DS3114-1.3

DVS200

SPEECH/DATA ENCRYPTION PROCESSOR

The DVS200 is a digital encryption processor, with on-chip A-D and D-A converters for speech bandwidth signals, that implements a TDM (Time Division Multiplexing) encryption algorithm. The device can be used to protect virtually any vulnerable analog speech or digital data communication channel. The high security is provided by a complex on-chip key generator, and an algorithm that checks the 'randomness' of the encrypted output.

For basic speech encryption applications, the DVS200 requires the addition of only a DRAM, SRAM and a few other external components.

The device uses correlation for sync tone decoding, which gives high synchronisation performance even on relatively noisy channels.

An on-chip notch filter eliminates sync tones from the speech channel, thus enabling frequent synchronisation without significant loss of speech.

The DVS200 has a range of user selectable options: clear voice override, periodic sync, 8/16 segments per frame, message key, and sync delay.

The chip uses multiple methods of code entry: switches, keyfill gun or PROM dump and supports battery backup, enabling it to be powered down when not in use.

FEATURES

- Complete Encryption System on a chip
- Excellent Speech Quality due to On-chip High Performance A to D and D to A Converters
- Low Power CMOS Fabrication - typically 25mW
- Multiple Methods of Code Entry
- Supports Battery Backup
- High Synchronisation Performance
- On-chip Notch Filter for Eliminating Sync Tones from the Speech Channel
- A Range of User-Selectable Options
- Data Encryption Rate up to 4.8kbits/s

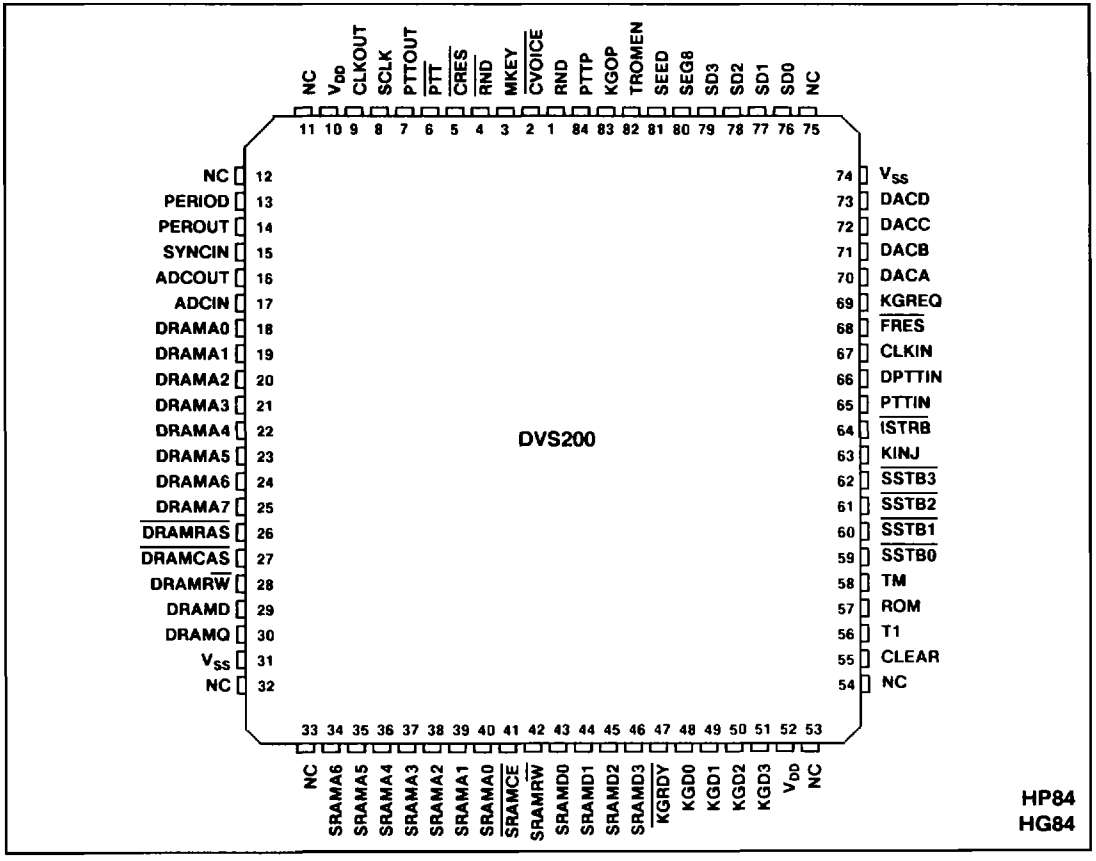


Fig. 1 Pin connections - top view

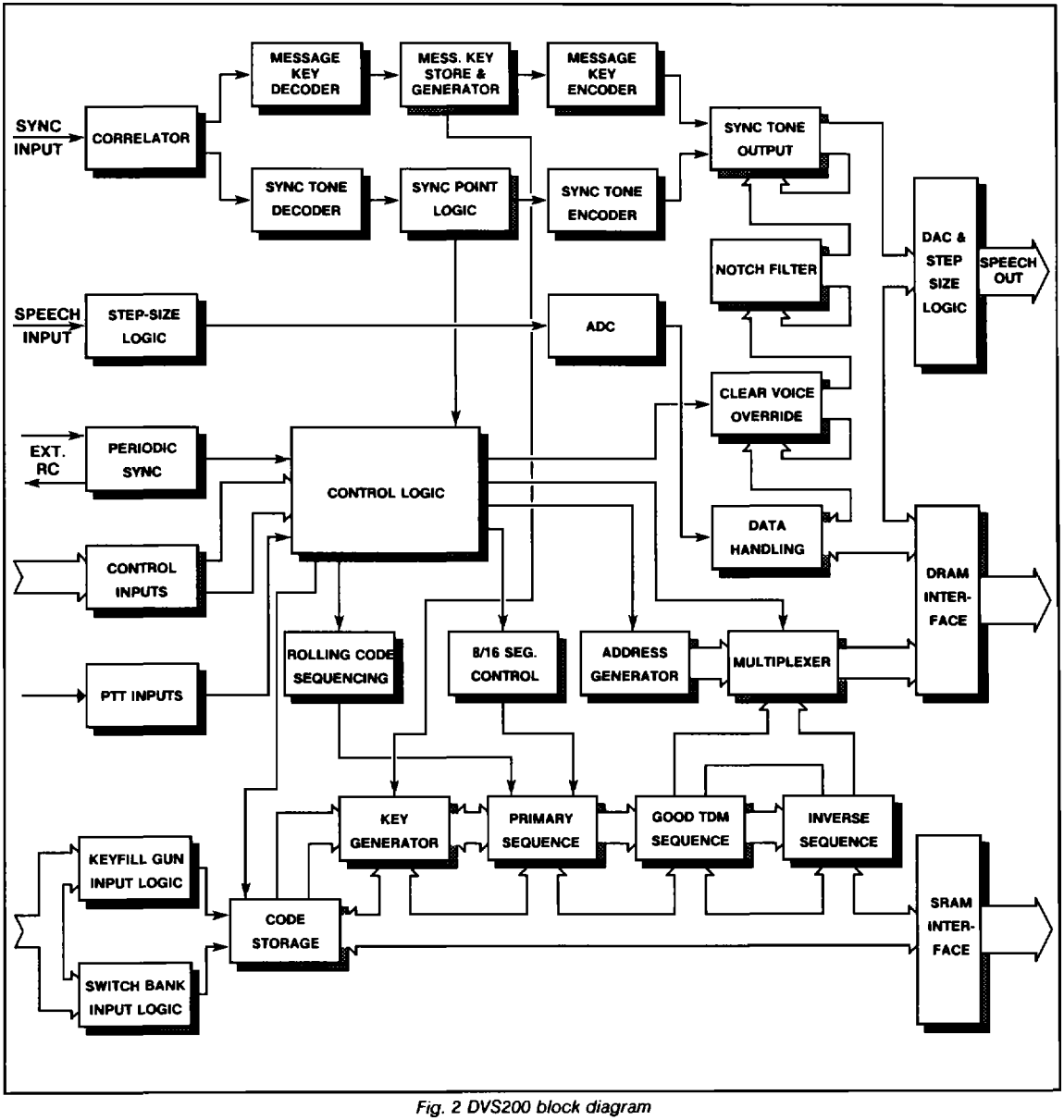


Fig. 2 DVS200 block diagram

PIN DESCRIPTIONS

Pin	Name	Type	Description
1	RND	I	Input for the source of the message key data.
2	$\overline{\text{CVOICE}}$	IP	Active low clear voice override pin. When a logic '0' is applied the device outputs unencrypted speech. When a logic '1' is applied, the device is in secure mode.
3	MKEY	IP	Used for selecting the message key option. A logic '1' enables the device.
4	$\overline{\text{RND}}$	O	This is a latched, inverted version of RND (pin 1). It can be used, together with pin 1, to provide a random data stream for the message key.
5	$\overline{\text{CRES}}$	O	Test pin - Pulses low when the device synchronises.
6	$\overline{\text{PTT}}$	O	Inverted version of PTTOUT (pin 7).
7	PTTOUT	O	This pin, when active, indicates that the device is in transmit mode. It can therefore be used to control the Tx/Rx mode of the equipment that the device is installed in.
8	SCLK	O	Buffered version of CLKOUT (pin 9). Can be used to set the clock oscillator frequency.
9	CLKOUT	O	With CLKIN (pin 67), connection for clock oscillator crystal.
10	V_{DD}	I	+5V
13	PERIOD	SI	Connections for external RC timing components for the periodic sync oscillator.
14	PEROUT	O	
15	SYNCIN	SI	Received sync tone input.
16	ADCOUT	O	The analog to digital converter is formed around these two pins
17	ADCIN	I	
18	DRAMA0	O	DRAM Address bus.
19	DRAMA1	O	
20	DRAMA2	O	
21	DRAMA3	O	
22	DRAMA4	O	
23	DRAMA5	O	
24	DRAMA6	O	
25	DRAMA7	O	
26	$\overline{\text{DRAMRAS}}$	O	DRAM Control bus.
27	$\overline{\text{DRAMCAS}}$	O	
28	DRAM$\overline{\text{RW}}$	O	
29	DRAMD	O	Connect to DRAM data input.
30	DRAMQ	I	Connect to DRAM data output.
31	V_{SS}	I	0V
34	SRAMA6	O	SRAM Address bus
35	SRAMA5	O	
36	SRAMA4	O	
37	SRAMA3	O	
38	SRAMA2	O	
39	SRAMA1	O	
40	SRAMA0	O	
41	$\overline{\text{SRAMCE}}$	O	SRAM Control bus.
42	SRAM$\overline{\text{RW}}$	O	
43	SRAMD0	BP	SRAM Data bus.
44	SRAMD1	BP	
45	SRAMD2	BP	
46	SRAMD3	BP	
47	$\overline{\text{KGRDY}}$	O	This is relevant whenever the device is used for encrypting data. It strobes low when a valid word is present on the key generator output port.

