EB line is applied to condition the address decoder AND invert circuit 398 and to condition the ER flip flop 384 to permit stepping of the round counter 390. Referring now to FIG. 22/4, the negative signal on the -EB line is applied to set the START EB END latch 612 and referring to FIG. 22e5, if the EMK1 order operation is being performed, to reset the KEY VAR 1 CTRL latch 513.

The encipher function operation is similar to that previously described in detail in connection with the encipher order operation and can generally be followed by referring to the timing diagram of FIGS. 29a-29c. Generally, the encipher function is performed by repeating a product cipher function for 16 rounds. During each round, the contents of the upper data register UDR 200 is enciphered under control of the contents of the key register UKR 350 and LKR 400, which may contain the master key or a variant of the master key, depending upon whether the EMK0 or EMK1 order operation is being performed, with the results being added to the contents of the lower data register LDR 250 by the modulo-2 adders 650-664. At the end of each round, the outputs of the modulo-2 adders are parallel transferred to the upper data register UDR 200 while the contents of the upper data register UDR 200 are parallel transferred to the lower data register LDR 250 to form the arguments for the next round and the key registers are shifted by the control signal on the SL line in accordance with the key shift schedule shown. As a result of the single pre-shift signal on the SL line and the 27 additional signals on the SL line during the encipher operation, the key registers shift left exactly 28 times to return the master key or the variant of the master key back to the initial home position in the key register. At the end of the encipher function, half of the enciphered operational or secondary key is available at the output of the upper data register UDR 200 and the other half is available at the outputs of the cipher function circuits.

Following the encipher operation, a series of 8 PIOR data commands are received for reading the enciphered operational or secondary key. The first such command initiates an output cycle which is performed in a similar manner to that described in detail in connection with the encipher order operation. In general terms, during the execution of the PIOR data command, while the block count is at a count of one, the enciphered operational or secondary key is parallel transferred from the upper data register and the outputs of the cipher function circuits to the buffer registers where it is then available for reading, a byte at a time. At the beginning of the execution of the first PIOR data command, a negative signal is applied on the OUT CYCLE START line to reset the EMK latch 346 in FIG. 22c3' and at the end of

the execution of each PIOR command, the buffer registers are shifted one position to present the next byte of the enciphered operational or secondary key for reading. At the 8th count of the byte counter, the output cycle ends and the block counter is reset to end the operation.

REENCIPHER FROM MASTER KEY (RFMK) ORDER OPERATION

The function of this operation is to reencipher an operational key enciphered under a host master key to the operational key enciphered under a secondary key which is itself enciphered under a variant of the host master key.

During command time of this operation, when the order code specifying a RFMK order is decoded, a load master key (LMK) latch and a key variant 1 latch are set and a special encipher (SP ENC) latch is reset. With the LMK latch set, the contents of the MK memory is caused to be read out for transfer to the crypto engines and with the key variant 1 latch set each byte of the master key transferred is modified to provide a variant (KMH1) of the master key (KMH0). The variant of the master key is parity checked, a byte at a time, and loaded as a working key into the key registers of the crypto engines. During synch TD time of this operation, a RFMK latch is set causing a key order (K ORD) signal to be produced indicating that a key order operation is to be performed and an encipher (ENC) latch is reset causing the processing mode to be set for a decipher (DEC) operation. After the 8th byte is loaded into the key registers, the LMK latch is reset to terminate further MK memory read out. A series of 8 PIOW data commands is then received with the data fields associated with the commands, constituting a secondary key enciphered under the same variant of the host master key stored in the key registers, being loaded into the buffer registers of the crypto engines. The first such command initiates a first input cycle and a byte counter counts each such command received. After the 8 PIOW commands have been received and the 8th byte written into the buffer registers, then, at the 8th count, the input cycle ends, the enciphered secondary key is transferred from the buffer registers to the data registers of the crypto engines, a block counter is set, the crypto engines start a decipher operation, indicated by the generation of an engine busy signal, and the key variant 1 latch is reset. During the decipher operation the secondary key enciphered under the variant of the host master key in the data registers of the crypto engines is deciphered under control of the same variant of the host master key in the key registers of the crypto engines to obtain the secondary key in clear form. At the end of the decipher operation, half of the secondary key, now in clear form, is available at the outputs of the upper data register UDR and the other half is available at the outputs of the cipher function circuits. Additionally, at the end of the decipher operation, a special key operation (SP KEY OP) latch is set.

A second series of 8 PIOW data commands is then received with the data fields associated with the commands, constituting the operational key enciphered under the host master key, being loaded into the buffer registers of the crypto engines. The first such command received initiates a second input cycle and the byte counter again counts each such command received. After the 8 PIOW commands have been received and the 8th byte written into the buffer registers, then, at the

8th count, the second input cycle ends, the block counter is reset and the operational key enciphered under the host master key is transferred from the buffer registers to the data registers of the crypto engines while, at the same time, the secondary key, in clear form, is transferred from the outputs of the upper data register and the outputs of the cipher function circuits to the buffer registers. Following the end of this second input cycle, the LMK latch is again set and the host master key contents of MK memory (KMH0) is caused to be read out for transfer to the crypto engines. The host master key is parity checked, a byte at a time, and loaded as the working key into the key registers of the crypto engines. After 8th byte is loaded into the key registers, the LMK latch is reset to terminate further MK memory read out and the crypto engines then start a second decipher operation, indicated by the EB signal, to decipher the operational key enciphered under the host master key in the data registers of the crypto engines under control of the host master key in the key registers of the crypto engines to obtain the operational key in clear form. At the end of the second decipher operation, half of the operational key, now in clear form, is available at the outputs of the upper data register UDR and the other half is available at the outputs of the cipher function circuits. Additionally, at the end of the second decipher operation, with the RFMK and SP K OP latches set, a first output cycle is initiated, at the start of which, the special encipher (SP ENC) latch is set causing the processing mode to now be set for an encipher (ENC) operation. Additionally, at the start of the output cycle, an end of round 16 (ER16) signal is produced to cause the half of the operational key at the outputs of the cipher function circuits to be transferred to the lower data register LDR so that the full operational key in clear form is now stored in the combined upper and lower data registers of the crypto engines. During the first output cycle, the buffer registers and the key registers are shifted in synchronism, once for each clock cycle, causing the secondary key, now stored in the buffer registers, to be shifted into the key registers, a byte at a time. During this transfer, each byte is checked for a parity error. The byte counter counts clock cycles and at the 8th count, the first output cycle ends, the block counter is again set and the RFMK latch is reset causing the key order signal to be terminated.

During the first clock cycle after the end of the first output cycle, the key registers are pre-shifted one position in preparation for the encipher operation. At the end of this clock cycle, the crypto engines then start the special encipher operation, indicated by the generation of the EB signal, and the EB signal together with the SP ENC latch still being set cause the SP K OP latch to be reset signaling the end of the special key operation. During the special encipher operation, the operational key, presently in the data registers, is enciphered under control of the secondary key, presently in the key registers, to obtain the operational key enciphered under the secondary key. At the end of the special encipher operation, half of the operational key enciphered under the secondary key is available at the outputs of the upper data register and the other half is available at the outputs of the cipher function circuits.

A series of 8 PIOR data commands is now received for reading the enciphered operational key. The first such command initiates a second output cycle and the byte counter counts each such command received. Dur-

ing the execution of the first PIOR data command, while the block count is at a count of 1, the enciphered operational key is parallel transferred from the outputs of the upper data register and the outputs of the cipher function circuits to the buffer registers where it is then available for reading, a byte at a time. At the end of the execution of each PIOR command, the buffer registers are shifted one position to present the next byte of the enciphered operational key for reading. At the 8th count of the byte counter, the second output cycle ends and the block counter is reset to end the RFMK operation.

