CA34C168

DATA ENCRYPTION PROCESSOR

- **High speed VLSI cryptographic device for real-time or message forwarding systems**
- **Supports Public Key and conventional cryptosystems**
- **Public Key Exchange system compatible with current DES systems**
- **Block size = 593 bits**
- **One Block Cipher mode and 2 Cipher Stream modes**
- **Digital signature capability**
- **Message Authentication Code generator**
- **Command/status/profile 8-bit port**
- **Data port configurable as one 16-bit bidirectional or two 8-bit unidirectional parallel ports, or as two full duplex synchronous key stream ports**
- **I/O supported with interrupts and DMA**
- **Use in a secure conventional system with any means of key exchange**
- **TTL compatible, low power CMOS**

The CA34C168 is a versatile, very high speed data encryption device designed for the digital voice/data communications industry. Featuring facilities to complement both Public Key systems and conventional cryptosystems, the CA34C168 is intended for use in both real-time file encryption or message forwarding environments. It is also suitable for key exchange purposes in systems using the Data Encryption Standard (DES).

The CA34C168 can be programmed to work in either block or stream cipher mode (two stream cipher modes are available). In block mode, the device can be used for interactive key exchange, standalone key exchange, asymmetric key block data encryption or symmetric (conventional) key block data encryption. When used for conventional block encryption, the CA34C168 operates at rates in excess of 300Kbits/sec.

The CA34C168 is supplied in both commercial and military temperature ratings, and is manufactured using a low power CMOS process. It is ideal for use in any applications which require public key distribution, secure data communications, authentication or digital signature.

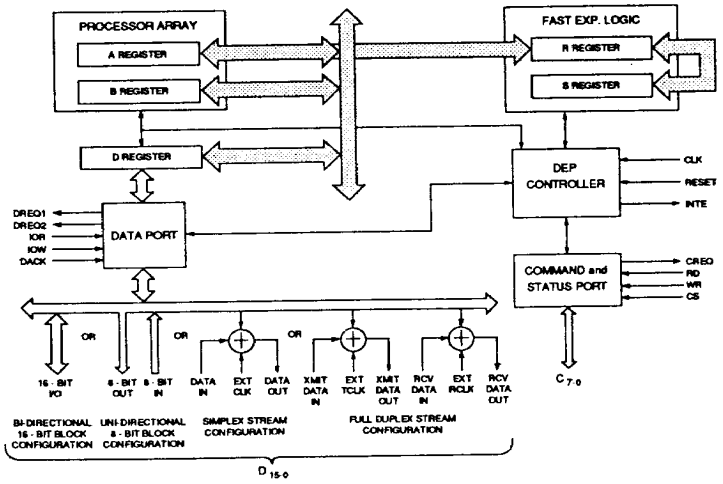


Figure 1 : CA34C168 BLOCK DIAGRAM

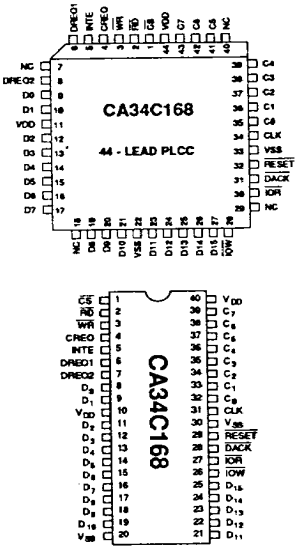


Figure 2 : PLCC and DIP PIN CONFIGURATIONS

U.S. Patent Number 4,745,586 Cryptech Systems (Canada) Inc.

Table 1 : PIN DESCRIPTIONS

Symbol	Pin	Type	Name and Function
C_{0-7}	32-39	I/O	**Command/Status Bus:** Three state, bi-directional data bus lines used to transfer commands into the device and status out of the device.
CLK	31	I	**Clock:** Master clock input (20 MHz maximum).
CREQ	4	O	**Command Request:** Output signal used to indicate command/status port readiness to accept a command.
$\overline{CS}$	1	I	**Chip Select:** A low signal to this pin enables reading and writing to the command/status port.
D_{0-15}	8, 9, 11-19, 21-25	I/O	**Data Bus:** Three-State, bi-directional data bus lines used to transfer data in and out of the device in both block and stream cipher modes. This port is user configurable as a 16 bit bi-directional port, an eight bit uni-directional port, or as a stream cipher port.
$\overline{DACK}$	28	I	**DMA Acknowledge:** Input signal from a DMA controller acknowledging that the requested DMA cycle has been granted. This signal enables the data port.
DREQ1	6	O	**DMA Request 1:** Output signal to a DMA controller requesting a DMA cycle. Indicates that the Data port is ready to receive data.
DREQ2	7	O	**DMA Request 2:** Output signal to a DMA controller requesting a DMA cycle. Indicates that the Data port is ready to transmit data.
INTE	5	O	**Interrupt Error Request:** Output signal used to indicate that the CA34C168 needs service and that an internal error has occurred.
$\overline{IOR}$	27	I	**I/O Read:** An active low signal at this pin accesses data from the data port (during a DMA write transfer).
$\overline{IOW}$	26	I	**I/O Write:** An active low signal at this pin loads data into the data port (during a DMA read transfer).
$\overline{RD}$	2	I	**Read:** An active low read strobe at this pin enables the reading of status data from the command/status port.
$\overline{RESET}$	29	I	**Reset:** A low signal to this pin resets the CA34C168.
V_{DD}	10, 40	-	**Power:** 5 V ± 10% power supply.
V_{SS}	20, 30	-	**Ground:** Pin must be tied to ground.
$\overline{WR}$	3	-	**Write:** An active low write strobe at this pin enables the writing of commands to the command/status port.

FUNCTIONAL DESCRIPTION

The basic function of the Data Encryption Processor (DEP) is to perform arithmetic in the finite field $GF(2^{593})$. The operations that are performed include, multiplication and exponentiation. In addition, the device will compute the multiplicative inverse of an element and implement several other functions required for data encryption/decryption in Block Cipher and Stream Cipher Modes.

Since elements of $GF(2^{593})$ may be represented by binary vectors of length 593, internal data is organized into 593-bit blocks. There are three main 593-bit registers labeled A, B, and D which are used to hold operands, multiply, exponentiate, store results and buffer data into and out of the chip. There are also two 256-bit registers labeled R and S for exponent representation and key storage.

An internal microcontroller executes DEP instructions, maintains device status, and controls the I/O ports. The 8-bit command/status port and 16-bit reconfigurable data port are used to communicate with microprocessors or peripheral controllers. A block diagram of the internal structure is shown in Figure 1.

The DEP can be in one of three states depending on the instruction issued. After the completion of any instruction, the DEP goes into an Idle State waiting for a new command. During the execution of a command, the DEP goes into a Busy or Processing State, and while executing an instruction involving data I/O, the device will go into a Wait State requesting data I/O transfer. Figure 3 illustrates the three possible states of the DEP.

3

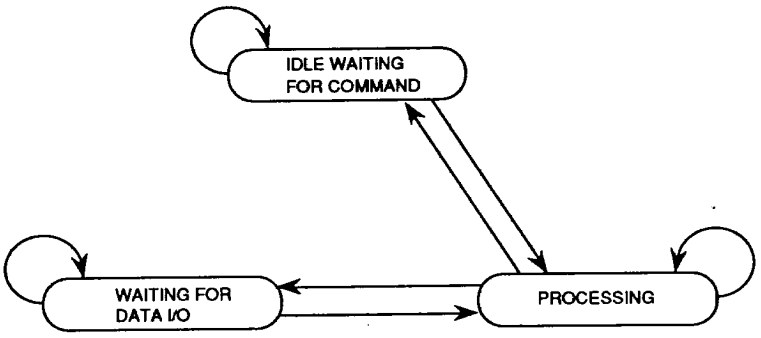


Figure 3 : DEP STATE DIAGRAM

Table 2 : AC CHARACTERISTICS, COMMAND/STATUS PORT (T_A = 0 to 70 °C, V_{DD} = 5V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Limits		Units
		Min	Max	
Read Cycle				
t_{CR}	$\overline{CS}$ ↓ to $\overline{RD}$ ↑	50		ns
t_{RC}	$\overline{CS}$ hold after $\overline{RD}$ ↑	0		ns
t_{RDF}	$\overline{RD}$ ↑ to data float delay		30	ns
t_{RDV}	$\overline{RD}$ ↓ to data out delay		40	ns
t_{RR}	$\overline{RD}$ pulse width	50		ns
t_{RIE}	(INTE) Interrupt error request to RD ↓		40	ns
Write Cycle				
t_{CW}	$\overline{CS}$ ↓ to $\overline{WR}$ ↓	0		ns
t_{DW}	Data setup to $\overline{WR}$ ↑	50		ns
t_{WC}	$\overline{CS}$ hold after $\overline{WR}$ ↑	0		ns
t_{WCR}	(CREQ) Command request low from $\overline{WR}$ ↓		40	ns
t_{WD}	Data hold after $\overline{WR}$ ↑	0		ns
t_{WW}	$\overline{WR}$ pulse width	50		ns