NOTES
1. Key to pin type: I = Input, IP = Input with pullup, SI = Schmitt input, O = Output, TO = Tri-state output, BP = Bidirectional output with pullup
2. Tie all unused inputs to either V_{DD} or V_{SS}.
3. Pins 11, 12, 32 and 33 are NC (No Connection).

Table 1 Pin descriptions

PIN DESCRIPTIONS (continued)

Pin	Name	Type	Description
48 49 50 51	KGD0 KGD1 KGD2 KGD3	O O O O	Key generator output port
52	V_{DD}	I	+5V
55	CLEAR	O	Indicates whether the device is operating in clear or secure mode. Logic '1' clear mode, logic '0' secure mode.
56 57 58	T1 ROM TM	O O IP	Test pins.
59 60 61 62	$\overline{SSTB0}$ $\overline{SSTB1}$ $\overline{SSTB2}$ $\overline{SSTB3}$	TO TO TO TO	These pins strobe low, in sequence, when the device is being seeded. They are only used when a bank of switches is used to provide the seed data.
63	KINJ	I	Used to select which mode of seed entry is to be used. A logic '0' selects switch entry (automatic), a logic '1' selects keyfill gun/PROM dump entry (external strobe).
64	$\overline{ISTRB}$	SI	Strobe pin (active low) for keyfill gun/PROM entry of seed data.
65	PTTIN	SI	Used to select the transmit mode of the device. The polarity of the active level (i.e. 0 or 1) is determined by PTTP (pin 84).
66	DPTTIN	SI	Used to provide an additional delay between start of transmission and sync tone transmission. Thus allowing for delays in the channel opening; due to squelch circuitry etc.
67	CLKIN	I	With CLKOUT (pin 9), connection for clock oscillator crystal.
68	$\overline{FRES}$	SI	Device reset (active low).
69	KGREQ	I	When in data encryption mode, this pin is strobed (active high) to request a key generator word.
70 71 72 73	DACA DACB DACC DACD	O O O O	Digital to analog converter outputs.
74	V_{SS}	I	0V
76 77 78 79	SD0 SD1 SD2 SD3	IP IP IP IP	Seed data input port.
80	SEG8	IP	Option pin for selecting number of segments per frame. Logic '0' sixteen segments, logic '1' eight segments.
81	SEED	IP	Normally the device loads new seed data each time it is reset. Taking this pin low inhibits this function. This enables seed data already present in the SRAM, due to battery back-up for example, to be retained. The device can therefore be powered down without loss of seed data.
82	TROMEN	IP	Test pin.
83	KGOP	IP	Selects which mode of encryption the device is required to operate in A logic '0' selects data encryption, a logic '1' selects speech encryption.
84	PTTP	IP	Used for selecting which polarity PTTIN and PTTOUT are active. A logic '0' selects active high, a logic '1' selects active low.

NOTES
1. Key to pin type: I = Input, IP = Input with pullup, SI = Schmitt input, O = Output, TO = Tri-state output, BP = Bidirectional output with pullup
2. Tie all unused inputs to either V_{DD} or V_{SS}.
3. Pins 53, 54 and 75 are NC (No Connection).

Table 1 Pin descriptions (continued)

Pin	Name	Logic '0'	Logic '1'
2	$\overline{\text{CVOICE}}$	Clear Speech mode.	Encrypted Speech mode.
3	MKEY	Message key disabled.	Message key enabled.
63	KINJ	Automatic seed data entry (switches).	Strobe controlled seed data entry using keyfill gun/PROM dump).
80	SEG8	Sixteen segments per frame.	Eight segments per frame.
81	SEED	Disable seed data loading on reset.	Enable seed data loading on reset.
83	KGOP	Data encryption mode.	Speech encryption mode.
84	PTTP	PTT active high.	PTT active low.

NOTE
All of the above pins except KINJ (pin 63) have internal pullups. So, if a logic 1 is desired, the pin should simply be left unconnected.

Table 2: Summary of Options

OVERVIEW OF OPERATION

ENCRYPTION TECHNIQUE

The DVS200 is an integrated circuit that encrypts speech using a TDM (Time Division Multiplexing) encryption technique. This process involves dividing speech, in the time domain, into sections; these sections are known as frames. The frames are then sub-divided into smaller sections or segments. The device then reverses and re-arranges (transposes) the segments of speech within each of the frames. Once this has been done, the encrypted speech is output from the DVS200. Fig. 3 demonstrates the effect that the DVS200 would have on a signal that had a ramped envelope.

Two things will be noticed from Fig. 3: first, that the signal is delayed by an equivalent of one frame, i.e. 236ms (this figure is valid for the nominal device clock frequency of 4.433619MHz). This means that there will be a system delay of 472ms (236ms for encrypt and 236ms for decrypt).

The second thing to notice, is that, in Fig. 3, there are eight segments per frame. The DVS200 has the option of increasing this to sixteen segments per frame; this is achieved by simply tying an external pin (pin 80-SEG8) to ground.

The sixteen segments per frame option offers greater security (due to the increased number of permutations available), but its use may reduce the recovered speech quality. The speech is recovered, i.e. decrypted, simply by reversing the process performed at the encryption stage.

KEY GENERATOR

The way in which the segments are transposed within the frame is determined by two functions in the DVS200. The first is the on-chip key generator. The key generator is a sub-system that outputs a set of numbers in a pseudo-random sequence. The position of each segment is determined by the output of the key generator. The key generator is complex and offers a high degree of unpredictability.

This means that it will be difficult to extract the original speech from the encrypted signal. What sequence the key generator uses, and from what point in the sequence the key generator starts, is determined by the seed data (code) that has been entered by the user. This code can be any one of approximately 3×10^{38} permutations (depending on the method of entry) and must be entered in both the encrypting and decrypting DVS200s for the original speech signal to be recovered correctly.

The other function that determines the transposition of the segments is the 'Good TDM Algorithm'. This algorithm ensures that the segments have been transposed in a non-linear fashion. For example, the sequence A5,A6,A7,A8,A1,A2,A3,A4 would not be suitable for encryption purposes, whereas the sequence shown in Fig. 3 (A5,A8,A2,A4,A6,A1,A7,A3) is eminently suitable.

SYNCHRONISATION - NO MESSAGE KEY

In order for the receive DVS200 (Rx) to correctly decrypt the incoming encrypted speech, it must be synchronised to the transmit DVS200 (Tx) in two ways. First, the frame and segment boundaries of the two devices must be aligned in time; secondly, the two key generators must be at the same point in the same sequence for each corresponding segment.

Both of these phases of synchronisation are achieved with a sync tone. This is a 128 period tone at a frequency of 1.082kHz (with a clock frequency of 4.433619MHz) that is transmitted across the transmission channel by the Tx DVS200. When the Rx DVS200 receives the sync tone it is recognised (using a form of correlation) and a sync point is extracted.

At this point the frames are aligned and the key generator is loaded with the code previously entered by the user. The two devices then have an equal time reference from which to start operation (this reference point is shown in Fig. 6a).

A sync tone is transmitted each time a transmission is initiated. Sync tones can also be transmitted at regular intervals (periodic sync); the period between each sync tone transmission is determined by the user. Note that in Fig. 6a, the DAC output is shown with only sync tones present. Normally encrypted speech is also present, but this has been omitted for clarity.

SYNCHRONISATION - MESSAGE KEY

The message key facility is an option, selected by MKEY (pin 3), that significantly increases the operational security of the DVS200. The main function of the message key is connected with synchronisation. Normally, as mentioned above, the key generator is set to a particular point (determined by the user code) each time the devices synchronise. The net result of this is that the DVS200 repeats a sequence of segment transpositions each time a sync tone is received.