A more detailed description of the RFMK order operation will now be given in conjunction with the timing diagrams of FIGS. 30a-30g. After address selection at TA time and loading the command byte into the command register at TC time, the command code is decoded by the AND invert circuit 266 in FIG. 22b2 to produce a negative signal which is inverted by inverter 268 to a positive signal on the WR DSD ORDER line thereby indicating the presence of a WR DSD ORDER command. At the same time, the order code is decoded by the AND invert circuit 324 to apply a negative signal via the -RFMK DEC line to the inverter 326 where it is inverted to a positive signal and applied to one input of the AND invert circuit 328. Referring now to the inverter 478 in FIG. 22d5, the negative signal on the -RFMK DEC line is inverted to a positive signal and passed via the OR circuit 484 to the SET LMK line. Referring now to the OR invert circuit 564 in FIG. 22g4, the positive signal on the SET LMK line is applied to render the OR invert circuit 564 effective to apply a negative signal to set the LMK latch 566 producing a positive signal on the LMK line and a negative signal on the -LMK line. Referring now to the AND invert circuit 368 in FIG. 22c2, the negative signal on the -LMK line is applied to decondition the AND invert circuit 368 which, in turn, maintains a positive signal at one input of the AND invert circuits 370 and 374 so long as the LMK latch 566 remains set i.e. while the MK memory is being read out. Referring now the KEY VAR 1 CTRL latch 513 in FIG. 22e5, the negative signal on the -RFMK DEC line is applied to set the KEY VAR 1 CTRL latch 513 which, in being set, applies a positive signal to the VARIANT 1 line and via the OR circuit 518 to the VARIANT $\frac{1}{2}$ line. Referring now to FIG. 22e1, the positive signals on the VARIANT $\frac{1}{2}$ and VARIANT 1 lines are applied to the exclusive OR circuits 704A and 704B which are used to invert bits 0 and 2 of each byte read out of the MK memory 700 thereby providing a variant of the master key for transfer to the crypto engines. The balance of the operation for loading the variant of the master key into the key registers of the crypto engine can be followed from the timing diagrams of FIGS. 30a-30g and is similar to that described in detail in connection with the DECK order operation which may be referred to for such detail.

Referring now to FIG. 22b2, at TD time, while the variant of the master key is being loaded into the key registers, a positive signal is applied via the SYNCH TD line to render the AND circuit 270, conditioned by the positive signal on the WR DSD ORDER line, effective to provide a positive signal on the WR ORD TIME line. Referring now to FIG. 22b2', the positive signal on the WR ORD TIME line is applied to the inverter 322 where it is inverted to a negative signal on the -WR ORD TIME line to reset RFMK latch 330 in FIG. 22c3'

and the SPEC ENC latch 494 in FIG. 22d5. Referring now to FIG. 22b2', the positive signal on the WR ORD TIME line is applied to the remaining input of the AND invert circuit 328 to render it effective to produce a negative signal on the -SET RFMK line which is applied to set the RFMK latch 330 which, in being set, applies a positive signal to the RFMK line and a negative signal to the -RFMK line. Referring now to FIG. 22c4, the negative signal on the -RFMK line is applied to decondition the AND invert circuit 298 causing a positive signal to be applied to the K ORD line and via the inverter 300 to a negative signal on the -K ORD line. The negative signal on the -K ORD line is applied to reset the ENC latch 312, which, in being reset, applies a negative signal to the ENC line. Referring now to FIG. 22g3, the negative signal on the ENC line is applied to decondition the AND circuits 536 and 538 and via the inverter 546 applies a positive signal to the DEC line to condition the AND invert circuits 548 and 560 for a decipher operation. Referring now to FIG. 22g4, after the 8th byte of the variant of the master key is loaded into the key registers, a negative signal on the -16 STEP line is applied to reset the LMK latch 566 to terminate further MK memory read out.

The next operation to be performed is to write the secondary key enciphered under the same variant of the host master key into the buffer registers of the crypto engines. This writing operation can be followed from the timing diagrams of FIGS. 30a-30g and is similar to the writing operation described in detail in the DECK order operation. In general terms, a series of 8 PIOW data commands is received with the data fields associated with the commands, constituting the secondary key enciphered under the same variant as the host master key stored in the key registers, being loaded into the buffer registers of the crypto engines. The first such command initiates a first input cycle and the byte counter 448, in FIG. 22d4, counts each such command received. After the 8 PIOW commands have been received and the 8th byte written into the buffer registers, then, at the 8th count, the input cycle ends, the BLOCK COUNT flip flop 414, in FIG. 22d3, is set, the enciphered secondary key is transferred from the buffer registers to the data registers of the crypto engines and the crypto engines then start a decipher operation, indicated by the generation of an engine busy EB signal, to decipher the secondary key enciphered under the variant of the host master key in the data registers of the crypto engines under control of the variant of the host master key in the key registers of the crypto engines to obtain the secondary key in clear form. Referring to FIG. 22e5, additionally, at the start of the decipher operation a negative signal on the -EB line is applied to reset KEY VAR 1 CTRL latch 513 which, in being reset, applies a negative signal to the VARIANT 1 line and via the OR circuit 518 to a negative signal on the VARIANT $\frac{1}{2}$ line, both of which are effective to decondition the exclusive OR circuits 704A and 704B in FIG. 22e1, respectively, so that a subsequent transfer of the master key from the MK memory to the crypto engines will be in unmodified form. At the end of the decipher operation, half of the secondary key, now in clear form, is available at the outputs of the upper data register and the other half is available at the outputs of the cipher function circuits. Referring now to FIG. 22d5, at the end of the decipher operation, a positive signal is applied to the EB END line which is applied, in combination with positive signals on the RFMK and -SP ENC

lines, to render the AND circuit 480 effective for one clock cycle, at the end of which, the positive signal on the EB END line is terminated with a negative signal being applied to decondition the AND circuit 480 causing a negative signal to be applied to turn on the SPEC KEY OP latch 504 in FIG. 22e5 to signal a special key operation.

The next operation to be performed is to write the operational key enciphered under the host master key into the buffer registers of the crypto engines. This operation can also be followed from the timing diagrams of FIGS. 30a-30g and is similar to the write operation described in detail in the DECK order operation. In general terms, a series of 8 PIOW data commands is received with the data fields associated with the command, constituting the operational key enciphered under the host master key being loaded into the buffer registers of the crypto engines. The first such command initiates a second input cycle and the byte counter 448 again counts each such command received. After the 8 PIOW commands have been received and the 8th byte written into the buffer registers, then, at the 8th count, the input cycle ends, the BLOCK COUNT flip flop 414 in FIG. 22d3 is reset and the operational key enciphered under the host master key is transferred from the buffer registers to the data registers of the crypto engines by the control signals LDR and $\overline{\text{LDR}}$ in FIG. 22g1 while at the same time, the secondary key in clear form is transferred from the outputs of the upper data register UDR 200 and the outputs of the modulo-2 adders 650-664 to the buffer registers UBR 100 and LBR 150 by the control signals ELR and $\overline{\text{LIB}}$ as shown in FIG. 22g1.

Referring now to the AND circuit 475 in FIG. 22d5, at the end of the input cycle, a positive signal is applied to the IN CYCLE END line which in combination with positive signals on the RFMK and SP K OP lines render the AND circuit 475 effective to apply a positive signal via the OR circuit 484 to the SET LMK line. Referring now to FIG. 22g4, the positive signal on the SET LMK line is applied to render the OR invert circuit 564 effective to apply a negative signal to set the LMK latch 566 which, in being set, initiates the operation for reading the contents of the MK memory 700 for transfer in unmodified form to the crypto engines. Referring now to FIG. 22g1, successive control signals LDK and $\overline{\text{LDK}}$ permit the master key to be loaded, a byte at a time, as the working key into the key registers of the crypto engines. Additionally, the successive control signals LDK successively condition the AND circuit 807, to permit a parity check to be made of each byte loaded into the key registers.