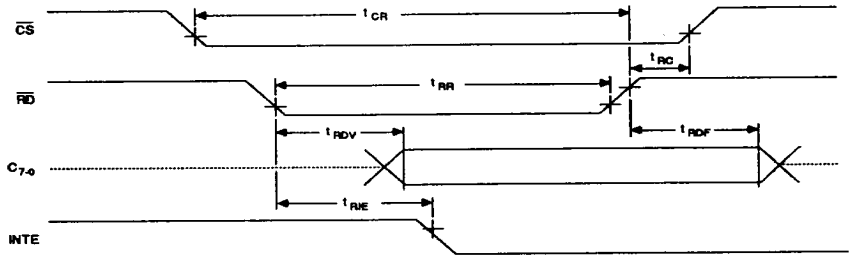
Table 3 : AC CHARACTERISTICS, CLOCK PARAMETERS (T_A = 0 to 70 °C, V_{DD} = 5V ± 10%, V_{SS} = 0V)

Symbol	Parameter	CA34C168-10 10 MHz Limits		CA34C168-12 12 MHz Limits		CA34C168-16 16 MHz Limits		CA34C168-20 20 MHz Limits		Units
		Min	Max	Min	Max	Min	Max	Min	Max	
t_{PWH}	High pulse width	40		33		25		20		ns
t_{PWL}	Low pulse width	40		33		25		20		ns
t_{CLK}	Clock period	100	Note 1	82.5	Note 1	62.5	Note 1	50	Note 1	ns
t_R , t_F	Clock rise and fall time	0	15	0	15	0	15	0	15	ns
th_{MAX}	Maximum attainable throughput	150		180		240		300		Kbps

Note: 1. Minimum frequency is 100 KHz during arithmetic operations only. The contents of all registers are fully static.

FIGURE 4 : TIMING DIAGRAMS, COMMAND/STATUS PORT

a) Read Cycle



b) Write Cycle

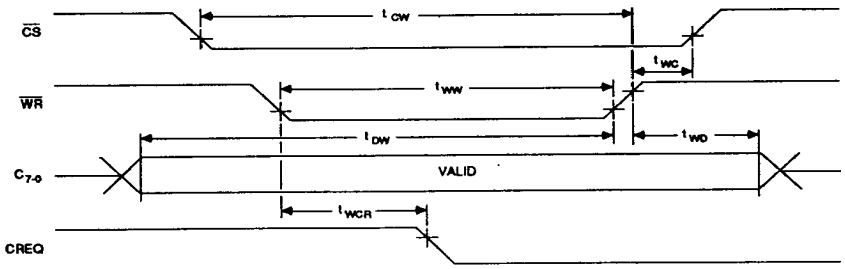


Figure 5 : CLOCK PARAMETERS

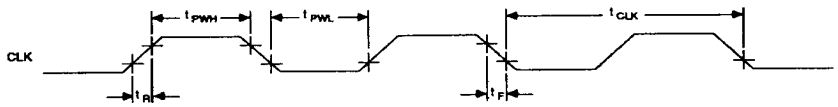


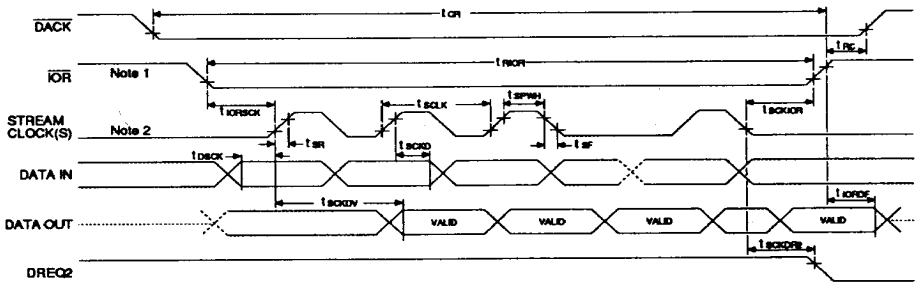
Table 4 : AC CHARACTERISTICS, DATA PORT (T_A = 0 to 70 °C, V_{DD} = 5V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Limits		Units
		Min	Max	
Read Cycle (Stream Modes)				
t_{CR}	$\overline{DACK}$ ↓ to $\overline{IOR}$ ↑	Note 1		ns
t_{DSCK}	Data setup to stream clock ↑	50		ns
t_{IORDF}	$\overline{IOR}$ ↑ to data float		30	ns
t_{IORSCK}	First clock issue from $\overline{IOR}$ ↓	50		ns
t_{RC}	$\overline{DACK}$ hold after $\overline{IOR}$ ↑	0		ns
t_{RIOR}	Read pulse width	Note 1		ns
t_{SCLK}	Stream clock cycle	100		ns
t_{SCKD}	Data hold after stream clock ↓	0		ns
t_{SCKDR2}	(DREQ2) Data request low from final stream clock low		40	ns
t_{SCKDV}	Data valid from stream clock ↑		70	ns
t_{SCKIOR}	Stream clock ↓ to $\overline{IOR}$ ↑	50		ns
t_{SPWH}	Stream clock high pulse width	25		ns
t_{SR}, t_{SF}	Stream clock rise and fall time	0	15	ns
Read Cycle (Block Modes)				
t_{CR}	$\overline{DACK}$ ↓ to $\overline{IOR}$ ↑	50		ns
t_{IORDF}	$\overline{IOR}$ ↑ to data float		30	ns
t_{IORDV}	$\overline{IOR}$ ↓ to data valid out		40	ns
t_{RC}	$\overline{DACK}$ hold after $\overline{IOR}$ ↑	0		ns
t_{RDR2}	(DREQ2) Data request low from $\overline{IOR}$↓		40	ns
t_{RIOR}	$\overline{IOR}$ pulse width	50		ns
Write Cycle				
t_{ACW}	$\overline{DACK}$ ↓ to $\overline{IOW}$ ↑	50		ns
t_{DIOW}	Data setup to $\overline{IOW}$ ↑	50		ns
t_{IOWD}	Data hold after $\overline{IOW}$ ↑	0		ns
t_{WAC}	$\overline{DACK}$ hold after $\overline{IOW}$ ↑	0		ns
t_{WDR1}	(DREQ1) Data request low from $\overline{IOW}$↓		40	ns
t_{WIOW}	$\overline{IOW}$ pulse width	50		ns

Note: 1. IOR must be low during the stream operation.

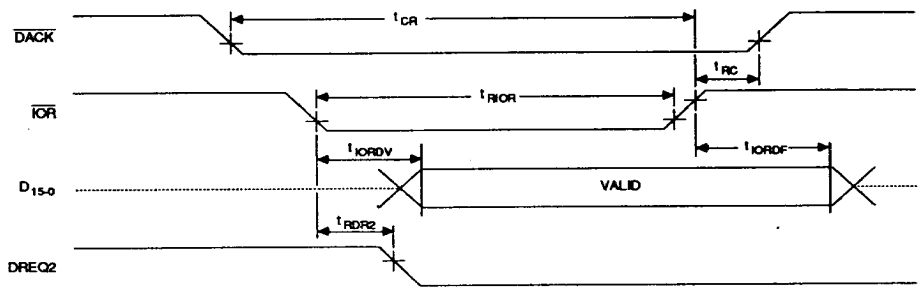
Figure 6 : TIMING DIAGRAMS, DATA PORT

a) Read Cycle (Stream Modes)

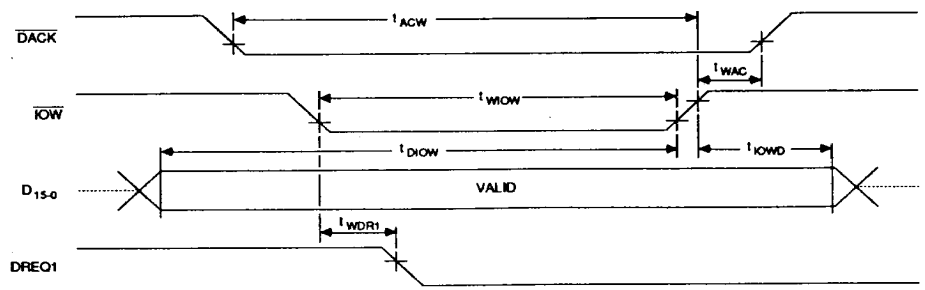


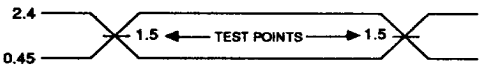
Notes : 1. When IOR is high, the stream clock is masked and will not affect the data output.
2. Stream clock must be low 50 ns before the falling edge of IOR.

b) Read Cycle (Block Modes)



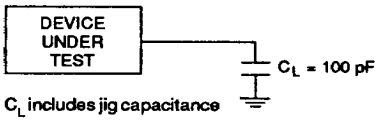
c) Write Cycle





A.C. Testing Inputs are driven at 2.4V for a Logic 1 and 0.45V for a Logic 0. Timing measurements are made at 1.5V for a logic 1 and 1.5V for a Logic 0.