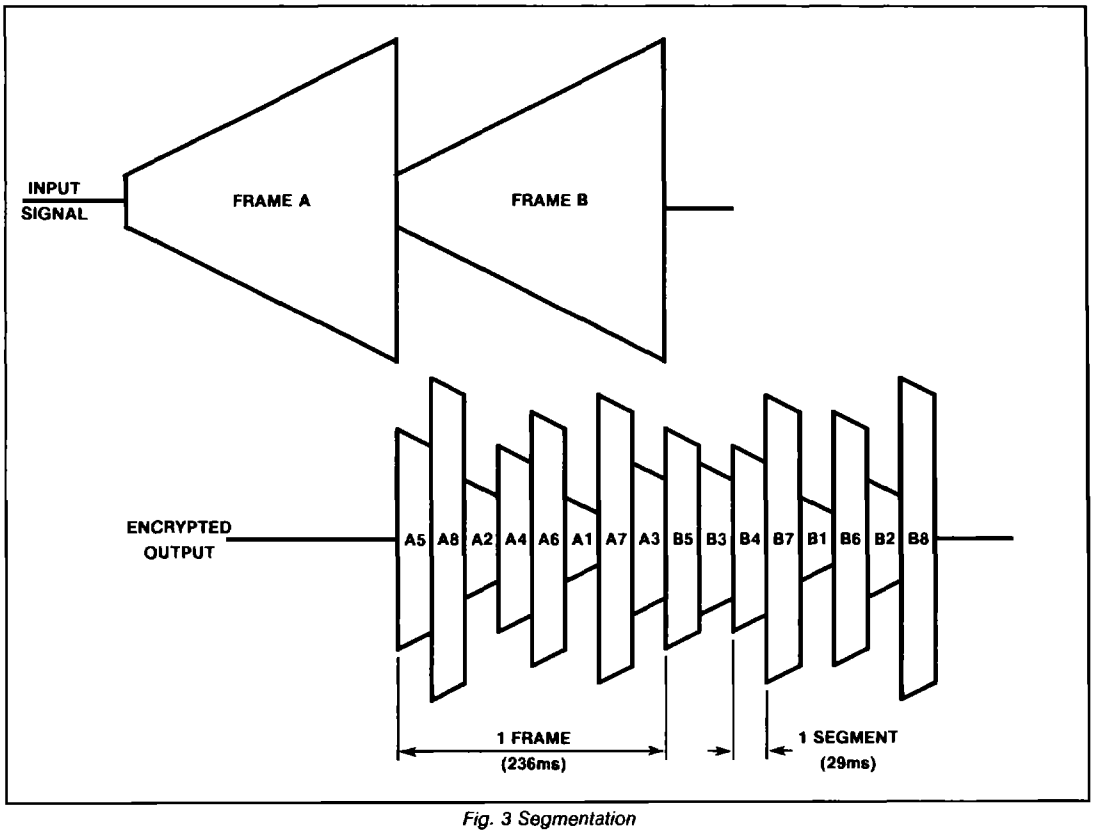


Fig. 3 Segmentation

When the message key option is selected, the key generator is set to a different point each time the device synchronises. The point to which the key generator is set is determined by the user code and a new set of data. This new data is the message key.

The message key data is derived by the Tx DVS200 and then transmitted to the Rx DVS200 (using phase modulation) each time a sync tone is transmitted (for derivation of message key data see page 4-10). The fact that the key generator is reset to a different point each time devices synchronise means that the period between the transmission of sync tones can be very short (as little as a second) without diminishing the security of the DVS200, thus allowing the late-entry-into-net facility that many communication systems require.

There are 32 bits of data exchanged between the two devices each time they synchronise. Each bit is represented by 32 periods of a 1.082kHz tone (the same frequency as the sync tone). It would therefore take approximately one second to complete the synchronisation process. To avoid this excessive delay, and to initialise the message key exchange, a message key precursor is transmitted before the message key itself (see Fig. 6b). This precursor is of the same length and frequency as that of the sync tone discussed on page 4-7.

The DVS200 temporarily synchronises to the precursor, loading only user code into the key generator. So, between the precursor sync point and the final sync point the DVS200 is operating with the user code exclusively (as in non-message key mode). It is only once all of the message key has been received that it can be utilised by the encryption facilities.

As mentioned above, the data is encoded using phase modulation. Each set of 32 periods (one data bit) is either in phase or anti-phase with the precursor; if it is in phase it represents a logic '0', anti-phase a logic '1'. The first bit, D1 in Fig. 6b, is always a logic '1'; i.e. in anti-phase to the precursor. The DVS200 detects this phase change and switches over to message key decode mode.

The example shown in Fig. 6b has the second data bit (D2) as a logic '0', and it can be seen that at the junction of D1 and D2 the tone reverts to being in phase with the message key precursor.

The final sync point always occurs at the final edge of the message key tone. In the case of Fig. 6b, the last bit, D32 is a logic '0' (in-phase), so the final edge is negative-going. If D32 were a logic '1', the final edge would be positive-going.

CLEAR VOICE OVERRIDE

The DVS200 outputs unprocessed speech when either one of two things happen. The first possibility is that clear speech mode is selected manually by the user. This is done by applying a logic '0' to the $\overline{\text{CVOICE}}$ input (pin 2).

The second possibility is that the DVS200 has automatically invoked the clear speech mode because the encryption facility is not being used.

This facility allows a piece of equipment incorporating the DVS200 to be used on channels that are not exclusively encrypted, without the user manually switching the equipment between clear and secure mode.

There are three different events that can trigger the automatic switch to clear mode. They are as follows:

(a) Device Reset - Each time the device is reset, the DVS200 switches to clear speech mode.

(b) Post PTT - At the point that PTTOUT (pin 7) goes inactive (i.e. the transmission has been completed) the DVS200 switches to clear speech mode.

(c) Non-receipt of Sync Tone - If, when using periodic sync, a sync tone has not been received within twice the normal interval between sync tones, the DVS200 switches to clear speech mode.

When the DVS200 has been switched to clear speech mode by one of the above events (a, b or c) it remains in that state until it either receives a sync from another DVS200, or the transmit mode is selected (i.e. PTT goes active). It then switches back to secure speech mode.

From the above, it will be noticed that the speech is always transmitted encrypted unless $\overline{\text{CVOICE}}$ is active (logic '0'). A logic '1' on the CLEAR output (pin 55) indicates that the DVS200 is in clear speech mode.

APPLICATION NOTES

DRAM AND SRAM SPECIFICATIONS

For basic operation the DVS200 needs two external ICs: a dynamic RAM (DRAM), and a static RAM (SRAM). The DRAM is used by the DVS200 to store sections of speech. The DRAM should have an organisation of 64K×1 and an access time of no greater than 150ns. The minimum timing requirements are shown in Fig. 8a; the TMS4164-15 is recommended, though any DRAM may be used as long as it has similar (or better) operational characteristics to those shown. Similarly, a larger bit-wide DRAM (the TMS4256-15, for example) may be used as long as the unused address inputs are tied.

The SRAM is used for code storage and as a scratch pad for general DVS200 operation. The SRAM requirements for the DVS200 are that it should have an organisation of at least 128×4, and a maximum access time of 200ns. The minimum timing requirements are shown in Fig. 8b; the PCD5114 satisfies this specification, though again, any SRAM whose performance is within the specification shown in Fig. 8b may be used.

Larger SRAMs can be used with the extra addresses either tied, or alternatively, be used as part of a paging system; this would allow the user to switch between sets of codes (by means of a switch on the equipment, for example) without having to continually re-seed the system. See Seed Data Paging (page 4-12).

DEVICE RESET

Each time the DVS200 is powered up, it must be reset so that the internal logic is set to a known state. This is achieved by taking the $\overline{\text{FRES}}$ input (pin 68) low for a period of time not less than 2 microseconds. A simple circuit for achieving this is shown in Fig. 11.

CLOCK OSCILLATOR

The DVS200 has a nominal clock frequency of 4.433619MHz, though it can run at clock frequencies of up to 8MHz (note that if the frequency is increased from the nominal, the access times of the DRAM and SRAM will have to be reduced by a similar factor). As well as the two oscillator pins, the DVS200 has an extra pin (SCLK-pin 8) that is a buffered version of the oscillator output, CLKOUT (pin 9). The SLCK output can, therefore, be used to set the oscillator frequency without loading the oscillator circuitry. The SCLK output can also be used to clock any external logic being used. The basic circuitry required to implement the oscillator is shown in Fig. 12.

ANALOG TO DIGITAL CONVERTER

The DVS200's analog to digital converter (ADC) is a serial adaptive delta modulator (ADM) that runs at a sample rate of 139kbit/s. The average input signal level should be approximately 1.7Vp-p; the ADC input should be driven by an impedance of less than 1kΩ. The external circuitry required, together with the recommended component values, are shown in Fig. 13.

DIGITAL TO ANALOG CONVERTER

The DVS200 has four outputs which, together with a few external passive components, form the digital to analog converter (DAC); these outputs are DACA (pin 70), DACB (pin 71), DACC (pin 72) and DACD (pin 73). Fig. 14 shows the connection details. It is recommended that the values shown in Fig. 14 are used as any modification may adversely affect the performance of the DAC. It is important to not to load the output of the resistor/capacitor network with an impedance or less than 100kΩ. If the input impedance of the interface circuitry is less than 100kΩ then the network should be buffered.

Any one of five different signals can be present on each of the outputs; the signals are: clear speech data, encrypted speech data, notch filter data, transmit sync tones and device clock. The mode in which the device is operating determines which of these signals are present on each output. The DVS200's DAC has six different modes of operation, each of which is selected by the control logic of the DVS200. A description of each mode, together with the signals present on each of the DAC outputs is given below:

(a) Tx Encrypted - The DVS200's normal transmit operation. Encrypted speech outputs from the DAC at the same amplitude as the signal input to the ADC. Encrypted speech data is present on all four of the DAC outputs.

(b) Tx Clear - In this mode the DVS200 outputs clear speech, again at the same amplitude as the signal input to the ADC. Clear speech data is present on all four of the DAC outputs.

(c) Tx Sync - This mode is invoked whenever transmission of a sync tone is requested, either by an activation of the DPTTIN input (pin 66; see Push-to-Talk Circuitry, page 4-10), or the periodic sync circuitry. The operation consists of two phases. The main phase involves the transmission of the sync tones. During this phase encrypted speech data is output from the DADC and DACB outputs, and sync tones are output from the DACC and DACD outputs. This has the effect of attenuating the speech by the factor of two (this will be compensated for by the Rx DVS200). This phase lasts for either 1.06s or 118ms (depending on whether the message key mode has been selected)

The other phase of this mode, which occurs immediately before the sync tone transmission phase, attenuates the speech output from the DAC (again, by a factor of two) for a period of 118ms. This has the effect of maintaining the speech at a constant level for the duration of a whole frame (or an exact multiple with the message key option selected) The attenuation is achieved by replacing the sync tone on DACC and DACD with the device clock

(d) Rx Encrypted - The DVS200's normal receive operation. Note about that the output is attenuated (again, by a half) with respect to the ADC input. As with the first phase in (c) above, this is achieved by outputting encrypted speech data on DACA and DACB, and device clock on DACC and DACD.