Referring now to FIG. 22g4, after the 8th byte is loaded into the key registers, a negative signal on the -16 STEP line is applied to reset the LMK latch 566, which, in being reset, terminates further MK memory readout. Additionally, referring to the AND invert circuit 621 in FIG. 22f4, a positive signal on the 16 STEP line together with positive signals on the -SP ENC, RFMK and SP K OP lines are applied to render the AND invert circuit 621 effective to apply a negative signal to decondition the AND circuit 626 which, in turn, applies a negative signal to set the START EB latch 628. At the end of the positive signal on the 16 STEP line, the AND invert circuit 621 is deconditioned causing a positive signal to be applied to render the AND circuit 626 effective to apply a positive signal to one input of the AND invert circuit 630. Accordingly,

with the START EB latch now set, a positive signal is applied to the other input of the AND invert circuit 630 to render the AND invert circuit 630 effective to apply a negative signal to set the EB latch 632 producing a positive signal on the EB line and a negative signal on the -EB line indicating the start of the second decipher operation. A second decipher operation is then performed to decipher the operational key enciphered under the host master key in the data registers of the crypto engines under control of the host master key in the key registers of the crypto engines to obtain the operational key in clear form. Referring now to FIG. 22g1, at the end of the second decipher operation, half of the operational key, now in clear form, is available at the outputs of the upper data register UDR 200 and the other half is available at the outputs of the modulo-2 adders 650-664.

Referring now to FIG. 22f4, at 04 time, a 04 clock pulse in combination with positive signals on the C1 and 14, 15 lines are applied to render the AND invert circuit 624 effective to apply a negative signal to reset the START EB latch 628 and the EB latch 632 which, in being reset, applies a negative signal on the EB line and a positive signal on -EB line. At 01 time of the next clock cycle, a 01 DEL clock pulse in combination with the positive signal on the -EB line and the positive signal from the START EB EBD latch 612 are applied to render the AND invert circuit 614 effective to apply a negative signal to set the EB EBD latch 616 which, in being set, applies a positive signal to EB END line and a negative signal to the -EB END line. Referring now to the AND circuit 382 in FIG. 22c2, the negative signal on the -EB END line is applied to decondition the AND circuit 382 causing a negative signal to be applied to reset the round counter 390 in FIG. 22d2.

Referring now to the AND circuit 508 in FIG. 22e5, the positive signal on the EB END line in combination with the positive signals on the RFMK and SP K OP lines are applied to render the AND circuit 508 effective to apply a positive signal on the INIT OUT CYC line. The positive signal on the INIT OUT CYC line is applied to the OR invert circuit 490 in FIG. 22d5 where it is inverted to a negative signal to set the SPEC ENC latch 494 which, in being set, applies a positive signal to the SP ENC line and a negative signal to -SP ENC line. Referring now to FIGS. 22e3, and 22g3, the positive signal on the SP ENC line is passed via the OR circuit 522 to the ENC line where it is applied to condition the AND circuits 536 and 538 for an encipher operation and is inverted to a negative signal on the DEC line via the inverter 546 to decondition the AND invert circuits 548 and 560 used during a decipher operation. Referring now to FIG. 22e3, the positive signal on the INIT OUT CYC line is also applied to the OR invert circuit 456 causing a negative signal to be applied to set the OUTPUT CYCLE latch 464 which, in being set, applies a positive signal on the OUT CYCLE line and a negative signal on the -OUT CYCLE line. Referring now to FIG. 22f3, the positive signal on the OUT CYCLE line in combination with the 01 DEL clock pulse and the positive signal from the set START OUT CYCLE START latch 554 are applied to render the AND invert circuit 556 effective to apply a negative signal to set the OUT CYCLE START latch 558 which, in being set, applies a positive signal to the OUT CYCLE START line and a negative signal to the -OUT CYCLE START line. Referring now to FIG. 22e5, the positive signal on the OUT CYCLE START

line in combination with the positive signals on the SP K OP and RFMK lines are applied to render the AND invert circuit effective to apply a negative signal via the —ER 16 line to one input of the OR invert circuit 646 in FIG. 22g4. The positive signals on the OUT CYCLE and K ORD lines are applied to render the AND invert circuit 598 effective to apply a negative signal to decondition the AND circuit 600 and via the —LKD line to decondition the AND circuit 572 and to one input of the OR invert circuit 604. The AND circuit 600 in being deconditioned applies a negative signal via the —LIB line to one input of the OR invert circuit 602 while the AND circuit 572 in being deconditioned applies a negative signal via the —SR line to one input of the OR invert circuit 574. Referring now to FIG. 22/3, the negative signal on the —OUT CYCLE line is applied to set the START OUT CYCLE END latch 580. Referring now to FIG. 22g4, at 02 time, a —C clock pulse is applied to the other inputs of the OR invert circuits 602, 604, 574 and 646, causing them to be deconditioned to apply positive signals via the LIB, LKB, SR and ER 16 lines to the control signal cable connected to the crypto engines. The positive signal on the LIB line is also applied to the OR invert circuit 648 causing a negative signal, delayed by delay circuit 650, to be applied via the LIB line to the control signal cable. The positive signal on the SR line is also applied to the OR applied to render the AND invert circuit 556 effective to apply a negative signal to set the OUT CYCLE START latch 558 which, in being set, applies a positive signal to the OUT CYCLE START line and a negative signal to the —OUT CYCLE START line. Referring now to FIG. 22e5, the positive signal on the OUT CYCLE START line in combination with the positive signals on the SP K OP and RFMK lines are applied to render the AND invert circuit effective to apply a negative signal via the —ER 16 line to one input of the OR invert circuit 646 in FIG. 22g4. The positive signals on the OUT CYCLE and K ORD lines are applied to render the AND invert circuit 598 effective to apply a negative signal to decondition the AND circuit 600 and via the —LDK line to decondition the AND circuit 572 and to one input of the OR invert circuit 604. The AND circuit 600 in being deconditioned applies a negative signal via the —LIB line to one input of the OR invert circuit 602 while the AND circuit 572 in being deconditioned applies a negative signal via the —SR line to one input of the OR invert circuit 574. Referring now to FIG. 22/3, the negative signal on the —OUT CYCLE line is applied to set the START OUT CYCLE END latch 580. Referring now to FIG. 22g4, at 02 time, a —C clock pulse is applied to the other inputs of the OR invert circuits 602, 604, 574 and 646, causing them to be deconditioned to apply positive signals via the LIB, LKB, SR and ER 16 lines to the control signal cable connected to the crypto engines. The positive signal on the LIB lines is also applied to the OR invert circuit 648 causing a negative signal, delayed by delay circuit 650, to be applied via the LIB line to the control signal cable. The positive signal on the SR line is also applied to the OR clock pulse is applied to reset the OUT CYCLE START latch 558 and the EB END latch 616. Referring now to FIG. 22e5, the negative signal on the OUT CYCLE START line is applied to decondition the AND invert circuit 506 which, in turn, applies a positive signal to the —ER 16 line to effectively terminate any further ER 16 control signals to the crypto engine.

Referring now to FIGS. 22g4, and 22h4, at 02 time, a —C clock pulse is effective to again decondition the OR invert circuits 602, 604 and 574 to initiate production of the control signals on the LIB, LKB, SR, LIB and LDK. Referring now to the crypto engines in FIG. 22g1, the LKB and LDK control signals are effective to load the next byte of the operational key from the buffer registers to the key registers, the LIB and LIB and SR and LDK control signals are effective to simultaneously shift the buffer registers and the key registers in synchronism so that the next byte of the operational key is available at the outputs of the buffer registers and the previously loaded byte of the operational key in the key registers is shifted one position. In a similar manner, the buffer registers and the key registers of the crypto engine are shifted in synchronism, once for each clock cycle, causing successive bytes of the operational key, in clear form, to be transferred from the buffer registers to the key registers.

The byte counter 448 counts the clock cycles and, at the 8th count, a negative signal is applied to set the COUNT 8 latch 450, which, in being set, applies a negative signal via the —CT8 line to reset the OUTPUT CYCLE latch 454 in FIG. 22e3. The OUTPUT CYCLE latch 454, in being reset, applies a positive signal to the —OUT CYCLE line and a negative signal on the OUT CYCLE line. Referring now to FIG. 22d3, the combination of positive signals on the —OUT CYCLE line and the —IN CYCLE line render the AND invert circuit 410 effective to apply a negative signal to reset the COUNT 8 latch 450 in FIG. 22d4, and is inverted by inverter 412 to a positive signal to reset BLOCK COUNT flip flop 414 producing a negative signal on the —BLK0 line and a positive signal on the —BLK1 line. The negative signal on the OUT CYCLE line is also applied to decondition the AND invert circuit 598 in FIG. 22g4 to initiate termination of the positive signals on the LIB, LKB and SR control lines to inhibit further shifting of the buffer key registers in the crypto engines. Referring now to FIG. 22/3, the negative signal on the OUT CYCLE line is applied to set the START OUT CYCLE START latch 554. Referring now to FIG. 22/3, at 01 time of the next clock cycle, a 01 DEL clock pulse in combination with the positive signal on the —OUT CYCLE line and the positive signal output of the START OUT CYCLE END latch 580 are applied to render the AND invert circuit 582 effective to produce a negative signal to set the OUT CYCLE END latch 584 which, in being set, applies a positive signal to the OUT CYCLE END line.