Figure 7: AC TESTING I/O WAVEFORM



C_L includes jig capacitance

Figure 8: AC TESTING LOAD CIRCUIT

Table 5 : DC CHARACTERISTICS (T_A = 0 to 70 °C, V_{DD} = 5V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Test Conditions	Limits		Units
			Min	Max	
I_{LIH}	Input leakage current high	$V_{IN} = V_{DD}$		10	µA
I_{LIL}	Input leakage current low	V_{IN} = 0V		–10	µA
I_{LIR}	Input leakage on Reset pin 29	V_{IN} = 0V		–100	µA
I_{LOH}	Output leakage current high	$V_{OUT} = V_{DD}$		10	µA
I_{LOL}	Output leakage current low	V_{OUT} = 0V	0	–10	µA
V_{IH}	Input voltage high		2.0	V_{DD}+0.3	V
V_{IL}	Input voltage low		–0.5	0.8	V
V_{OH}	Output voltage high	I_{OH} = -400 µA	2.4		V
V_{OL}	Output voltage low	I_{OL} = 2.5 mA		0.4	V
	Supply current operating	Clock freq. = 20 MHz		60	mA
	Supply current standby (Note 1)	Clock freq. = 20 MHz		15	mA

Note: 1. Processor Idle waiting for command

Table 6 : CAPACITANCE (T_A = 25 °C , V_{DD} = 5V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Test Conditions	Limits		Units
			Min	Max	
C_{IN}	Input capacitance	Unmeasured pins		10	pF
C_{OUT}	I/O Capacitance	Returned to V_{SS}		20	pF

Table 7 : RECOMMENDED OPERATING CONDITIONS

DC Supply Voltage		+4V to +6V
Operating Temperature Range	Commercial	0° to 70°C
	Industrial	–40° to +85°C

Table 8 : ABSOLUTE MAXIMUM RATINGS

Power Supply Voltage (V_{DD})	–0.5V to +7.0V
Power Dissipation (PD_{MAX})	1 Watt
Operating Temperature (T_{OPT})	0° to 70°C
Storage Temperature (T_{STG})	–65° TO +150°C

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

PORT DESCRIPTIONS

Command/Status Port

The Command/Status port is an 8-bit wide bi-directional port (C_{7-0}). This port is used to set the DEP mode of operation, write commands and read DEP status. This port is addressed as shown in Table 9.

The DEP's Status Register can be read at any time. However, in order to write instructions, the Command Input Buffer must be empty. Status of the Command Input Buffer can be determined by reading the Status Register's Command Buffer Full (CBF) bit or by examining the level of the Command Request (CREQ) pin. If CBF is low or CREQ is high, the Command Input Buffer is empty, and the next command can be written.

Table 9 : COMMAND/STATUS REGISTER ACCESS

CREQ	$\overline{RD}$	$\overline{WR}$	$\overline{CS}$	REGISTER
1	1	0	0	Command Input Buffer
X	0	1	0	Status Output Buffer
X	X	X	1	Don't Care

Data Port

The data port is a reconfigurable 16-bit port (D_{15-0}) used for data transfer (key data, plain text data, or cipher text data) into and out of the DEP. This port is addressed as shown in Table 10.

In order to read this port, the Data Output Buffer must be full. Its status can be determined by reading the Status Register's Output Buffer Full (OBF) bit or by examining the level of the Data Request 2 (DREQ2) pin. If OBF or DREQ2 is high, the Data Output Buffer is full, and data can be read from the port. Similarly, in order to write data to this port, the Data Input Buffer must be empty. Status of the Data Input Buffer can be determined by reading the Status Register's Input Buffer Full (IBF) bit or by examining the level of the Data Request (DREQ1) pin. If IBF is low or DREQ1 is high, the Data Input Buffer is empty, and data can be written to the port.

The Data Port can be configured as a 16-bit bi-directional port, an 8-bit uni-directional port or in one of two stream cipher port configurations. All port configurations are set in the Mode Register via the SETMODE command. Table 11 describes the Data Port bit assignments for the DEP's Block Cipher and Stream Cipher Modes of operation.

Bit assignments for Stream Modes in Table 11 pertain to data output commands (CPDO, CPA2DO or STRM macros). The data input command, LOADD, will request data to load the D Register in an 8 or 16-bit block configuration. This allows the user to load the D Register from one of two standard buses while in stream mode. The allowable input/output bus configurations are described in the Register Section under the Mode Register.

Table 10 : DATA BUFFER ACCESS

DREQ1	DREQ2	$\overline{IOW}$	$\overline{IOR}$	$\overline{DACK}$	REGISTER
1	X	0	1	0	Data Input Buffer
X	1	1	0	0	Data Output Buffer
X	X	X	X	1	Don't Care

Table 11 : DATA PORT BITS FOR BLOCK CIPHER AND STREAM CIPHER MODES

8 Bit Uni-directional Block Configuration (default)	D_{15-8}	Uni-directional data out
	D_{7-0}	Uni-directional data in
16 Bit Bi-directional Block Configuration	D_{15-0}	Bi-directional data
Simplex Stream Configuration	D_0	Tx data in
(Configurations of port on read cycle only)	D_1	Tx data out
	D_2	Tx clk in
	D_{15-3}	Hi-impedance
Synchronous Full Duplex Stream Configuration	D_0	Tx data in
(Configurations of port on read cycle only)	D_1	Tx data out
	D_2	Tx clk in
	D_3	Rx data in
	D_4	Rx data out
	D_5	Rx clk in
	D_{15-6}	Hi-impedance

REGISTERS

The following registers can be accessed in all modes of operation:

Program Control	Command Input Buffer	(write only)
	Status Output Buffer	(read only)
	Mode Register	(write only)
	Permute Loop Count Register	(write only)
	Data Input Buffer	(write only)
	Data output Buffer	(read only)
Arithmetic	A Register	(read/write)
	B Register	(read/write)
	D Register	(read/write)
	R Register	(write only)
	S Register	(write only)

Command Input Buffer

Data written to the 8-bit Command Input Buffer is interpreted as instructions or operands to instructions. For example, the SETMODE command requires a one-byte operand which changes the DEP's mode of operation. See the Programming Section for details of all DEP instructions.

Status output Buffer

The 8-bit Status Register will give the following DEP summary: mode of operation (Block or Stream), processing status (Busy or Idle), internal error status (Multiply or Exponentiation Error), command buffer status (Empty or Full), and data buffer status (Empty or Full). See Figure 9.

The Block/Stream Mode bit (BSM) indicates whether the device is in Block Mode (logic "1") or Stream Mode (logic "0").

The Busy/Idle bit (B/I) when set to "1" indicates that the DEP is busy executing an instruction. Zero means that the DEP is idle waiting for an instruction. This flag will go into an Idle state (logic "0") after all commands have been processed.

The Multiply Error bit (MTE) is set to "1" whenever a multiply (MULT) is issued where either of the operands (Registers A or B) has the value zero or all ones. In other words, any attempt to multiply by zero or all ones will cause a multiply error. The Interrupt pin (INTE) will go high when an error occurs. Both the MTE status bit and INTE will be cleared automatically after the Status Register has been read. Multiplication will not proceed if this is the case, and the contents of registers A and B will remain unchanged.

The exponentiate error bit (EPE) is set to "1" whenever an exponent register (Register D or R) is loaded with zero or all ones. That is, attempting to exponentiate with zero or all ones as the exponent will cause an exponentiation error. The Interrupt pin (INTE) will go high when an error occurs. Both the EPE status bit and INTE will be cleared automatically after the status register has been read.

Note that as soon as an error has been detected processing stops and the INTE pin is set to "1" indicating an error has occurred (MTE and/or EPE). The Status Register must be read to determine the type of error which has occurred, and to clear the appropriate error flags.

The Completion Flag bit (CF) is an active low signal used to indicate the completion of data transfers into and out of the DEP. In 8-Bit Block Mode, the CF bit will go low for the 75 byte transfer. In 16-Bit Block Mode, the CF bit will go low for the 37 16-bit word transfer. This signal may be used to flag a CPU or a DMA controller at the end of a data transfer.