(e) Rx Clear - In this mode the DAC outputs undecrypted speech (see Clear Voice Override, page 4-8): so if there is clear speech on the ADC, there will be clear speech on the DAC output. The situation is the same as that in (d) above, except for the fact that clear speech data outputs from DACA and DACB instead of encrypted speech data.

(f) Rx Notch Filter - The notch filter function is used to remove sync tones from the receive channel, and is therefore centred at the sync tone frequency of 1.082kHz.
As the notch filter attenuates other adjacent frequencies as well as the sync tone frequency, it is only selected whenever a sync tone has been received. When the DAC is in this mode, the speech is output from the DAC at the same level as it was presented to the input of the ADC. As the speech was transmitted at half its normal level during Tx sync (see (c), previous page) the level will be consistent throughout the receive mode of operation.

Table 3 summarises the various modes of operation of the DAC outputs, as well as the signal combinations that appear at the outputs during the various phases.

MESSAGE KEY

Basic Circuitry

The message key option is is selected by leaving the MKEY pin (pin 3) unconnected as an internal pullup holds the input at logic '1'. There is a small amount of external circuitry required for the message key operation which is shown in Fig. 16. This external circuitry is inserted between the DVS200 and SRAM on the D0 connection. Note that the circuit in Fig. 16 is for PTT active low - if PTT is active high, the $\overline{\text{PTT}}$ output should be used instead of PTTOUT). It is only functional in Tx mode, so if a DVS200 is being used exclusively in the Rx mode (in a duplex system for example) this circuitry is not required.

Message Key Derivation

While the DVS200 is in message key mode, 32 bits of data (the message key) are required each time a sync tone is transmitted. Each time the Tx sync circuitry requires a data bit for the message key, it samples the input RND (pin 1); there is a free-running latch on this input, clocked at a frequency of 138kbits/s. The signal presented to this input can be derived from any source, but it should be random in nature. There are many ways of deriving this signal; one way is to connect the RND input to the ADCIN input. Another method of deriving this signal is to connect a noisy diode to the RND input.

There is in addition to the RND input, an output called $\overline{\text{RND}}$ (pin 4). This is the inverted output of the latch on the RND input and can be used to help derive the message key data. For example, it could be used, with RND, to form an oscillator circuit; or it could be used to form another ADC circuit (like that shown in Fig 13) Any of these methods, or indeed any other, can be used to derive the message key

Message Key Mute

When the Rx DVS200 receives a sync tone (with or without message key) the notch filter at the DAC is activated; this notch filter is centred at the sync tone frequency. With a message key transmission the sync tone may be changing phase every 32 periods, depending on whether the message key data is changing.

At these data boundaries the sync tone will not be a 50% duty cycle square wave (see Fig. 6b). The notch filter will not be able to eliminate this from the channel. This will result in a glitch on the final speech waveform which may be large enough to be heard over the speech present on the channel.

One way to eliminate this glitch is to mute the channel (post-DVS200) each time a glitch is expected. A circuit providing a 1ms pulse each time a glitch is present is shown in Fig. 17. This logic output (Mute Out) can then be connected to an FET, or analog switch, that will shunt the channel each time a glitch is present.

The channel should be shunted to a voltage equal to the bias level, otherwise a glitch may be introduced that is larger than the one the circuit is designed to eliminate!

SYNC INPUT

The receive analog channel of the equipment should be fed into the SYNCIN Input (pin 15) before it has been processed by the Rx DVS200. SYNCIN is a digital input, so the signal present on this input must be a squarewave with a 50% duty cycle.

You will have noticed in Fig. 6a that the sync tone present on the Rx SYNCIN input is inverted with respect to the sync tone at the Tx DAC output. This relationship should be maintained wherever possible. A simple sync tone inverter-cum-conditioner is shown in Fig. 15

PUSH-TO-TALK (PTT) CIRCUITRY

The PTT circuitry usually indicates that a piece of simplex equipment (a mobile radio, for example) is in transmit mode. It is usually derived by the user by means of an external switch. As the DVS200 is also a single channel device it has receive and transmit modes; the simplex equipment's PTT signal can therefore be used to select the operational mode of the DVS200 (i.e. receive or transmit).

Mode of operation	DACA (Pin 70)	DACB (Pin 71)	DACC (Pin 72)	DACD (Pin 73)
Tx Encrypted	Encrypted Data	Encrypted Data	Encrypted Data	Encrypted Data
Tx Clear	Clear Data	Clear Data	Clear Data	Clear Data
Tx Sync	Encrypted Data	Encrypted Data	Clock/Sync Tone	Clock/Sync Tone
Rx Encrypted	Decrypted Data	Decrypted Data	Clock	Clock
Rx Clear	Clear Data	Clear Data	Clock	Clock
Rx Notch Filter	Notch Filter Data	Decrypted Data	Decrypted Data	Notch Filter Data

Table 3 Summary of Digital-to-Analog Converter operation

The DVS200 has two PTT inputs and two PTT outputs. The polarity of these pins, i.e. whether the transmit mode is active on a high PTT or low PTT, is determined by the option pin PTTP (pin 84). In the following paragraphs it is assumed, for simplicity, that the PTT signal is active low.

As mentioned above, there are two PTT inputs; they are PTTIN (pin 65) and DPTTIN (pin 66). The PTTN input should be connected directly to the PTT signal. On some pieces of equipment, there is a delay between the PTT signal going active and the channel opening on the receive equipment. This can be due to any number of factors; squelch circuitry and voting systems are just two examples of channel opening delays. On PTT activation, the DVS200 transmits sync tones. It is imperative that the DVS200 in the receive equipment receives all of the sync tones, otherwise it may not synchronise correctly (the DVS200 must receive a minimum of 96 out of 128 periods of the sync tone transmitted by the Tx DVS200). It is therefore necessary to delay the transmission of the sync tones until the channel is open on the receiver. The input DPTTIN is used for this purpose. The sync tone is transmitted 118ms after DPTTIN goes active. If this is long enough for the receive channel to open, then DPTTIN should be connected directly to PTTIN. If this is not a long enough delay, a delay stage should be inserted between PTTIN and DPTTIN. Alternatively, if there is a signal available on the transmitting equipment that indicates that the channel is open, then this may be connected to the DPTTIN input (assuming it is the same polarity as the PTT signal).

Note that this delay should be on the active edge of the PTT signal only, otherwise the transmit channel will be held open for a time equal to that of the DPTTIN delay. A simple circuit for introducing a delay is shown in Fig. 18. The resultant timing is shown in Fig. 4.

Because of the nature of the encryption technique, there is a time delay, of approximately 236ms, between the speech input and the encrypted output. A consequence of this is, that when the user releases the PTT switch, there will still be speech stored in the DRAM waiting to be output. For this reason the DVS200 delays de-selecting the transmit mode of the transmitting equipment. This delay, PTT_{DEL} in Fig. 4, ranges from 236ms (one frame length) to 450ms, depending on the point in the frame at which the PTT switch is released.

The result of this is that there is a difference between the PTT input and the PTT output. So, the PTT signal that was previously connected to the transmitter cannot now be used; it must be disconnected and the DVS200's PTTOUT (pin 7) signal should be re-connected in its place.

The $\overline{PTT}$ output (pin 6) is an inverted version of PTTOUT, and can be used to control any analog switches that are needed to switch between the Rx and Tx speech channels.

PERIODIC SYNC

In transmit mode, the periodic sync circuitry automatically initiates the transmission of a sync tone at regular intervals. There are several problems that can be solved by utilising the periodic sync option. One is the problem of late entry into net. This phenomenon occurs when a receiver is turned on during a transmission. Normally, the user in this situation will be unable to recover encrypted speech correctly until another transmission has been initiated, i.e., another sync tone has been transmitted. With periodic sync, the maximum duration the late entry user will be out of synchronisation will be equal to just over the periodic sync interval.

Another problem that can be cured with periodic sync is that of multiple path reception. This occurs when the transmitter and/or receiver are mobile and results in varying time reference between the Tx and Rx DVS200s; thus causing synchronisation error. With periodic sync, this error will only persist until the next sync tone is received, so the periodic sync option is again beneficial.

The periodic sync option is implemented by connecting a resistor/capacitor time constant between the pins PERIOD (pin 13) and PEROUT (pin 14) as shown in Fig. 19. The periodic sync interval is then 190 times the RC time constant. If the periodic sync option is not required, then the PERIOD input should be tied to either V_{DD} or V_{SS}.

Note that the sync tones are transmitted at a particular point in a frame, so the intervals between each sync tone will not correspond exactly to the interval determined by the periodic sync RC; there may be an additional time of anything between 0 and 460ms, depending upon where in a frame the periodic sync operation is completed.

As mentioned earlier, the periodic sync also affects the device in receive mode. The periodic sync circuitry is used to detect whether the device is being used in encrypted mode during receive operation. If the Rx does not receive a sync tone within a period equal to that of twice the periodic sync interval, the device switches to clear speech mode. It remains in this state until it either receives a sync tone, or PTT goes active (assuming the $\overline{CVOICE}$ pin is not active, i.e. high).

If this automatic override is not required, then the periodic sync option should not be selected in receive mode.