Referring now to FIG. 22e5, the positive signal on the OUT CYCLE END line in combination with the positive signal on the SP K OP line render the AND invert circuit 505 effective to apply a negative signal to the —SET EB line. Referring now to FIG. 22c3' the negative signal on the —SET EB line is applied to reset the RFMK latch 330, which, in being reset, applies a positive signal via the —RFMK line to render the AND invert circuit 298 in FIG. 22c4 effective to apply a negative signal to the K ORD line and via the inverter 330 a positive signal on the —K ORD line indicating the end of the key order operation. Referring now to FIG. 22/3, the negative signal on the —SET EB line is inverted to a positive signal on the SET EB line and applied via the SET EB line to the OR invert circuit 540 causing a negative signal to be applied to one input of the OR invert circuit 544 to initiate production of the SL control signal to pre-shift the key registers of the

crypto engines in preparation for the encipher operation. Referring now to FIG. 22/4, the negative signal on the -SET EB line is applied to decondition the AND circuit 626, which, in being deconditioned, applies a negative signal to set the START EB latch 628. Referring now to FIGS. 22e3, and 22/3, at 04 time, a 04 clock pulse is applied to render the AND invert circuit 578 effective to apply a negative signal to reset the START OUT CYCLE END latch 580. At 01 time of the next clock cycle, a -01/L clock pulse is applied to reset the OUT CYCLE END latch 584 which, in being reset, applies a negative signal via the OUT CYCLE END line to decondition the AND invert circuit 505 in FIG. 22e5 causing a positive signal to now be applied to the -SET EB line. Referring now to FIG. 22/4, the positive signal on the -SET EB line is applied to render the AND circuit 626 effective to apply a positive signal together with the positive signal output of the START EB latch 628 to render the AND invert circuit 630 effective to apply a negative signal to set the EB latch 632. The EB latch 632 in being set applies a positive signal to the EB line and a negative signal to the -EB line indicating the start of the encipher operation. Referring now to FIGS. 22d5 and 22e5, the positive signal on the EB line in combination with the positive signal on the SP ENC line is applied to render the AND invert circuit 502 effective to apply a negative signal to reset the SPEC K OP latch 504 which, in being reset, applies a negative signal to the SP K OP line indicating the end of the special key operation. During the encipher operation, the operational key stored in the data registers of the crypto engine are enciphered under control of the secondary communication key stored in the key registers of the crypto engine to obtain, at the end of the encipher operation, the operational key enciphered under the secondary communication key. Referring now to FIG. 22g1, at the end of the encipher operation half of the enciphered operational key is available at the output of the upper data register UDR 200 and the other half is available at the outputs of the modulo-2 adders 650-654.

The balance of the RFMK order operation can be followed from the timing diagram of FIGS. 30a-40g and is similar to that described in detail in connection with the encipher order operation which may be referred to for such details. In general terms, a series of 8 PIOW data commands is received for reading the enciphered operational key. The first such command initiates a second output cycle and the byte counter counts each such command received. During the execution of the first PIOW data command, while the block count is at a count of one, the enciphered operational key is parallel transferred from the outputs of the upper data register and the outputs of the cipher function circuits to the buffer registers where it is then available for reading, a byte at a time. At the end of the execution of each PIOW command, the buffer registers are shifted one position to present the next byte of the enciphered operational key for reading. At the 8th count of the byte counter, the second output cycle ends and the block counter is reset to end the RFMK order operation.

PROCEDURAL ERRORS

A procedural error is one in which the DSD receives a command out of sequence or at the wrong time, such that its execution would cause the destruction or loss of good data in the crypto engines or the providing of useless data from the crypto engines. There are three

commands that may cause a procedural error, namely, the PIOW data command, the PIOR data command and the WR DSD order command. The various error conditions which may occur for these three commands are described in the following.

1. Procedural errors for a PIOW data command

a. If a PIOW data command is issued while a read operation is being performed (an output cycle is in progress), this causes a procedural error since the buffer registers cannot be used concurrently for both reading and writing. Accordingly, referring to FIG. 22d3, while the output cycle is in progress, a negative signal is applied to decondition the AND invert circuit 428 causing a positive signal to be applied to one input of the AND invert circuit 432. Since a WMK order operation is not in progress, a positive signal is applied via the -WMK line to a second input of the AND invert circuit 432. Now, if an attempt is made to execute a PIOW data command before the end of the output cycle, a positive signal is applied via the PIOW DATA line to a third input of the AND invert circuit 432 thereby conditioning this circuit. At 03L time of the same clock cycle in which the positive signal is applied to the PIOW DATA line, a 03L clock pulse is applied to render the AND invert circuit 432 effective to apply a negative signal to decondition the AND circuit 438 which, in turn, applies a negative signal to the -PROC ERR line indicating a procedural error.

b. If a PIOW data command is issued while a block of data is contained in the buffer registers, this causes a procedural error since the buffer registers can only contain one block of data at a time. Accordingly, referring to FIG. 22d3, while a block of data is contained in the buffer registers, a negative signal is applied via the -BLK 1 line to decondition the AND invert circuit 428 causing a positive signal to be applied to one input of the AND invert circuit 432 and since a WMK order operation is not in progress and a PIOW data command is being attempted, positive signals are again applied via the -WMK and PIOW DATA lines to condition the AND invert circuit 432. At 03L time, the 03L clock pulse is again applied to apply a negative signal to decondition the AND circuit 438 which then applies a negative signal to the -PROC ERR line indicating a procedural error.

c. After a reset or after a WMK order operation, the cipher key in the key registers is invalid and a new cipher key must be loaded into the key registers by a DECK order command. If a PIOW data command is issued while an invalid key is present in the key registers, this causes a procedural error since a valid key is not present in the key registers. Accordingly, referring to FIG. 22d3, while an invalid key is present in the key registers, a negative signal is applied via the -key invalid line to decondition the AND invert circuit 428 causing a positive signal to be applied to one input of the AND invert circuit 432 and since a WMK order operation is not in progress and a PIOW data command is being attempted, positive signals are again applied via the -WMK and PIOW DATA lines to condition the AND invert circuit 432 to produce a procedural error signal at 03L time on the -PROC ERR line.

d. If a PIOW data command is issued to write a new master key into the MK memory less than 16 mi-

croseconds after issuing a WMK order command, a procedural error will occur since a WMK overwrite operation is in progress for overwriting the old master key in the MK memory. Therefore, referring to FIG. 22d3 a positive signal on the MK OVW line in combination with a positive signal on the PIOW DATA line renders the AND invert circuit 427 effective to apply a negative signal to decondition the AND circuit 438 to produce a negative signal on the -PROC ERR line indicating a procedural error.