The Command Buffer Full bit (CBF) when set to "1" indicates that a command has been written. When the DEP has accepted a new command, it clears the Command Input Buffer so that a new command can be written while the current command is being processed. In interrupt driven systems, the active high Command Request pin (CREQ) can be used to indicate that the Command Buffer is empty, and that the next command can be written.

The Output Buffer Full bit (OBF) when set to "1" indicates that the Data Output Buffer is full waiting for the processor to read the buffer. In interrupt driven systems, the active high Data Request 2 pin (DREQ2) can be used to indicate that the Output Buffer is full, and that it can be read.

The Input Buffer Full bit (IBF) when set to "1" indicates that data has been written to the Data Input Buffer. The DEP will clear this bit when it has accepted the data so that the next byte or word can be written. In interrupt driven systems, the active high Data Request 1 pin (DREQ1) can be used to indicate that the Data Input Buffer is empty, and that data can be written to it.

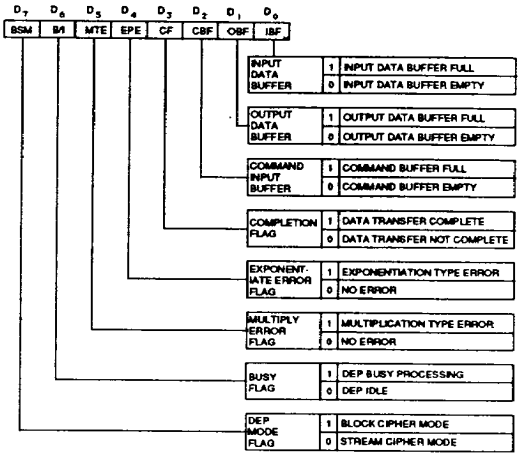


Figure 9: STATUS REGISTER

Mode Register

The Mode Register configures the Data Port, sets the device in Block or Stream Mode, and masks or enables Interrupts. The Mode Register is configured with the operand of the SETMODE command. See Figure 9 for the Mode Register bit assignments.

Data Buffer Control bit 1 (DBC_1) configures the Data Port in Block or Stream Mode. This control bit is used in conjunction with DBC2 and DBC0 to completely specify the bus configuration.

Data Buffer Control bits 2 and 0 (DBC_2 and DBC_0) specify the configuration for the Data Input Buffer and Data Output Buffer respectively. Loading data into the D Register, for all modes of operation, can only be performed in the 8 or 16-bit Block configuration. This is done so that the D Register can be loaded from a system bus while in one of the Stream Modes. Reading data from the D Register can be performed in any one of the four bus configurations. After a reset, DBC_{2-0} will be in a low state (8-Bit In, Block Mode, 8-Bit Out). The combinations of DBC_{2-0} are shown in Figure 10.

The least significant nibble of the Mode Register is used to selectively enable and disable output interrupts. Upon reset, all interrupts are enabled (bits set to "1"). The interrupts include INTE, DREQ2, DREQ1 and CREQ. Writing a zero to any one of these bits disables the interrupt.

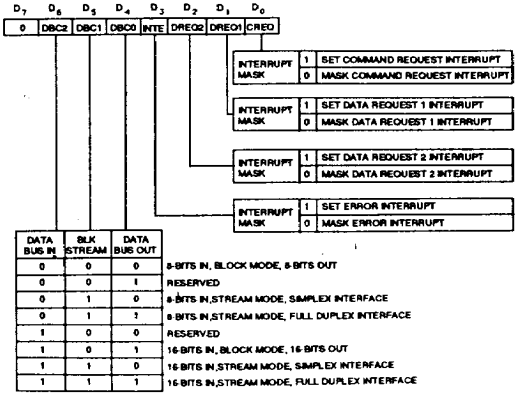


Figure 10: MODE REGISTER ASSIGNMENTS

Permute Loop Count Register

The Permute Loop Count (PLC) Register contains the number of R Register permutations which will be performed on the command PERMR. This Register can be loaded via the LOADPLC command where the operand specifies the number of permutations. After a reset, the PLC Register will have the value one, indicating one permutation of R when PERMR is issued. IF the PLC Register is loaded with hex "FF", then 255 permutations of R are performed on a PERMR command, and the value "0" would perform 256 permutations on the R Register. The value of the PLC Register will only change on a reset (hard or soft), a SETMODE, or LOADPLC command. PERMR does not change the PLC Register.

Data Input Buffer

Data written to this register may be key data, plain text data, or cipher text data. To use this register, the LOADD command must be issued. The opcode for this command is written to the Command port and data is written to the Data Port.

The D Register is the only register which can be loaded via the Data Input Buffer, and since the D Register is 593 bits long, the data transfer for LOADD is either 75 bytes or 38 16–bit words, depending on the port configuration used. Data is always loaded most significant bit first. For example, in 16–bit input mode, on the first 16–bits of data written, D<15> is bit 592 of the D Register, and the last 15 bits of the 38th word are ignored (37 words plus one bit is 593). Similarly, in 8–bit input mode, the last 7 bits of the last byte (75th byte) written are ignored. The interface can be interrupt driven (using the DREQ1 pin) or poll driven (using the IBF bit in the Status Register). The Interface Protocol Section describes the control and timing information required to use this command.

Data Output Buffer

The Data Output Buffer is used to transfer data from the D Register to the Data port in various port configurations as defined by the Mode Register.

In Block Mode, the full 593-bit D Register is read in the 8 or 16-bit output mode. Reading data from this buffer is, as the input buffer, most significant byte or word first. In 8–bit output mode, 75-bytes of data are read where the least significant 7 bits of the last byte can be ignored. In 16-bit output mode, 38-words of data are read where the least significant 15 bits of the last word can be ignored. The interface can be interrupt driven (using the DREQ2 pin) or poll driven (using the OBF bit in the Status Register). The Interface Protocol Section describes the control and timing information required to use commands which read from this buffer. Those commands include "copy D out" (CPDO), "copy A to D out" (CPA2DO), and the message block (BLK) macro instruction.

In Stream Cipher Modes, the D Register becomes the source of a serial key stream used to exclusive-or with a serial data stream for encrypting and decrypting data. The two different types of Stream Cipher Modes available are Simplex Stream and Synchronous Full Duplex Mode.

In Simplex Stream Mode, communication is only one way, and all 593 bits of D are used as the key stream. In this mode, bit D_1 of the Data Port becomes the output stream, bit D_0 is data into the exclusive-or function, and D_2 is clock input to shift data out as required. The port configuration and connection to the D Register is illustrated in Figure11.

In Synchronous Full Duplex Mode, the D Register is divided into 74 8-bit segments where 37 are allocated for one direction (transmit), and 37 are allocated for the other (receive). Key stream data is extracted serially in an 8-bit interleaved fashion for transmit and receive. Since this mode is synchronous, key stream bits in each direction must be used up at the same rate. The port configuration and connection to the D Register is illustrated in Figure 12.

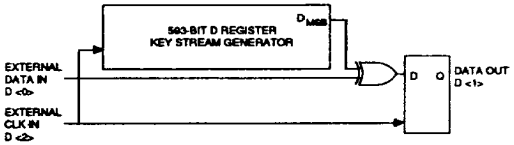


Figure 11: SIMPLEX STREAM MODE PORT CONFIGURATION

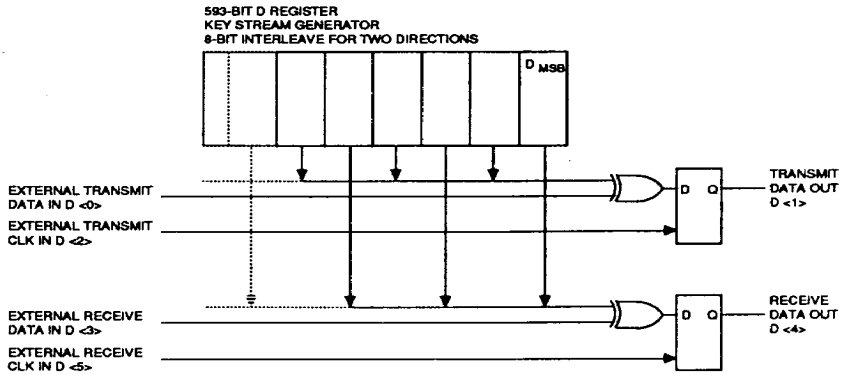


Figure 12: SYNCHRONOUS FULL DUPLEX MODE PORT CONFIGURATION

A and B Registers

The A and B registers are 593–bits long and are principally used to hold the operands for multiplication and the base for exponentiation. If a multiplication instruction is issued, the operands, A and B are tested for zero or all ones. An error is generated if this condition is detected (MTE in the Status Register). Exponentiation can also cause a multiply error since multiplication is part of the internal exponentiation algorithm. All forms of exponentiation requires both A and B Registers to be equal to form the base.