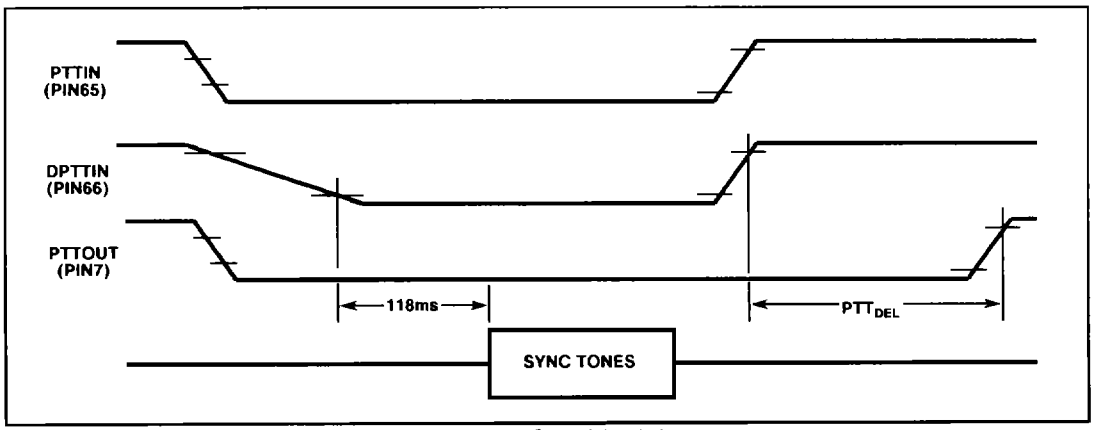


Fig. 4 PTT to Sync delay timing

SEED DATA ENTRY

Before the DVS200 can perform any encryption function seed data has to be loaded into the code storage registers in the SRAM. With this seed data the key generator can be used to derive a sequence of segment transpositions. This seed data then is the code that must be inserted into the DVS200, of both the Tx and Rx user, before the encrypted speech can be correctly recovered. There are several different ways of entering the code. These can be divided into two categories; automatic strobe, and external strobe. Both of these should be performed immediately after the device has been reset ($\overline{FRES}$ active).

Seed Data Entry - Automatic Strobe

With this method the seed data is loaded automatically from an external bank of switches. It is selected by tying the KINJ input (pin 63) to V_{SS}. It has the advantage of removing the necessity for battery back-up facilities, as the switches are always present on the seed data input port. So, whenever the device is reset, the switches are simply read into the code storage registers.

The switches must be arranged in banks of four, and can be any multiple from four to sixteen. The four switch option gives low security (16 possible codes) but uses a smaller amount of board space (see Fig. 20). The inverse is true of the sixteen switch configuration; it offers greater security (65336 possible codes), but this occupies greater board area. The decision about the number of switches to be used for code entry is, therefore, mainly governed by the amount of board space available, and the degree of security required.

One of the terminals of each switch in each bank is connected to one of the inputs on the seed data input port, SD0-SD3 (pins 76, 77, 78, 79). This connection should be made via a diode if the number of switches is greater than four (see Fig. 21). The other terminals are then grouped together in their respective banks. If there is more than one bank of four switches each bank should be connected to one of the seed strobe outputs. $\overline{SSTB0}$-$\overline{SSTB3}$ (pins 59, 60, 61, 62); otherwise these terminals should be connected to V_{SS} (see Fig. 20). Each one of these four strobe outputs must be connected to a bank of switches (if more than four switches are used). If an eight or twelve switch configuration is used some of the $\overline{SSTB}$ outputs should be connected together, ensuring that the number of strobe nodes is equal to the number of switch banks (see Fig. 21). The timing diagram for automatic seed data entry is shown in Fig. 9.

Seed Data Entry - External Strobe

This method of seed data entry is selected by tying the KINJ input (pin 63) to V_{DD}. The main advantage of this method of seed data entry is that there is a total of 128 bits (entered as 32 nibbles) of seed data. This gives approximately 3.4×10^{38} possible permutations. To enter the code in this method a nibble is placed on the seed data entry port, and then strobed into the DVS200 using the $\overline{ISTRB}$ input (pin 64 - active on the negative edge). This is repeated for each of the 32 nibbles. With this method of seed data entry the contents of the SRAM must be retained (using battery back-up) each time the DVS200 is powered down, otherwise the codes will be lost (see Seed Data Override below)

There are two ways to implement this. The first is to use a key fill gun; this supplies the necessary data and strobe signals via an external connector. The other way to do this is to use external logic to access a PROM (32×4 minimum) each time the DVS200 is reset. The necessary timings for strobe controlled seed data entry are shown in Fig. 10.

Seed Data Paging

When an SRAM with excess capacity is used (i.e. greater than 128×4), it is possible to utilise the remaining space to supply the user with a choice of codes. This is achieved by connecting a set of switches to the extra address pins available on the SRAM. Each one of the different switch settings will address a different page of 128×4 (the normal block used by the DVS200). Each one of these pages can be used to hold a different set of codes that can be selected by altering the switch settings.

This means, of course, that each page has to have a code loaded into it. This is done by resetting the DVS200 several times (thus loading seed data), changing the page address and seed data each time the device is reset. The sequence of events for paged data loading is shown in Fig. 5.

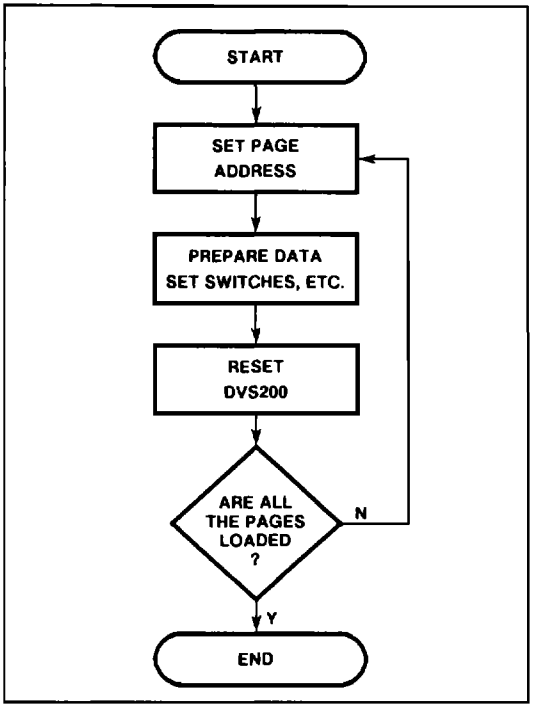


Fig 5 Loading Paged Seed Data

If the seeding is being done using the external strobe option, the $\overline{FRES}$ pulse can be supplied by either the keyfill gun, or the external logic, depending on which is being used. If automatic seeding is selected, the $\overline{FRES}$ pulse can be supplied by an external push-button switch. This is then pressed each time the switches have been correctly set to their new settings (both the seed data and page addresses).

When the paging option is used, the automatic seeding option (described under Automatic Strobe, above) will also have to have battery back-up on the SRAM. If this is not done, each page will have to be re-loaded each time the DVS200 is powered down.

Seed Data Override

In some applications it may not be desirable to load seed data each time the DVS200 is reset (when the device is powered-up). The code may be loaded into the device by a master keyfill gun at the beginning of the day and then retained, during power down phases, by battery back-up on the SRAM (this also applies to paged data).

Each time seed data entry is required, the SEED input pin (pin 81) must be taken high either before or during device reset (see under PTT Circuitry on page 4-10 and External Strobe, above). Once the code entry has been completed the seed input can then be taken low. This will then inhibit the device from overwriting the stored codes on each subsequent device reset.

TIMING DIAGRAMS

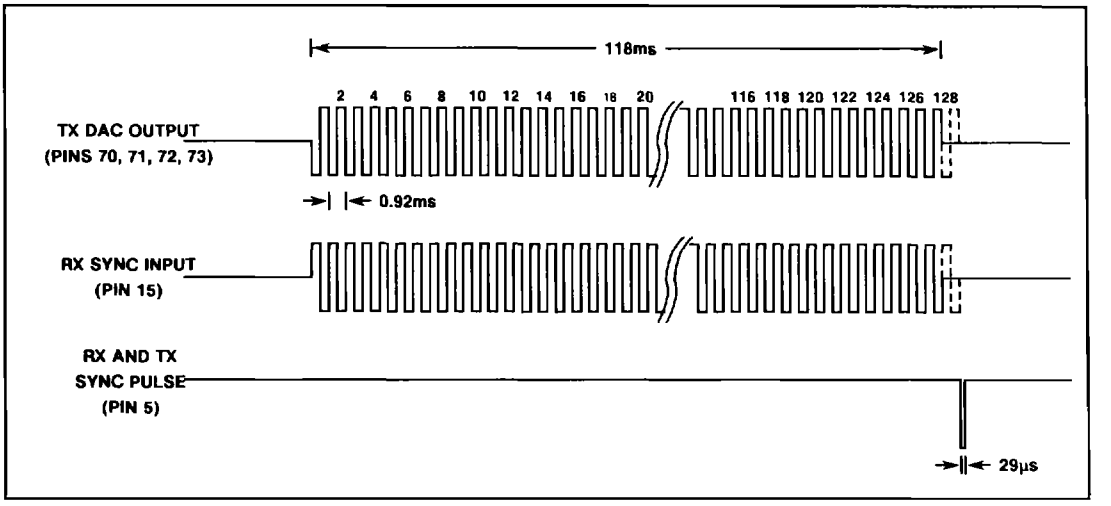


Fig.6a Synchronisation (no Message Key)