2. Procedural errors for a PIOR data command

- a. If a PRIOR data command is issued while a write operation is presently being performed (an input cycle is in progress), this causes a procedural error since the buffer registers cannot be used concurrently for both reading and writing. Accordingly, referring to FIG. 22d3, while an input cycle is in progress, a negative signal is applied to decondition the AND invert circuit 416 causing a positive signal to be applied to condition the AND invert circuit 436. Now, if an attempt is made to execute a PIOR data command, a positive signal on the PIOR EARLY line is applied to render the conditioned AND invert circuit 436 effective to apply a negative signal to decondition the AND circuit 438 causing a negative signal to be applied to the -PROC ERR line indicating a procedural error.
- b. If a PIOR data command is issued at a time when there is no data contained in the buffer registers of the crypto engines, this causes a procedural error since there is no data to be read. Accordingly, referring to FIG. 22d3, at a time when there is no data contained in the buffer registers of the crypto engines, the BLOCK COUNT flip flop 414 is in a reset condition causing a negative signal to be applied via the -BLK 0 line to decondition the AND invert circuit 416 causing a positive signal to be applied to condition the AND invert circuit 436. Consequently, if an attempt is made to execute a PIOR data command, a positive signal on the PIOR EARLY line is again applied to render the conditioned AND invert circuit 436 effective to apply a negative signal to decondition the AND circuit 438 causing a negative signal to be applied to the -PROC ERR line indicating a procedural error.
- c. If a PIOR data command is issued at a time when any of the cipher key handling orders are in progress, this causes a procedural error since no data is to be read during these cipher key handling operations. Accordingly, referring to FIG. 22d3, whenever a key order operation is in progress a negative signal is applied via the -K ORD line to decondition the AND invert circuit 416 causing a positive signal to be applied to condition the AND invert circuit 436. Now, if an attempt is made to execute a PIOR data command, a positive signal on the PIOR EARLY line is applied to render to conditioned AND invert circuit 436 effective to apply a negative signal to decondition the AND circuit 438 causing a negative signal to be applied to the -PROC ERR line indicating a procedural error.
- d. If a PIOR data command is issued at a time when a block of data is loaded in the buffer registers and fewer than 32 usec have elapsed since the last PIOW data command was issued, a procedural

error will result since the engine is still busy processing the block of data. Therefore, referring to FIG. 22d3, while the engine is busy, a negative signal is applied via the -EB line to decondition the AND invert circuit 416 causing a positive signal to be applied to condition the AND invert circuit 436. Now, if an attempt is made to execute a PIOR data command, a positive signal on the PIOR EARLY is applied to render the conditioned AND invert circuit 436 effective to apply a negative signal to decondition the AND circuit 438 causing a negative signal to be applied to the -PROC ERR line indicating a procedural error.

3. Procedural errors for a WR DSD order command

- a. If a WR DSD order command is issued at a time when any of the cipher key handling orders are in progress, this causes a procedural error since a cipher key handling operation once begun must be completed. Accordingly, referring to FIG. 22d3, whenever a key handling order command is being performed a negative signal is applied via the -K ORD line to decondition the AND invert circuit 433 causing a positive signal to be applied to one input of the AND invert circuit 434. Now, if a WR DSD order command is given while a previous cipher key handling order is in progress, then, positive signals on the WR DSD ORDER and TC SEL lines are applied to render the AND invert circuit 434 effective to apply a negative signal to decondition the AND circuit 438 causing a negative signal to be applied to the -PROC ERR line indicating a procedural error.
- b. If a WR DSD order command is issued at a time when data from the buffer registers of the crypto engines are being read, this causes a procedural error since unread data still remains in the crypto engines. Referring now to FIG. 22d3, while data is being read from the buffer registers of the crypto engines, the block count flip flop 414 is in a set state causing a positive signal to be applied via the -BLK 0 line to the inverter 418 where it is inverted to a negative signal to decondition the AND invert circuit 433 which, in being deconditioned, applies a positive signal to one input of the AND invert circuit 434. Now, when a WR DSD order command is issued, positive signals are applied via the WR DSD ORDER and TC SEL lines to render the AND invert circuit 434 effective to apply a negative signal to decondition the AND circuit 438 causing a negative signal to be applied to the -PROC ERR line indicating a procedural error.
- c. If a WR DSD order command is issued at a time when a write operation is being performed (an input cycle is in progress), this causes a procedural error since a process once begun must be completed. Accordingly, referring to FIG. 22d3, while an input cycle is in progress, a negative signal is applied via the -IN CYCLE line to decondition the AND invert circuit 433 which, in turn, applies a positive signal to one input of the AND invert circuit 434, as described above, so that when a WR DSD order command is issued the AND invert circuit 434 is rendered effective to initiate generation of a negative signal on the -PROC ERR line indicating a procedural error.
- d. If a WMK order command is issued at a time when the EW switch is off, this causes a procedural error since the command cannot be executed unless the

EW switch is switched on. Referring now to FIG. 22c3, if the enable write switch is off, a negative signal on the EWMK line is applied to the inverter 423 where it is inverted to a positive signal and applied to one input of the AND invert circuit 425. Now, when a cipher key handling order command is decoded and further particularized as a WMK order command by a positive signal on the -Y line then, positive signals are applied via the WMK and -Y lines to condition the AND invert circuit 425. At SYNCH TD time of the WMK order operation, a positive signal is applied via the WR ORD TIME line to render the AND invert circuit 425 effective to apply a negative signal to decondition the AND circuit 438 in FIG. 22e3 causing a negative signal to be applied to the -PROC ERR line indicating a procedural error.

Referring now to FIG. 22i2, whenever a procedural error occurs because of any of the above conditions, the negative signal on the -PROC ERR line is applied to set the bit 0 and bit 1 latches 954A and 954B of the status register 952 to provide an indication of the procedural error.

ERROR CONDITIONS

Six different kinds of errors are detected in the data security device. Each kind, when it is detected, results in the setting of a unique combination of bits in the status register thereby providing information usable by the processor in carrying out error recovery procedures. The combination of bits in the status register for the different kinds of errors is shown in the following table.

Error Condition	STATUS BITS				
	0	1	2	3	5
Command Error	—	—	—	—	1
Illegal Order	1	—	1	—	—
Procedural Order	1	1	—	—	—
Write Error	—	—	—	1	—
Key Bus Error	—	1	1	—	—
Engine Error	—	1	—	—	—

The contents of the status register, indicating error conditions, if any, are read back to the processor under control of a READ BS command which will now be described.

READ BASIC STATUS COMMAND OPERATION

The function of this operation is to read the contents of the status register with correct parity, to provide information as to the occurrence of any of the six different kinds of errors indicated above. Therefore, this operation is performed periodically to check for error conditions.

Referring now to FIG. 22b2, after address selection is performing during TA time and the command byte is loaded into the command register during TC time, the AND invert circuit 242 decodes the READ BS command code and produces a negative signal which is applied to one input of the OR invert circuit 246. At TC END time, a positive signal on the TC END line is applied to the inverter 244 where it is inverted to a negative signal and applied to the other input of the OR invert circuit 246 which thereby causes the OR invert circuit 246 to apply a positive signal to the READ BS line. The positive signal on the READ BS line is applied to one input of the AND invert circuits 956 in FIG.

22i2, the other inputs of which are connected to the bit latches 954 of the status register 952. Accordingly, a pattern of bit signals, corresponding to the setting of the latches 954 of the status register, are applied to the -DATA BUS IN and to the parity generator 914. It should be noted that the status bits 4, 6 and 7 are not implemented and, therefore, are treated as 0 bits in the parity generator 914 to produce the correct parity bit on the -P line of the -DATA BUS IN. The setting of the status register 952, now present on the -DATA BUS IN, remains stable until the end of this I/O operation when the command register is reset and the positive signal on the READ BS line is terminated.

SET/RESET BASIC STATUS COMMAND OPERATION

These commands are used for diagnostic purposes for testing the operation of the status register 952. Thus, in the case of the SET BS command, if the data fields associated with the command has good parity, then the status latches 954 that correspond to 1's in the data field associated with the command are set to 1's whereas in the case of the RESET BS command, if the data field associated with the command has good parity, then the status latches 954 that correspond to 1's in the data fields associated with the command are set to 0's. If a parity error is detected during the execution of either of these commands a write error signal will be produced, in a manner previously described, to set the bit 3 status latch 954D of the status register 952 to indicate the occurrence of this error. After execution of either of these commands, a READ BS command may be issued to read the content of the status register 952 in a manner described above, for subsequent determination as to whether a previously defined value written by either the SET BS or RESET BS commands is identical to that read by the READ BS command.