D Register

The D register is 593-bits long, and is used as an exponent register for full discrete exponentiation (EXP1) as well as a buffer to interface to the Data Input and Output Buffers. The D Register also has access to a read-only memory to load internal constants α, and α^{-1}. These constants can be used as the base for discrete exponentiation.

When the D Register is loaded from the Data Input Buffer, it is tested for zero or all ones. An exponentiation error is generated if this condition is detected (EPE in the Status Register).

R and S Registers

R and S are two 256–bit registers used for exponent representation and key storage. R is the primary exponent register, and is used for Repeated Exponentiation, and Message Authentication Code (MAC) generation.

The 256–bit exponent (R Register) has a mapping to a 593–bit exponent. The purpose of the mapping is to limit the hamming weight of the exponent for fast exponentia-

tion. There are three different types of exponentiation a programmer can issue depending on system requirements. The three variants provide an important speed-security trade-off, for various applications, and environments. The exponentiation instructions and their relative hamming weights are discussed in the Programming Section.

The R Register is connected as a 256–bit maximal length linear feedback shift register for the purpose of repeated exponentiation. R is rotated or permuted to a new exponent value with the "permute R" command (PERMR), and the number of permutations performed on the R Register can be programmed via the Load Permute Loop Counter command (LOADPLC).

For Message Authentication Code (MAC) generation using discrete exponentiation, the DEP cyclically adds (modular arithmetic) the encrypted result of one cycle (from the A Register) with the current value of R, and uses that as the next exponent. The instruction "copy A to R plus" (CPA2R+) performs this operation. A high level instruction (MAC) is provided to reduce the overhead in generating MAC's. See the Programming Sections for details.

Both R and S can be loaded from the A or D Register in a 593–bit transfer. Physically, the most significant bit of A and D is connected to the the least significant bit of the R Register, and the most significant bit of the R Register is connected to the least significant bit of the S Register. When a "copy A to R" (CPA2R) command is issued, the least significant 256 bits of A (A_{255-0}) will be stored in R, and a "copy A to RS" (CPA2RS) command will result in R storing the least significant 256 bits of A (A_{255-0}), and S having the next 256 bits of A ($A_{512-256}$).

The R register can also be loaded with a pre–programmed key via the "load R" (LDR) command. The programming of this key can only be changed physically by Calmos at the mask level. This is intended for applications where device authentication is required. When the R Register is loaded from any source, it is tested for zero or unity. An exponentiation error is generated if this condition is detected (EPE in the Status Register).

The contents of the two registers R and S may also be swapped (SWAPRS command), allowing two representations for exponents to be stored in the DEP for bi-directional encryption/decryption. The S Register is also important for re-synchronization, data recovery, and partial file encryption/decryption.

3

PROGRAMMING

The following section lists the instruction set for the DEP. The instructions are divided into three groups, Classes 1 to 3. The first set (Class 1), consists of indivisible, primitive operations such as basic register manipulations (loading, copying and swapping register contents). Class 2 instructions perform arithmetic operations, multiplication, exponentiation, and inversion. Class 3 operations involve macros which use the Class 1 and 2 functions. These macros implement the protocols for block and stream generation such that a single instruction may be issued to the device. This is intended to improve the throughput by reducing the amount of control information that must be passed to the device.

In the following section, the instruction mnemonics, their function, the registers they affect, and the number of DEP clock cycles required are listed.

Class 1 Instructions

Copy Instructions

Most copy (CP) instruction are self explanatory except those that deal with the DEP's I/O, and odd size register transfers. Those instructions that deal with the DEP I/O (CPDO and CPA2DO) are discussed in the Interface Protocol Section which follows the Programing Section.

Odd size register transfer instructions include those commands which copy data from A or D (593-bit registers) to R or R and S (256-bit registers). The R Register always receives the least significant 256 bits of a 593-bit register. If the command is to copy to the S Register as well as R, then the S Register receives the next 256 bits of a 593-bit register (bits 0 to 255 for R and bits 256 to 512 for S). CPA2R+ is a special variant on odd size register transfer which cyclically adds (modular arithmetic) one cycle from the A Register to the current value of R to form the next value of R.

Load Instructions

The load commands that deal with the DEP I/O (LOADD and LOADPLC) are discussed in the DEP Interface Protocol Section. The other load (LD) instructions load constants from internal ROM. Those constants include a, a^{-1}, and the mask programmed key for R.

Swap Instructions

The swap commands are used to simply interchange the contents of registers.

Permute Instruction

The Permute R Register (PERMR) command will rotate the R Register as a maximal length, linear feed back shift register n times, where n is the value of the Permute Loop Counter (PLC). Note that multiple permutations of R can only be achieved with the class 1 PERMR command. Macro commands will only perform one permutation regardless of the value stored in the PLC Register.

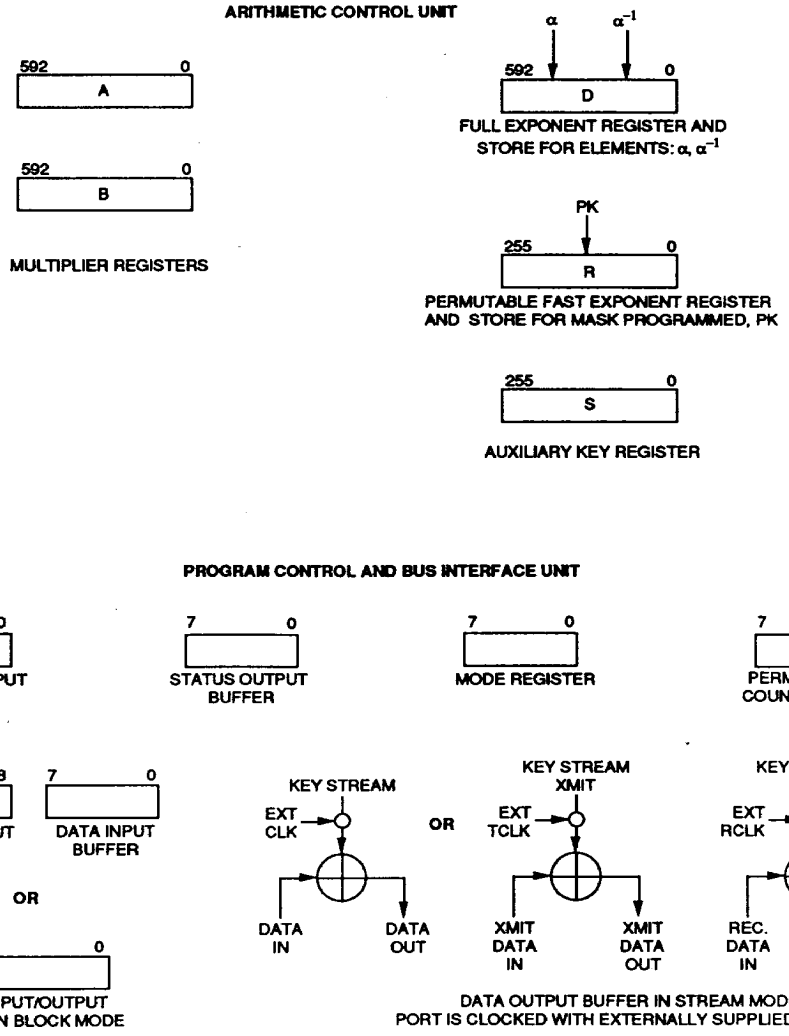


Figure 13 : CA34C168 USER PROGRAMMING MODEL

Table 12: CLASS 1 DEP INSTRUCTION SET

Instruction	OP Code	Operation	Register					DEP cycles
			A	B	D	R	S	
Class 1								
RESET	00	Resets internal DEP controller, Set Mode Register to its default value, and Permute Loop Counter to one.						5
HALT	04	Halts any macro (class 3) instruction. Acts like a NOOP if no macro is running.						5
NOOP	08	Does nothing						5
SETMODE	10	Uses operand bit pattern to set the internal mode of the DEP.						20
CPA2B	20	Copies A to B		A				60
CPB2A	24	Copies B to A	B					60
CPD2A	28	Copies D to A	D					60
CPA2D	2C	Copies A to D			A			60
CPD2B	30	Copies D to B		D				60
CPD2AB	34	Copies D to A and B	D	D				60
CPDO	38	Send D to Output Buffer						
CPA2R	40	Copies lowest 256 bits of A to R				A_l		600
CPA2RS	44	Low 256 of A to R & next 256 of A to S				A_l	A_h	600
CPD2R	48	Copies lowest 256 bits of D to R				D_l		600
CPD2RS	4C	Low 256 of D to R & next 256 of D to S				D_l	D_h	600
CPR2S	50	Copies R to S					R	260
CPA2R+	54	Combines A and R to form a MAC				A+R		600
CPA2DO	60	Copies A to D, then D to Output Buffer			D			
LOADD	64	Loads the D register from Input Buffer (Note 4)			IB			
LOADPLC	68	Loads Permute Loop Count with operand						
LDABA	70	Loads A, B and D with constant α (Note 1)	α	α	α			60
LDABIA	74	Loads A, B and D with constant α^{-1} (Note 2)	α^{-1}	α^{-1}	α^{-1}			60
LDDA	78	Loads D with constant α (Note 1)			α			60
LDDIA	7C	Loads D with constant α^{-1} (Note 2)			α^{-1}			60
SWAPAB	80	Swap Registers A and B	B	A				60
SWAPBD	84	Swap Registers B and D		D	B			60
SWAPRS	88	Swap Registers R and S				S	R	260
LDR	94	Loads R with Programmed Key (Note 3)				PK		5
PERMR	90	Rotate R (Value of Permute Loop Count)				R'		

Notes:
1. α = Internal Constant (primitive element)
2. α^{-1} = Internal Constant
3. PK = Mask Programmed Key
4. IB = Input Buffer

Class 2 Instructions

The Inverse (INVA) command generates the inverse of the value stored in the A Register. The result is stored in the A Register and the B Register becomes undefined.