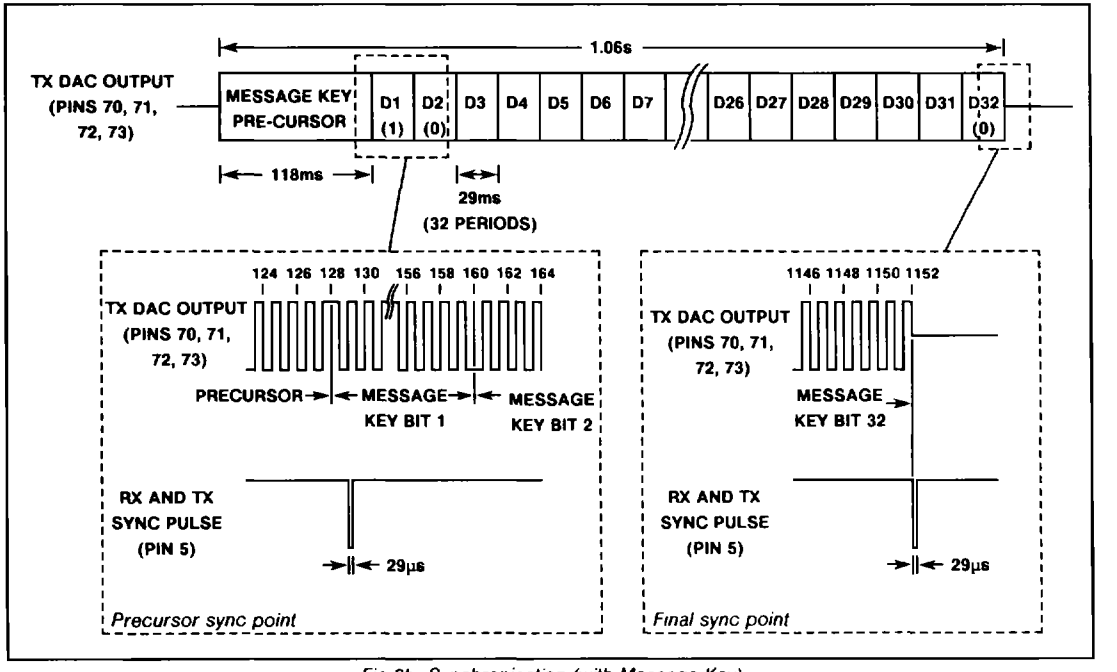


Fig.6b Synchronisation (with Message Key)

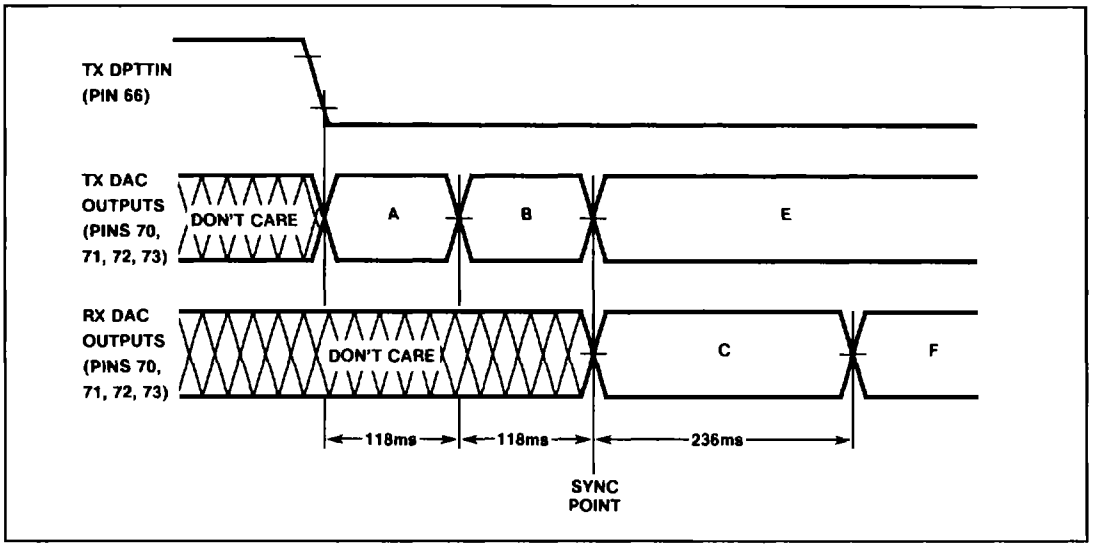


Fig.7a DAC operation (no Message Key)

Figs. 7a and 7b Key

A - Attenuated speech
B - Sync Tones with attenuated speech
C - Notch Filter
D - Message Key with attenuated speech
E - Normal Tx operation
F - Normal Rx operation (Attenuated)

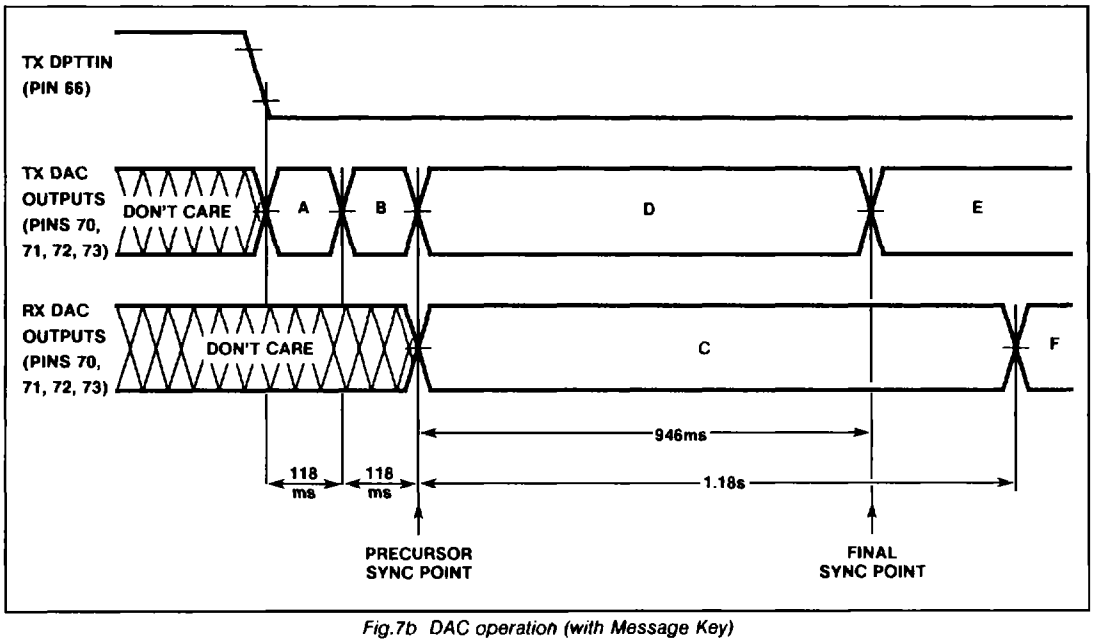


Fig.7b DAC operation (with Message Key)