Referring now to FIGS. 22a2 and 22b2, after the address selection is performed during TA time and the command bit is loaded into the command register during the TC time, the AND invert circuit 232 decodes the SET BS command while the AND invert circuit 238 decodes the RST BS command. The AND invert circuit 232 causes a negative signal to be applied to one input of the OR invert circuit 236 while the AND invert circuit 238 causes the negative signal to be applied to one input of the OR invert circuit 240. At TD time, the data field to be loaded into the status register is received via the -DATA BUS OUT and applied via the inverters 170 to the parity generator 178 to generate a parity bit which is compared with the parity bit received from the -DATA BUS OUT. If the parity bits do not compare then, at TD SEL time the AND invert circuit 362 in FIG. 22b3 will detect the bad parity to apply a negative signal to turn on the WR ERR latch 364 which, in being turned on, applies a positive signal to the AND invert circuit 944 in FIG. 22i2 which is conditioned by positive signal on the -RST line to cause a negative signal to be applied to set the bit 3 latch 954D of the status register 952 indicating the occurrence of the write error. Referring back to FIG. 22b2, if the parity is bad then a negative signal is maintained on the parity good line to decondition the AND invert circuit 234 causing a positive signal to be applied to the OR invert circuits 236 and 240 which, in turn, maintain negative signals on the SET BS or RST BS lines to inhibit execution of either of these commands. On the other hand if

good parity is detected, then a positive signal is applied to the AND invert circuit 234 causing a negative signal to be applied to the other inputs of the OR invert circuits 236 and 240. Accordingly, depending on which command is being called for, a positive signal is applied to either the SET BS or RST BS lines. Referring now to FIGS. 22h4 and 22i2, if the command being executed is the SET BS command, then a positive signal is applied to condition the AND invert circuits 924, 928, 934, 942 and 948. Therefore, those bits of the data field which correspond to 1's render these AND invert circuits effective to apply negative signals to set corresponding ones of the latches of the status register 952. On the other hand, if the command being executed is the RESET BS command, then a positive signal on the RESET BS line is applied to condition the AND invert circuits 926, 932, 940, 946 and 950. Therefore, those bits of the data field which correspond to 1's render these AND invert circuits effective to apply negative signals to reset corresponding ones of the latches of the status register 952.

While the invention has been particularly shown and described with reference to the preferred embodiment thereof, it will be understood by those skilled in the art that several changes in form and detail may be made without departing from the spirit and scope of the invention.

What is claimed is:

1. A data security device having a dual master key arrangement in which a first master key provides protection for data encrypting keys and a second master key provides protection for key encrypting keys, said arrangement for protecting said key encrypting keys, comprising:
 - working key storage means,
 - means storing said second master key in said working key storage means as a working key,
 - means providing input data representing a key encrypting key, and
 - cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing said key encrypting key enciphered under said second master key.
2. A data security device as defined in claim 1 wherein said first master key is a multi-bit master key and said second master key is a multi-bit variant of said first master key.
3. A data security device as defined in claim 2 wherein said storing means includes means inverting predetermined ones of said multi-bits of said first master key to obtain said second master key as a multi-bit variant of said first master key.
4. A data security device for performing a cryptographic operation comprising:
 - key storage means storing a first master key,
 - working key storage means,
 - means causing a variant of said first master key to be transferred from said key storage means as a second master key to said working key storage means as a working key,
 - means providing input data representing a key encrypting key,
 - cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing said key encrypting key enciphered under said second master key.
5. A data security device for performing a cryptographic operation comprising:

- working key storage means,
- means storing a key encrypting key in said working key storage means as a working key,
- means including a non-resettable counter providing a count value as input data,
- cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing a random number.
- 6. A data security device for performing a cryptographic operation comprising:
 - key storage means storing a multi-bit key encrypting key,
 - working key storage means,
 - means causing a variant of said key encrypting key to be transferred from said key storage means to said working key storage means as a working key,
 - means providing input data,
 - cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing a random number.
- 7. A data security device as defined in claim 6 wherein said transfer means includes means inverting predetermined ones of said multi-bits of said key encrypting key to obtain said variant of said key encrypting key.
- 8. A data security device having a dual master key arrangement in which a first master key provides protection for data encrypting keys and a second master key provides protection for key encrypting keys, said data security device performing a cryptographic transformation operation comprising:
 - working key storage means,
 - means storing said second master key in said working key storage means as a working key,
 - input means providing first enciphered data representing a key encrypting key enciphered under said second master key,
 - cipher means operable in a first cipher function to decipher said first enciphered data under control of said working key to obtain said key encrypting key in clear form,
 - said input means providing second enciphered data representing an operational key enciphered under said first master key,
 - means storing said first master key in said working key storage means to replace said second master key as the present working key,
 - said cipher means operable in a second cipher function to decipher said second enciphered data under control of said present working key storage means to obtain said operational key in clear form, and
 - means causing said key encrypting key in clear form to be transferred from said cipher means to said working key storage means to replace said first master key as the now present working key,
 - said cipher means operable in a third cipher function to encipher said operational key under control of said now present working key to obtain ciphertext representing said operational key enciphered under said key encrypting key.
- 9. A data security device for performing a cryptographic operation comprising:
 - key storage means storing a first master key,
 - working key storage means,
 - means causing a variant of said first master key to be transferred from said key storage means as a second master key to said working key storage means as a working key,

input means providing first enciphered data representing a key encrypting key enciphered under said second master key,
 cipher means operable in a first cipher function to decipher said first enciphered data under control of said working key to obtain said key encrypting key in clear form,
 said input means providing second enciphered data representing an operational key enciphered under said first master key,
 means causing said first master key to be transferred from said key storage means to said working key storage means to replace said second master key as the present working key,
 said cipher means operable in a second cipher function to decipher said second enciphered data under control of said present working key to obtain said operational key in clear form, and
 means causing said key encrypting key in clear form to be transferred from said cipher means to said working key storage means to replace said first master key as the now present working key,
 said cipher means operable in a third cipher function to encipher said operational key under control of said now present working key to obtain ciphertext representing said operational key enciphered under said key encrypting key.

10. A data security device for performing a cryptographic operation comprising:
 key storage means storing a key encrypting key,
 working key storage means,
 means causing said key encrypting key to be transferred from said key storage means to said working key storage means as a working key,
 data storage means,
 input control means controlling the writing of input data representing an operational key into said data storage means,
 cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing said operational key enciphered under said key encrypting key for storage in said data storage means, and
 output control means controlling the reading of said ciphertext from said data storage means to a utilization device.

11. A data security device having a dual master key arrangement in which a first master key provides protection for data encrypting keys and a second master key provides protection for key encrypting keys, said arrangement for protecting said key encrypting keys comprising:
 working key storage means,
 means storing said second master key in said working key storage means as a working key,
 data storage means,
 input control means controlling the writing of input data representing a key encrypting key into said data storage means,
 cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing said key encrypting key enciphered under said second master key for storage in said data storage means, and
 output control means controlling the reading of said ciphertext from said data storage means to a utilization device.

12. A data security device for performing a cryptographic operation comprising:
 key storage means storing a first master key,
 working key storage means,
 means causing a variant of said first master key to be transferred from said key storage means as a second master key to said working key storage means as a working key,
 data storage means,
 input control means controlling the writing of input data representing a key encrypting key into said data storage means,
 cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing said key encrypting key enciphered under said second master key for storage in said data storage means, and
 output control means controlling the reading of said ciphertext from said data storage means to a utilization device.

13. A data security device for performing a cryptographic operation comprising:
 working key storage means,
 means storing a key encrypting key in said working key storage means as a working key,
 data storage means,
 input control means controlling the writing of input data into said data storage means,
 cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing a random number for storage in said data storage means, and
 output control means controlling the reading of said ciphertext from said data storage means to a utilization device.

14. A data security device as defined in claim 13 wherein said input control means includes a non-resettable counter providing a count value as said input data.

15. A data security device for performing a cryptographic operation comprising:
 key storage means storing a key encrypting key,
 working key storage means,
 means causing a variant of said key encrypting key to be transferred from said key storage means to said working key storage means as a working key,
 data storage means,
 input control means controlling the writing of input data into said data storage means,
 cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing a random number for storage in said data storage means, and
 output control means controlling the reading of said ciphertext from said data storage means to a utilization device.

16. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device for generating a terminal key encrypting key for said communication terminal comprising:
 working key storage means,
 means storing a host key encrypting key in said working key storage means,
 means including a non-resettable counter providing a count value as input data, and
 cipher means operable in a cipher function to encipher said input data under control of said host key

encrypting key to obtain ciphertext representing said terminal key encrypting key for said terminal.

17. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device for generating a terminal key encrypting key for said communication terminal comprising:

key storage means storing a host key encrypting key,

working key storage means,

means causing a variant of said host key encrypting key to be transferred from said master key storage means to said working key storage means,

means providing a random number, and

cipher means operable in a cipher function to encipher said random number under control of said variant of said host key encrypting key to obtain ciphertext representing said terminal key encrypting key for said terminal.

18. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device having a dual master key arrangement in which a first master key provides protection for data encrypting keys and a second master key provides protection for terminal key encrypting keys, said arrangement for protecting terminal key encrypting keys comprising:

working key storage means,

means storing said second master key in said working key storage means as a working key,

means providing input data representing said terminal key encrypting key, and

cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing said terminal key encrypting key enciphered under said second master key.

19. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device for protecting a terminal key encrypting key for said terminal comprising:

key storage means storing a first host master key,

working key storage means,

means causing a variant of said first host master key to be transferred from said key storage means as a second host master key to said working key storage means as a working key,

means providing input data representing said terminal key encrypting key, and

cipher means operable to encipher said input data under control of said working key to obtain ciphertext representing said terminal key encrypting key enciphered under said second host master key.

20. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device for generating a different session key in protected form for each communication session to be established between said host system and said terminal comprising:

working key storage means,

means storing a host key encrypting key in said working key storage means,

means including a non-resettable counter providing a different count value as input data for each communication session to be established,

cipher means operable to encipher each said input data under control of said host key encrypting key to obtain different ciphertext each representing a different session key enciphered under a host master key for each communication session.

21. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device for generating a different session key for each communication session to be established between said host system and said terminal comprising:

key storage means storing a host key encrypting key,

working key storage means,

means causing a variant of said host key encrypting key to be transferred from said key storage means to said working key storage means,

means providing a different random number for each communication session to be established,

cipher means operable to encipher each said random number under control of said variant of said host key encrypting key to obtain different ciphertext each defining a different session key as being enciphered under said host key encrypting key for each communication session.

22. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device having a dual master key arrangement in which a first master key provides protection for data encrypting keys and a second master key provides protection for terminal key encrypting keys, said host data security device performing a cryptographic transformation function for reenciphering a data encrypting session key for a communication session from encipherment under a host key encrypting key to encipherment under a terminal key encrypting key of said terminal comprising:

working key storage means,

means storing said second master key in said working key storage means as a working key,

input means providing first enciphered data representing said terminal key encrypting key enciphered under said second master key,

cipher means operable in a first cipher function to decipher said first enciphered data under control of said working key to obtain said terminal key encrypting key in clear form,

said input means providing second enciphered data representing said session key enciphered under said first master key,

means storing said first master key in said working key storage means to replace said second master key as the present working key,

said cipher means operable in a second cipher function to decipher said second enciphered data under control of said present working key to obtain said session key in clear form, and

means causing said terminal key encrypting key in clear form to be transferred from said cipher means to said working key storage means to replace said first master key as the now present working key,

said cipher means operable in a third cipher function to encipher said session key under control of said now present working key to obtain ciphertext representing said session key enciphered under said terminal key encrypting key for transmission to said terminal.

23. In a data communication network providing communication security for data communications sessions between a host system and a communication terminal, a host data security device for reenciphering a session key for a communication session from encipherment under a host key encrypting key to encipherment under a terminal key encrypting key of said terminal comprising:

key storage means storing a host key encrypting key, working key storage means, means causing a variant of said host key encrypting key to be transferred from said key storage means to said working key storage means as a working key,

input means providing first enciphered data representing said terminal key encrypting key enciphered under said variant of said host key encrypting key,

cipher means operable in a first cipher function to decipher said first enciphered data under control of said working key to obtain said terminal key encrypting key in clear form,

said input means providing second enciphered data representing said session key enciphered under said host key encrypting key,

means causing said host key encrypting key to be transferred from said key storage means to said working key storage means to replace said variant of said host key encrypting key as the present working key,

said cipher means operable in a second cipher function to decipher said second enciphered data under control of said present working key to obtain said session key in clear form, and

means causing said terminal key encrypting key in clear form to be transferred from said cipher means to said working key storage means to replace said host key encrypting key as the now present working key,

said cipher means operable in a third cipher function to encipher said session key under control of said now present working key to obtain ciphertext representing said session key enciphered under said terminal key encrypting key for transmission to said terminal.

24. In a data communication network providing communication security for data communication sessions between a host system and a communication terminal, a host data security device providing a session key for cryptographic operations with said terminal comprising:

master key storage means storing a host master key, working key storage means, means causing said host master key to be transferred from said master key storage means to said working key storage means as a working key,

input means providing input data representing a session key enciphered under said host master key, cipher means for performing cipher functions,

decipher key control means causing said cipher means to decipher said input data under control of said working key to obtain data representing said session key in clear form, and

means causing said data representing said session key in clear form to be transferred to said working key storage means as the present working key for subsequent cryptographic operations with said terminal.

25. In a data communication network as defined in claim 24 for further providing host ciphertext for transmission to said terminal wherein said input means provides host plaintext, and further comprising:

encipher control means causing said cipher means to encipher said host plaintext under control of said present working key to obtain host ciphertext representing host plaintext enciphered under said session key for transmission to said terminal.

26. In a data communication network as defined in claim 24 for further deciphering terminal ciphertext received at said host system from said terminal wherein said input means provides said terminal ciphertext representing terminal plaintext enciphered under said session key, and further comprising:

decipher control means causing said cipher means to decipher said terminal ciphertext under control of said present working key to obtain said terminal plaintext in clear form at said host system.

27. In a data communication network providing data communication sessions between a host system having a data security device and a communication terminal having a data security device, the method of providing communication security for data communication sessions comprising the steps of:

storing a session key enciphered under a first host key encrypting key at said host system,

storing a terminal key encrypting key enciphered under a second host key encrypting key at said host system,

reenciphering said session key from encipherment under said first host key encrypting key to encipherment under said terminal key encrypting key, communicating said session key enciphered under said terminal key encrypting key as key synchronizing data to said terminal,

storing said terminal key encrypting key at said terminal,

providing said terminal key encrypting key as a terminal working key at said terminal,

providing said received key synchronizing data as input data at said terminal,

carrying out a decipher key operation at said terminal to decipher said input data under control of said terminal working key to obtain said session key in clear form, and

replacing said terminal key encrypting key with said session key as the present terminal working key at said terminal to establish a communication session between said terminal and said host system.

28. In a data communication network providing data communication sessions between a host system having a data security device and a communication terminal having a data security device, the method of providing communication security for data communication sessions comprising the steps of:

storing a session key enciphered under a host key encrypting key at said host system,

storing a terminal key encrypting key enciphered under a variant of said host key encrypting key at said host system,

reenciphering said session key from encipherment under said host key encrypting key to encipherment under said terminal key encrypting key,

communicating said session key enciphered under said terminal key encrypting key as key synchronizing data to said terminal,

storing said terminal key encrypting key at said terminal,
 providing said terminal key encrypting key as a working key at said terminal,
 providing said received key synchronizing data as input data at said terminal,
 carrying out a decipher key operation at said terminal to decipher said input data under control of said working key to obtain said session key in clear form, and
 replacing said terminal key encrypting key with said session key as the present working key at said terminal to establish a communication session between said terminal and said host system.

29. In the method as defined in claim 28 wherein said host key encrypting key is a host master key and said terminal key encrypting key is a terminal master key.

30. In the method as defined in claim 28 wherein said host key encrypting key is a host master key and said terminal key encrypting key is a private terminal master key.

31. In the method as defined in claim 27 further providing a cryptographic data communication between said terminal and said host system comprising the further steps of:

- providing terminal plaintext,
- carrying out an encipher operation at said terminal to encipher said terminal plaintext under control of said present terminal working key to obtain terminal ciphertext representing said terminal plaintext enciphered under said session key, and
- communicating said terminal ciphertext to said host system.