The multiply (MULT) instruction multiplies A times B in GF(2^{593}). A gets the result and B does not change.

There are three variations of exponentiation (EXP) instructions available for varying degrees of security and speed. In general, registers A and B start with the value to be exponentiated, and the result appears in the A Register. The exponent may be in vector form in the R Register (for EXP2 and EXP3) or may be represented in its full binary form in the D Register (for EXP1). If the exponent is taken from the R Register, then exponentiation will involve a maximum of 30 or 60 multiplications depending on the command used. Full exponentiation taken from the D Register may require 592 multiplications. Note that the true exponent representation in the D Register is from least significant bit to most significant bit, therefore, when a 593-bit exponent is loaded into the D Register as MSB to LSB, the true representation of the exponent is in reverse order.

EXP1 is the most secure mode of exponentiation in terms of the size of the exponent space. The number of elements in this space is on the order of 10^{180}. EXP2 has a smaller exponent space (it is on the order of 10^{50}) but it is considerably faster. EXP3 has an exponent space of size 10^{100} and so falls between EXP1 and EXP2 in both security and speed. The basic underlying security on types of exponentiation is the discrete logarithm problem. The security level of each mode based on this problem is the same. For more details pertaining to security issues, see the document "Security of the CA34C168".

Table 13 : CLASS 2 DEP INSTRUCTION SET

Instruction* OP Code		Operation	Register A	Register B	Register D	Register R	Register S	DEP cycles
Class 2								
INVA	D0	Compute the inverse of A (Note 1)	A^{-1}	U				50000
MULT	A0	A gets A * B	A * B					1300
EXP1	B0	Full exponentiation	$(A)^{D}$					up to 10^6
EXP2	C4	Fast exponentiation (Note 3)	$(A)^{Rm'}$	$(A)^{Rm'}$				up to 40000
EXP3	CC	EXP2 PERMR CPA2B SWAPRS EXP2 PERMR SWAPRS (Note 2)	$(A')^{f(R',S')}$	$(A')^{f(R',S')}$		R'	S'	up to 80000

Notes:
1. U = Undefined
2. R', S' = One rotation or permutation of the original values
3. Rm' = The R Register mapped to its equivalent 593 bit exponent
4. For EXP1 to EXP3, registers A and B must be equal
5. * Arithmetic in GF(2^{593})

Class 3 Instructions

Class 3 instructions are designed to improve throughput by reducing the amount of control information that must be passed to the DEP. These macro instructions are formed from Class 1 and 2 instructions.

Table 14 : CLASS 3 DEP INSTRUCTION SET

Instruction	OP Code	Operation
Class 3		
BLK	E4	Block Encryption/Decryption using internal or external base (Starts with the base loaded into B, and R loaded with the exponent) CPB2A CPA2D EXP2 SWAPBD LOADD SWAPBD MULT SWAPBD CPA2DO TEST CBF (IF CBF = 1, JUMP TO NEXT COMMAND) PERMR REPEAT BLK
STRM	F4	Stream using an internal/external base loaded into B (R is loaded with the exponent) CPB2A EXP2 (WAIT FOR STREAM LOW) CPA2DO (in stream mode) PERMR REPEAT STRM {RESULT IS PLACED IN D}
MAC	E8	(Used only in Block mode. Starts with R loaded) LOADD CPD2AB EXP2 TEST CBF (IF CBF = 1, JUMP TO NEXT COMMAND) CPA2R+ REPEAT MAC

Message Block (BLK) Macro

The BLK instruction can be executed after the base (A and B Register) and the exponent (R Register) have been loaded. When this command is written, 593 bits of a message are loaded into the D Register, encrypted using fast exponentiation, and the corresponding ciphertext block is output from the D Register for transmission. BLK will repeat the the enciphering process until a HALT or the next command is written. A HALT or the next command is written before the last block of data is read out if you wish to stop the BLK loop. Note that a full block of data must be read out before the next command stops the loop.

The receiving side starts with the same exponent R and the inverted value of the transmitting base. Upon receipt of a ciphertext block, the block is loaded into the D Register, decrypted, and output from the D Register as a message block.

Stream Cipher (STRM) Macro

When executing this instruction, the DEP will generate a continuous key stream for enciphering and deciphering data through a built-in exclusive-or function. The clock for extracting key stream bits is provided externally. The STRM instruction is executed after the base (A and B Register) and the exponent (R Register) have been loaded. Two configurations are possible for this macro depending on the port configuration: Simplex Stream Cipher or Synchronous Full Duplex mode. The STRM macro differs from the block macro since any command will stop STRM immediately.

Message Authentication Code (MAC) Macro

This macro is used to generate a MAC for any number of transmitted ciphertext blocks. The receiver will be able to regenerate the MAC and compare it to the transmitted MAC. The MAC macro is stopped by writing the next command before the last block of data is loaded. Usually a CPA2DO is written before the last block is loaded in order to read the Message Authentication Code out of the DEP for transmission.

DEP INTERFACE PROTOCOL

The DEP has a flexible interface to meet the needs of many existing system architectures. There are four data bus configurations to choose from as well as the support of interrupt or poll driven systems. Reading and writing to the DEP is completely asynchronous with respect to its clock. This allows easy integration into existing systems, and does not tie the system clock to the potentially faster DEP clock, a maximum 20 Mhz rate (for CA34C168-20 parts).

Initialization

The DEP is initialized in one of two ways. A hardware reset (bringing the reset pin low) will reset the internal controller, reset the PLC Register to one and put the device into the default mode. The reset line must be held low for five DEP clock cycles during a hardware reset. The default mode is 8-bit uni-directional Block mode with all external interrupts enabled (the Mode Register equals hex 0f). Writing to the Mode Register (via the SETMODE command) will re-initialize the I/O, and reset the PLC Register to one. The initialization procedure is illustrated in Figure 14.

Writing Commands (single byte)

Upon a reset, the CREQ pin will go high (requesting a command) and the CBF bit of the Status Register will go low indicating the command buffer is empty. A flowchart for entering commands is given in Figure 15, and the timing sequence is shown in Figure 16. An instruction can be written as long as CBF=0 whether the DEP is busy or idle. When the DEP has accepted a command and begins processing (Busy Flag goes active, B/I=1), CBF will be cleared so that a new command can be written while the previous instruction is still executing.

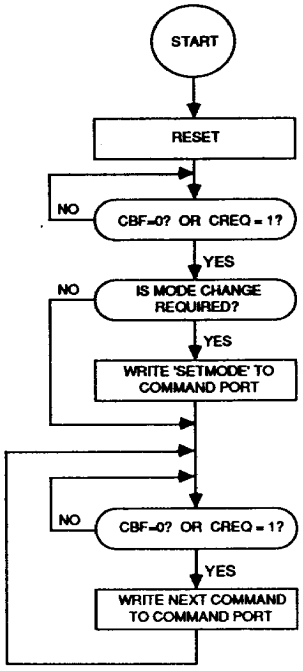


Figure 14: INITIALIZATION

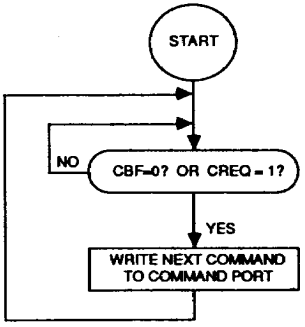


Figure 15 : WRITING SINGLE BYTE INSTRUCTIONS

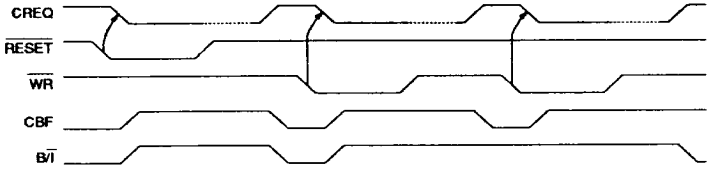


Figure 16 : WRITING DEP INSTRUCTIONS

Commands Requiring Operands

The SETMODE and LOADPLC commands require a single byte operand to be written to the Command Port. The operand is written when the DEP empties the command buffer (after the opcode has been accepted). A flowchart for these commands is shown in Figure 17, and the timing is the same as single byte commands (see Figure 15).