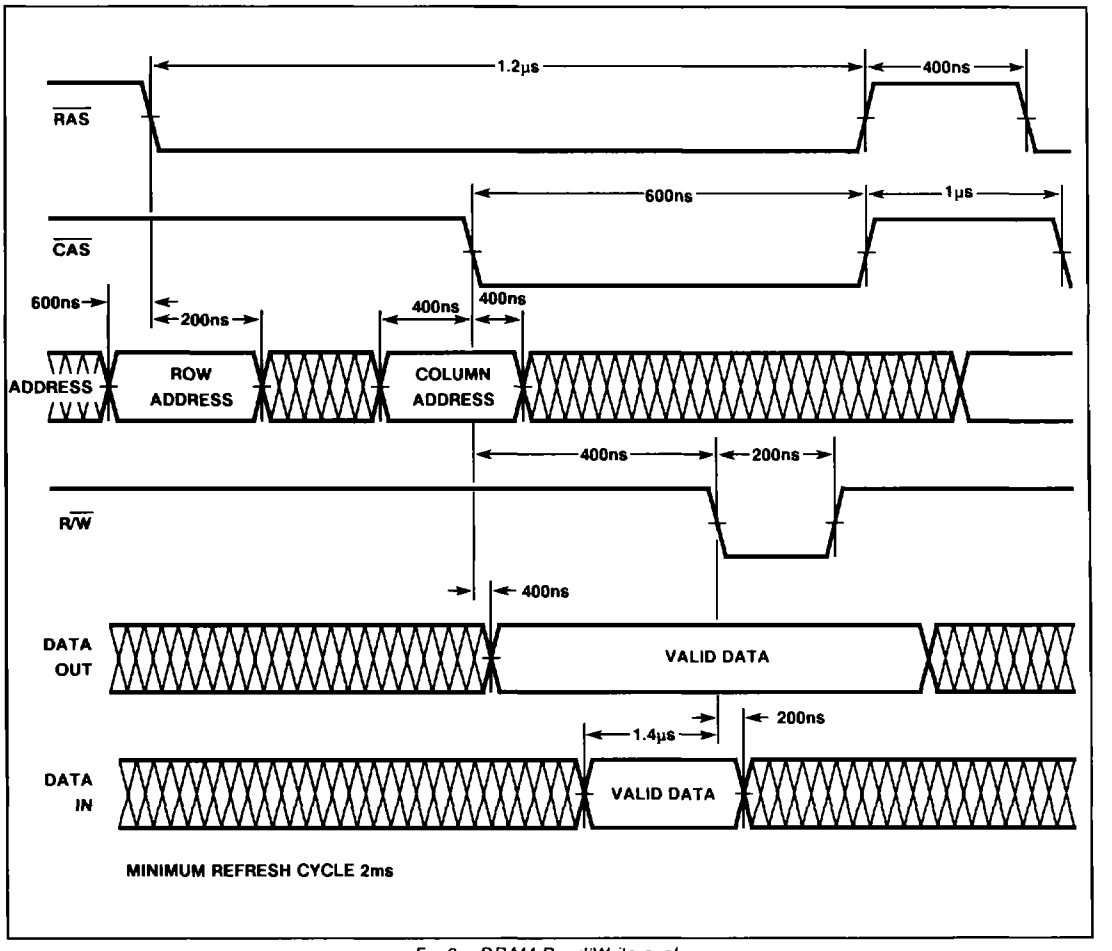


Fig.8a DRAM Read/Write cycle

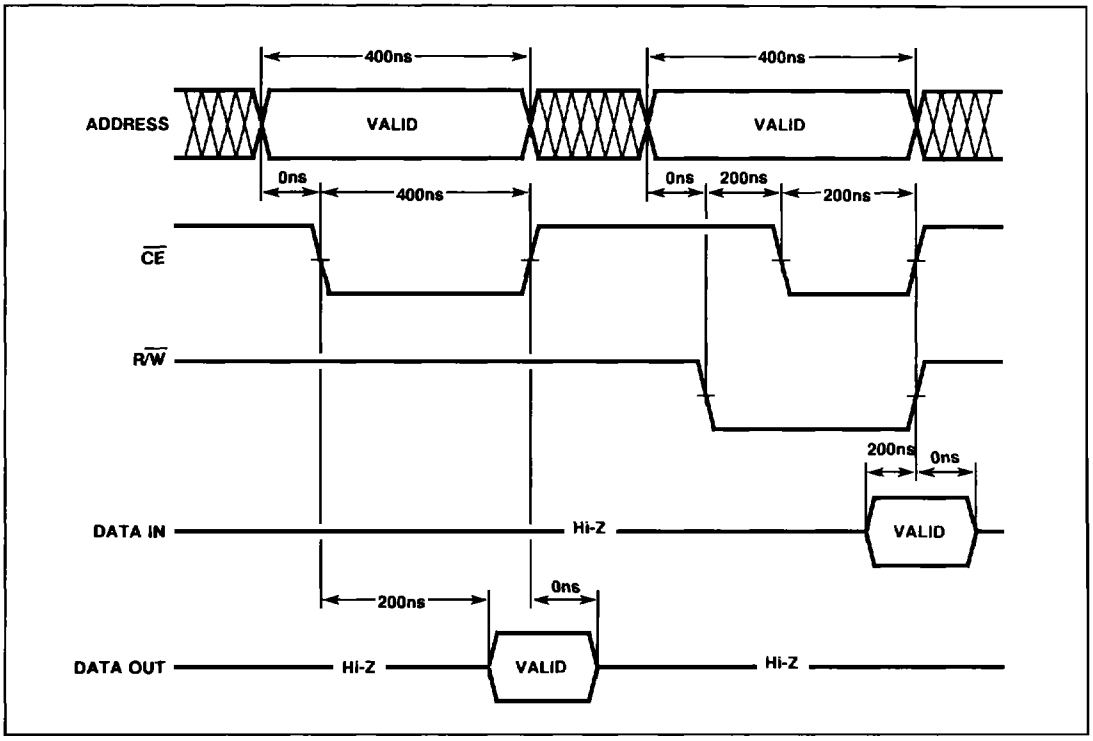


Fig.8b SRAM read/write cycle

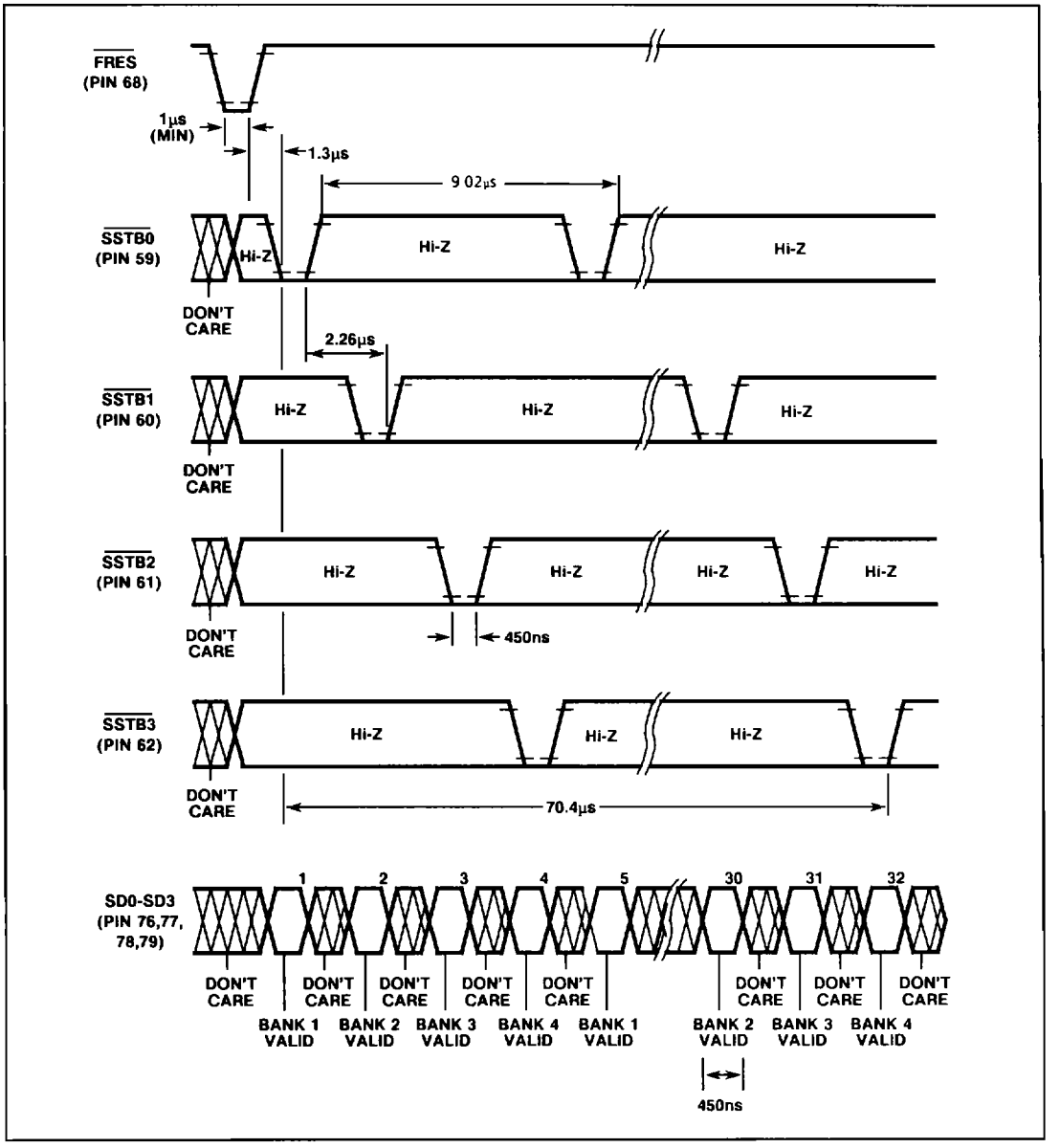


Fig.9 Automatic seed data entry timing

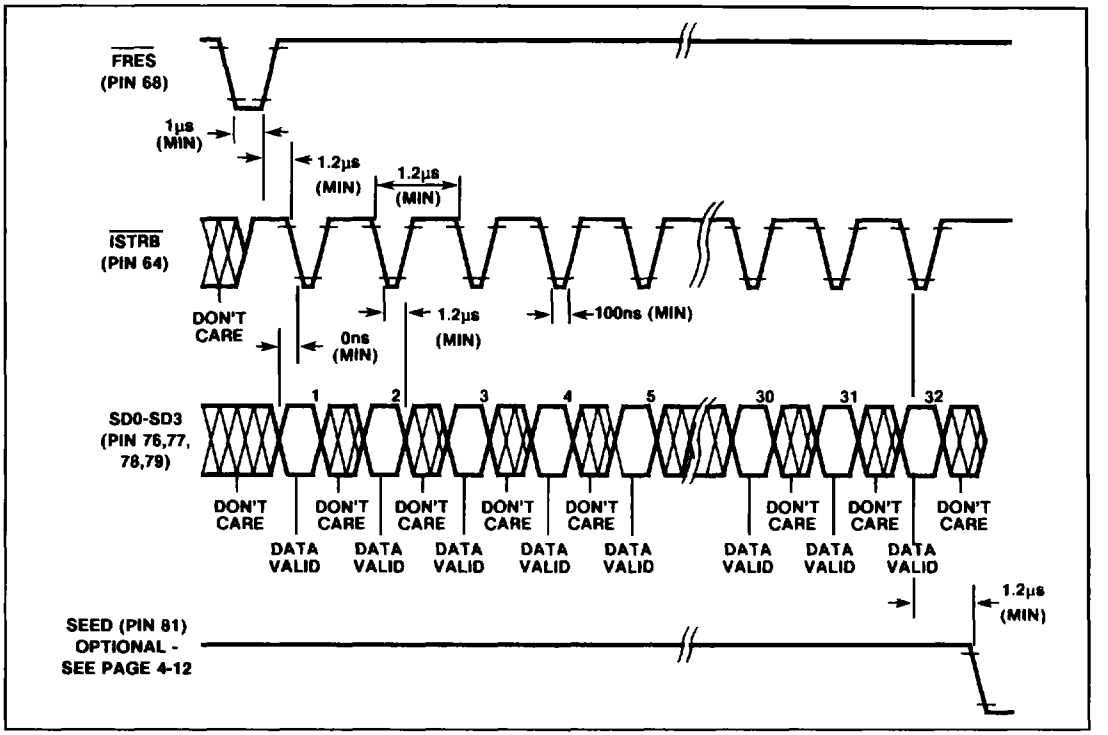


Fig.10 Strobe-controlled seed data entry timing

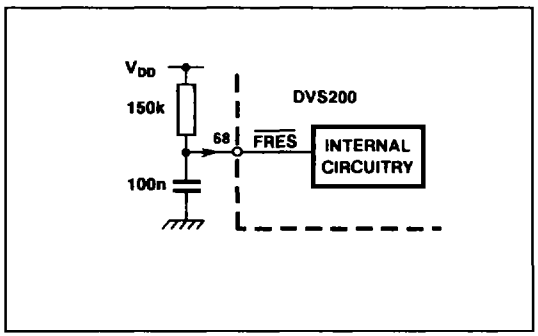


Fig.11 Device reset

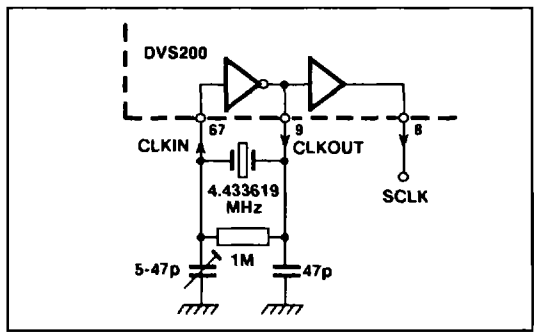


Fig.12 Clock oscillator

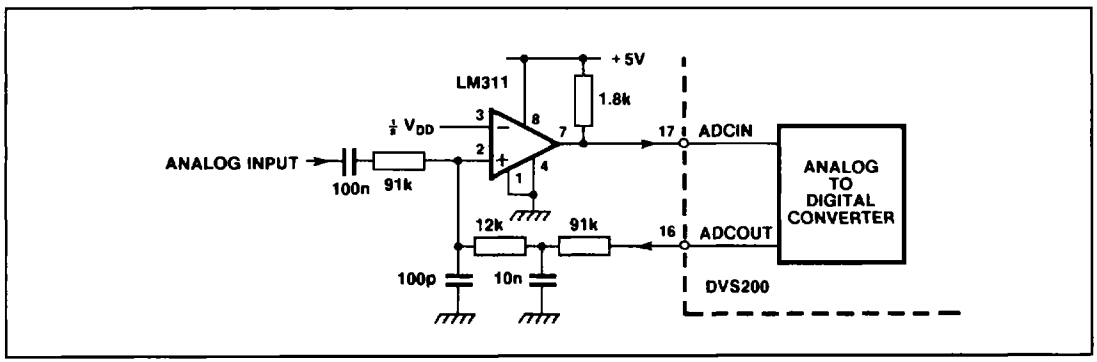


Fig.13 ADC external circuitry

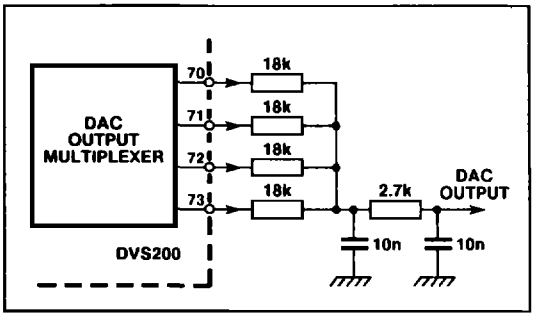