32. In the method as defined in claim 31 further providing a cryptographic operation to obtain said session key in clear form at said host system for subsequent cryptographic operations comprising the further steps of:

- providing said first host key encrypting key as a host working key at said host system,
- providing said session key enciphered under said first host key encrypting key as host input data,
- carrying out a decipher key operation at said host system to decipher said host input data under control of said host working key to obtain said session key in clear form, and
- replacing said first host key encrypting key with said session key as the present host working key at said host system for subsequent cryptographic operations.

33. In the method as defined in claim 32 further providing a cryptographic operation to obtain terminal plaintext in clear form at said host system comprising the further steps of:

- providing said received terminal ciphertext as present host input data at said host system, and
- carrying out a decipher operation at said host system to decipher said present host input data under control of said present host working key to obtain said terminal plaintext in clear form at said host system.

34. In the method as defined in claim 27 further providing a cryptographic operation to obtain said session key in clear form at said host system for subsequent cryptographic operations comprising the further steps of:

- providing said first host key encrypting key as a host working key at said host system,

providing said session key enciphered under said first host key encrypting key as host input data,
 carrying out a decipher key operation at said host system to decipher said host input data under control of said host working key to obtain said session key in clear form, and
 replacing said first host key encrypting key with said session key as the present host working key at said host system for subsequent cryptographic operations.

35. In the method as defined in claim 34 further providing a cryptographic data communication between said host system and said terminal comprising the further steps of:

- providing host plaintext,
- carrying out an encipher operation at said host system to encipher said host plaintext under control of said present host working key to obtain host ciphertext representing said host plaintext enciphered under said session key, and
- communicating said host ciphertext to said terminal.

36. In the method as defined in claim 35 further providing a cryptographic operation to obtain host plaintext in clear form at said terminal comprising the further steps of:

- providing said received host ciphertext as present terminal input data at said terminal, and
- carrying out a decipher operation at said terminal to decipher said present terminal input data under control of said present working key at said terminal to obtain said host plaintext in clear form at said terminal.

37. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal, the method of generating a terminal key encrypting key at said host system for said terminal comprising the steps of:

- providing a host key encrypting key,
- providing a random number, and
- carrying out an encipher operation to encipher said random number from a non-resettable counter under control of said host key encrypting key to obtain ciphertext representing said terminal key encrypting key for said terminal.

38. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal, the method of generating a terminal key encrypting key at said host system for said terminal comprising the steps of:

- storing a host key encrypting key,
- providing a variant of said host key encrypting key,
- providing a random number, and
- carrying out an encipher operation to encipher said random number under control of said variant of said host key encrypting key to obtain ciphertext representing said terminal key encrypting key for said terminal.

39. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal by a dual master key arrangement at said host system in which a first master key provides protection for data encrypting keys and a second master key provides protection for terminal key encrypting keys, the method of protecting a terminal key encrypting key at said host system comprising the steps of:

providing said second master key at said host system as a working key,
 providing said terminal key encrypting key at said host system as input data, and
 carrying out an encipher operation to encipher said input data under control of said working key to obtain said terminal key encrypting key enciphered under said second master key.

40. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal, the method of protecting a terminal key encrypting key at said host system comprising the steps of:

storing a host key encrypting key at said host system,
 providing a variant of said host key encrypting key as a working key,
 providing said terminal key encrypting key at said host system as input data, and
 carrying out an encipher operation to encipher said input data under control of said working key to obtain said terminal key encrypting key enciphered under said variant of said host key encrypting key.

41. In the method as defined in claim 40 wherein said host key encrypting key is a host master key and said terminal key encrypting key is a terminal master key.

42. In the method as defined in claim 40 wherein said host key encrypting key is a host master key and said terminal key encrypting key is a private terminal master key.

43. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal, the method of generating session keys for each communication session to be established between said host system and said terminal comprising:

providing a host key encrypting key,
 providing a different random number from a non-resettable counter for each communication session to be established,
 carrying out an encipher operation to encipher each said random number under control of said host key encrypting key to obtain different ciphertext each representing a different session key enciphered under a host master key for each communication session.

44. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal, the method of generating session keys for each communication session to be established between said host system and said terminal comprising:

storing a host key encrypting key,
 providing a variant of said host key encrypting key,
 providing a different random number for each communication session to be established,
 carrying out an encipher operation to encipher each said random number under control of said variant of said host key encrypting key to obtain different ciphertext each representing a different session key enciphered under said host key encrypting key for each communication session.

45. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal by an arrangement at said host system in which a host first key encrypting key provides protection for data encrypting keys and a host second key encrypting key provides protection for terminal key encrypting

keys, the method of performing a cryptographic transformation function for reenciphering a data encrypting session key for a communication session from encipherment under a host first key encrypting key to encipherment under a terminal key encrypting key of said terminal comprising:

providing a host second key encrypting key as a working key,
 providing first enciphered data representing said terminal key encrypting key enciphered under said host second key encrypting key,
 carrying out a first cipher function to decipher said first enciphered data under control of said working key to obtain said terminal key encrypting key in clear form,

providing second enciphered data representing said session key enciphered under said host first key encrypting key,

replacing said host second key encrypting key with said host first key encrypting key as the present working key,

carrying out a second cipher function to decipher said second enciphered data under control of said present working key to obtain said session key in clear form,

replacing said host first key encrypting key with said terminal key encrypting key as the now present working key, and

carrying out a third cipher function to encipher said session key under control of said now present working key to obtain ciphertext representing said session key enciphered under said terminal key encrypting key for transmission to said terminal.

46. In a data communication network which provides communication security for data communication sessions between a host system and a communication terminal, the method of reenciphering a session key for a communication session from encipherment under a variant of a host key encrypting key to encipherment under a terminal key encrypting key of said terminal comprising:

storing a host key encrypting key,
 providing a variant of said host key encrypting key as a working key,

providing first enciphered data representing said terminal key encrypting key enciphered under said variant of said host key encrypting key,

carrying out a first cipher function to decipher said first enciphered data under control of said working key to obtain said terminal key encrypting key in clear form,

providing second enciphered data representing said session key enciphered under said host key encrypting key,

replacing said variant of said host key encrypting key with said host key encrypting key as the present working key,

carrying out a second cipher function to decipher said second enciphered data under control of said present working key to obtain said session key in clear form,

replacing said host key encrypting key with said terminal key encrypting key as the now present working key, and

carrying out a third cipher function to encipher said session key under control of said now present working key to obtain ciphertext representing said

103

session key enciphered under said terminal key encrypting key for transmission to said terminal.

47. In a data communication network which provides communication security for a data communication session between a host system having a data security device and a communication terminal having a data security device, the method of establishing a common private session key for a private data communication session comprising the steps of:

providing a host master key as a working key at said host system,

providing said private session key enciphered under said host master key at said host system as input data,

carrying out a decipher operation at said host system to decipher said input data under control of said working key to obtain said private session key in clear form,

replacing said host master key with said private session key as the present host working key at said host system,

providing said private session key as the present terminal working key at said terminal so that a common private session key is maintained as the present working key at both said terminal and said host system for establishing a private communication session.

48. In the method as defined in claim 47 further providing a cryptographic data communication between said terminal and said host system comprising the further steps of:

104

providing terminal plaintext at said terminal as input data,

carrying out an encipher operation at said terminal to encipher said input data under control of said present terminal working key to obtain terminal ciphertext representing said terminal plaintext enciphered under said private session key,

communicating said terminal ciphertext to said host system,

providing said received terminal ciphertext as present input data at said host system, and

carrying out a decipher operation at said host system to decipher said present input data under control of said present host working key to obtain terminal plaintext in clear form at said host system.

49. In the method as defined in claim 47 further providing a cryptographic data communication between said host system and said terminal comprising the further steps of:

providing host plaintext at said host system as input data,

carrying out an encipher operation at said host system to encipher said input data under control of said present host working key to obtain host ciphertext representing said terminal plaintext enciphered under said private session key,

communicating said host ciphertext to said terminal, providing said received host ciphertext as present input data at said terminal, and

carrying out a decipher operation at said terminal to decipher said present input data under control of said present terminal working key to obtain host plaintext in clear form at said terminal.

* * * * *