Commands Requiring Data Transfer

Commands which involve reading and writing to the D Register require multiple byte or word transfers to be read from and written to the Data Port. In all DEP modes of operation, the following commands require I/O from the Data Port: CPDO, CPA2DO, and LOADD. However, the BLK macro command uses CPA2DO and LOADD in Block Mode only; and the STRM macro command uses CPA2DO only in the Stream Modes.

The commands, CPDO and CPA2DO, are issued for reading the D Register via the Data Port in all modes of operation. In general, reading the Data Port requires the monitoring of the OBF status bit or the DREQ2 pin, and the number of bits, bytes or 16-bit words transferred (CF status bit). The flowchart of Figure 18 shows the reading process.

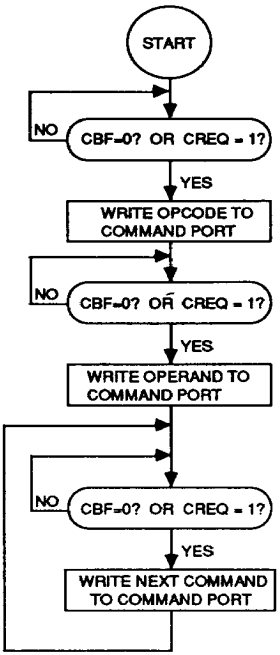


Figure 17 : WRITING COMMANDS WHICH REQUIRE OPERANDS TO THE COMMAND PORT

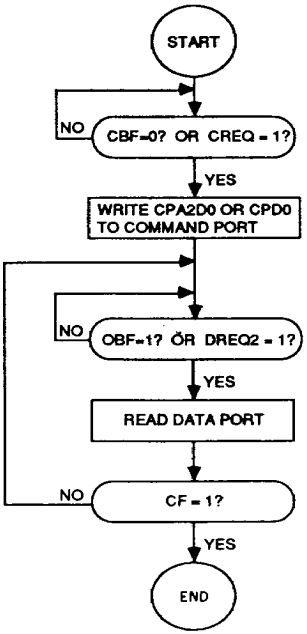
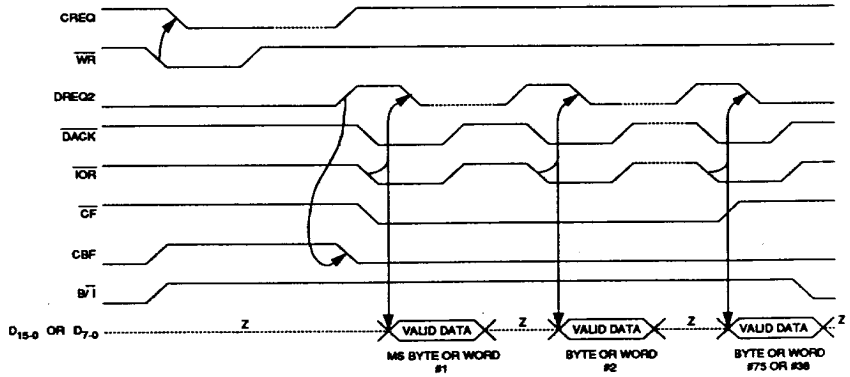


Figure 18: WRITING COMMANDS WHICH REQUIRE DATA TO BE READ FROM THE DATA PORT

In 8 or 16-bit Block Mode, the CPU has to read 75 bytes or 38 words respectively. In order for a valid read to occur, DREQ2 or OBF must be high when IOR and DACK are brought low. The timing diagram for these instructions in Block mode is shown in Figure 19.

Stream Cipher Mode timing is similar to that of the Block Mode where a valid read can only occur when DREQ or OBF is high and IOR and DACK are brought low, however, data and clock must be asserted as well. The clock pin must be low before the actual read because the rising edge of clock will shift the first bit of the D Register to the Data Port. This is key stream data (the most significant bit of D) exclusive-or'd with data in. In Simplex Stream Mode, DREQ2 will remain high for the full 593 bit transfer. The timing is shown in Figure 20. In Synchronous Full Duplex Mode, DREQ2 goes high for 8 bits of transmit and receive data (a total of 16 bits transferred), then low while the buffer is being filled with the next 16 bits. This process continues until 592 bits have been transferred (37 bytes for each direction). The timing is shown in Figure 21. While in stream mode, a new command will immediately stop the STRM macro and execute the new command written. A HALT will act as a NOOP to stop the STRM macro.



Note : Read 75 bytes or 38 words depending on bus configuration

Figure 19: READING D OR A REGISTER (CPD0 OR CPA2D0)

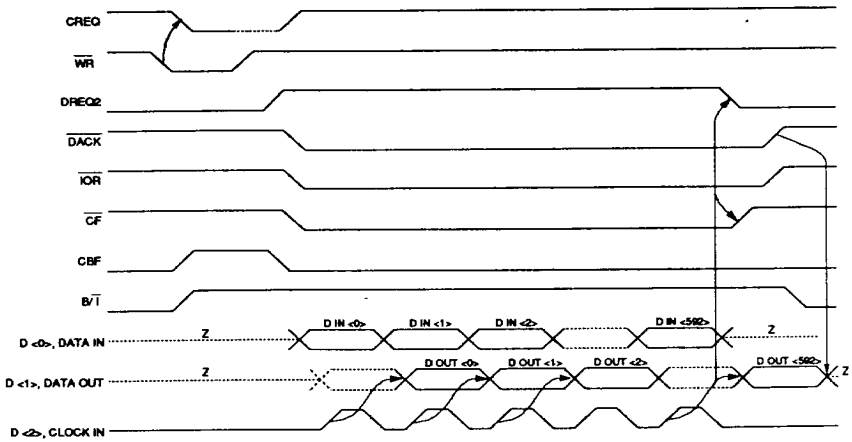


Figure 20: READING D REGISTER IN SIMPLEX STREAM MODE

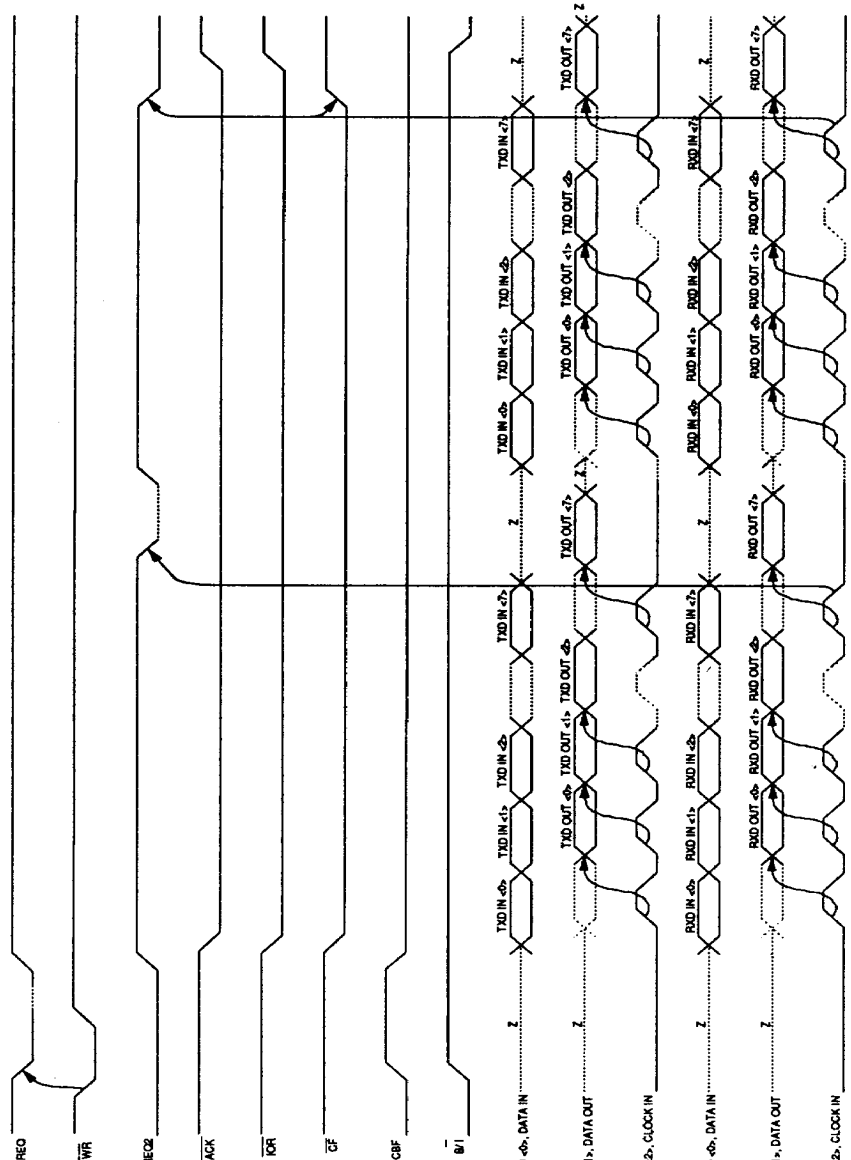


Figure 21: STREAM MODE, FULL DUPLEX

The command, LOADD, is issued to load the D Register via the Data Port in all modes of operation. Loading D requires monitoring the IBF status bit or the DREQ1 pin, and the number of bytes or 16-bit words transferred (CF status bit). The flowchart of Figure 22 shows the writing process.

In 8 or 16-bit Block Mode, the CPU has to write 75 bytes or 38 words respectively. In order to issue a valid write, DREQ1 must be high or IBF low when IOW and DACK are brought low. The timing diagram for this instruction is shown in Figure 23.

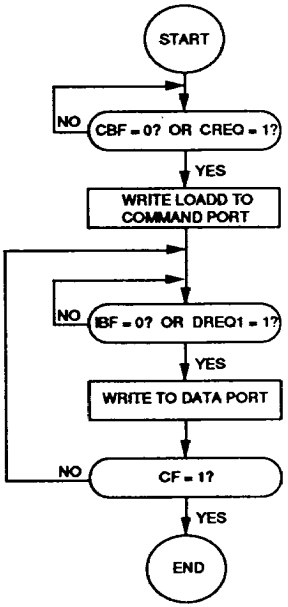
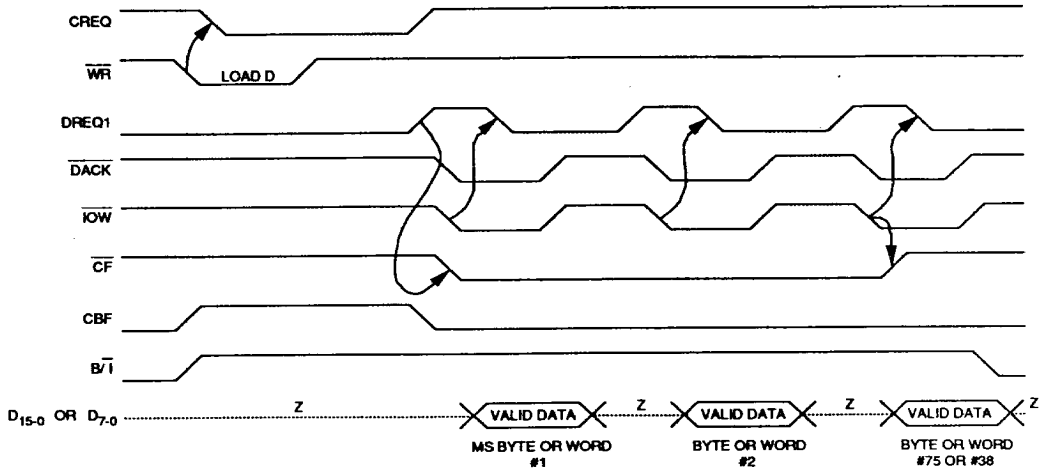


Figure 22: WRITING COMMANDS WHICH REQUIRE DATA TO BE WRITTEN TO THE DATA PORT



Note : Write 75 bytes or 38 words depending on bus configuration

Figure 23 : WRITING DATA TO THE D REGISTER (LOAD D)

APPLICATIONS

The CA34C168 can be incorporated into systems in a number of ways. Figure 24 shows the basic device being interfaced to a microprocessor bus for block encryption transfers. This configuration can be used as part of the communications control subsystem of a larger device.

Figure 25 shows a conceptual diagram of a standalone cryptosystem. Here, the device is used for both the exchange of keys and encryption/decryption of block data. The device can also be used in conjunction with conventional cryptosystems.

Figure 26 illustrates the CA34C168 used as a public key passing device along with a DES device for conventional encryption/decryption.

To improve compatibility with other systems, the configuration shown in Figure 27 may be used. Here the CA34C168 provides the public key exchange facilities allowing either system to be used for the data exchange. This technique is used to provide compatibility with existing private key systems (such as DES in North America), and allow users to communicate with the CA34C168. This is particularly convenient in countries where the export of DES is not permitted. Messages can also be enciphered with one system, then encrypted with the other for added security.

In Figure 28, the device is shown in a stream cipher application. This may include digitized voice or serial data applications.

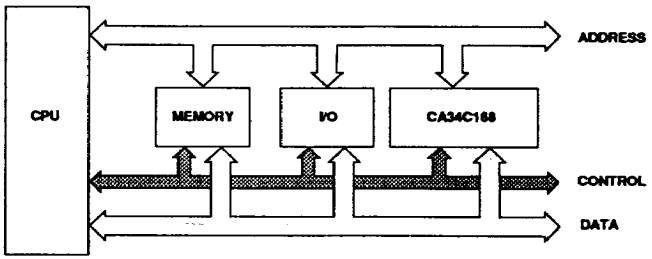


Figure 24 : MICROPROCESSOR INTERFACE for BLOCK TRANSFERS

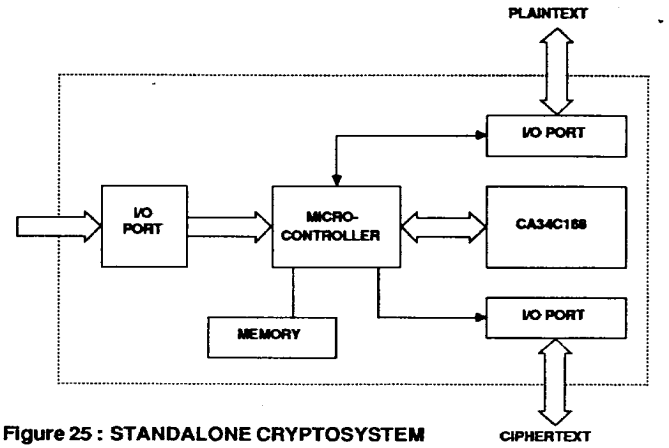


Figure 25 : STANDALONE CRYPTOSYSTEM

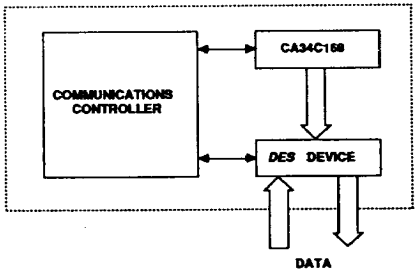


Figure 26 : CONVENTIONAL *DES* DEVICE with CA34C168 for KEY PASSING

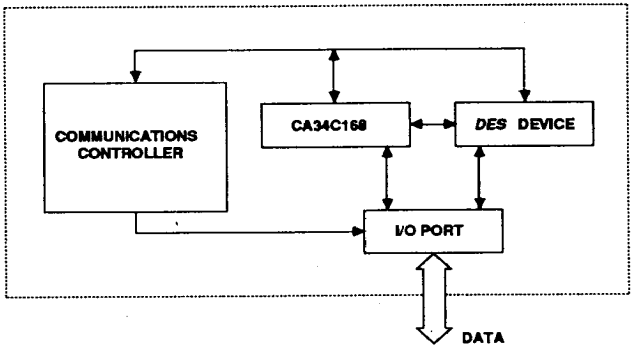


Figure 27 : CA34C168 with *DES* DEVICE

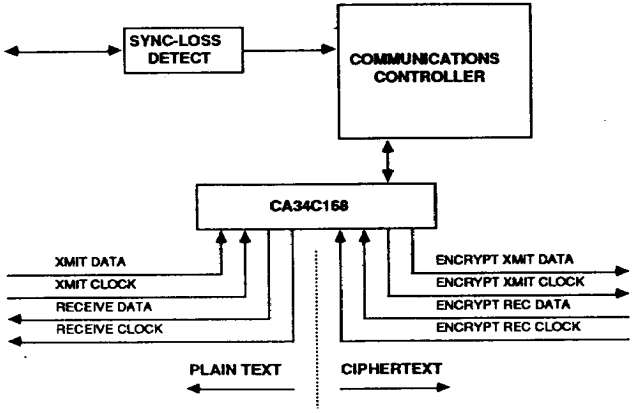


Figure 28 : STREAM CIPHER