Fig.14 Digital to analog converter

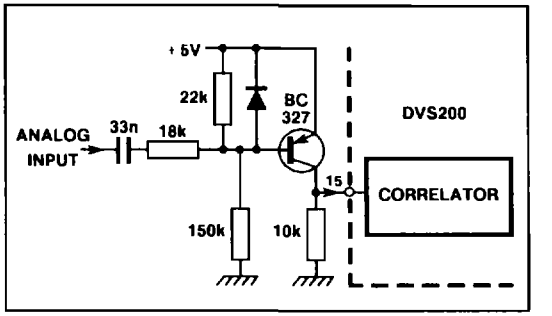


Fig.15 Sync tone inverter

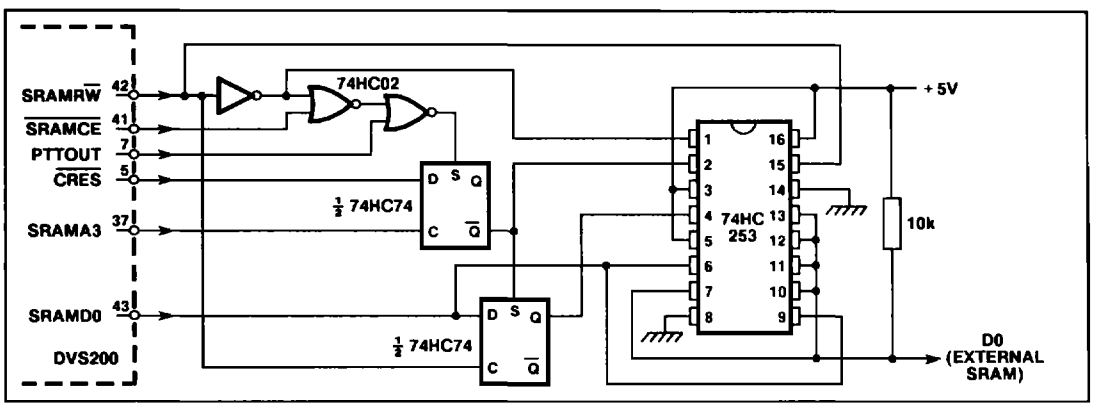


Fig.16 Tx message key circuitry

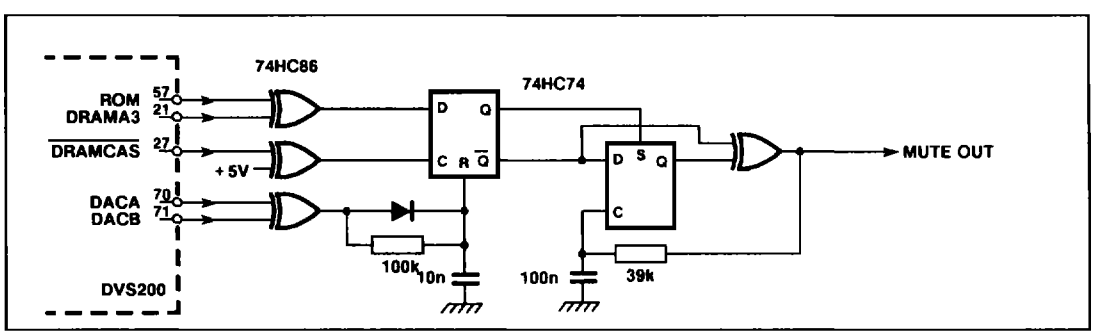


Fig.17 Rx message key circuitry

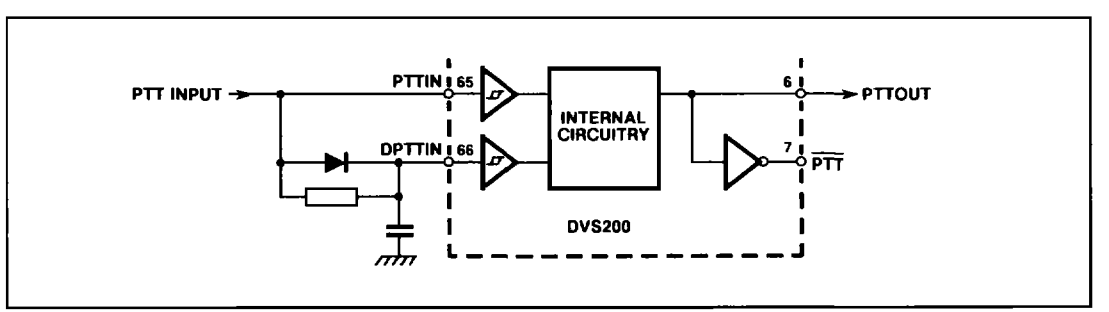


Fig.18 PTT to sync delay circuit

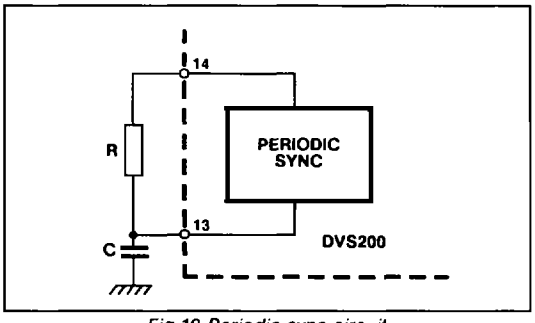


Fig.19 Periodic sync circuit

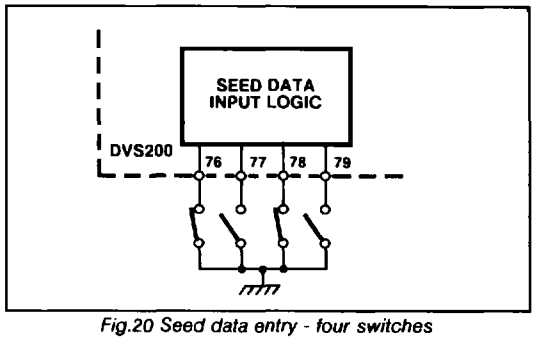


Fig.20 Seed data entry - four switches

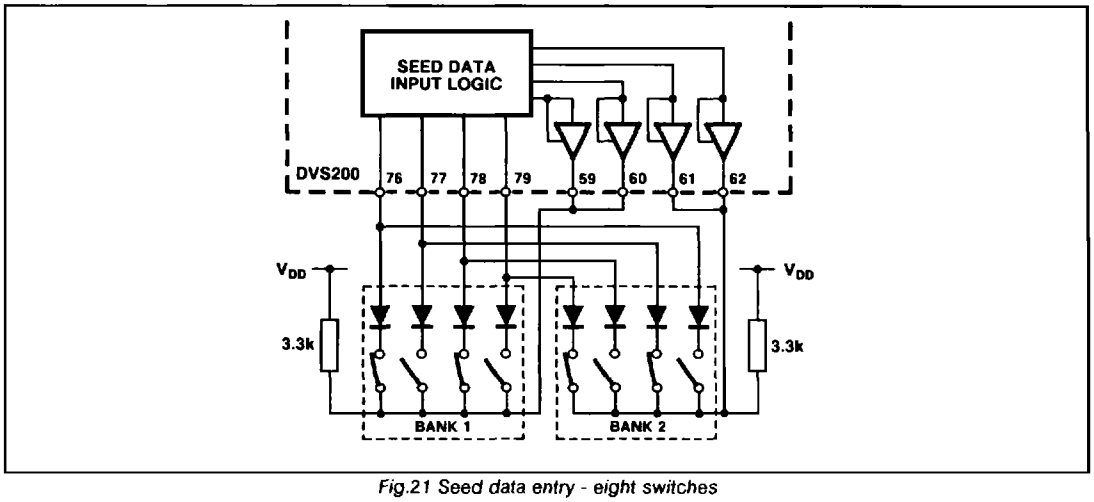


Fig.21 Seed data entry - eight switches

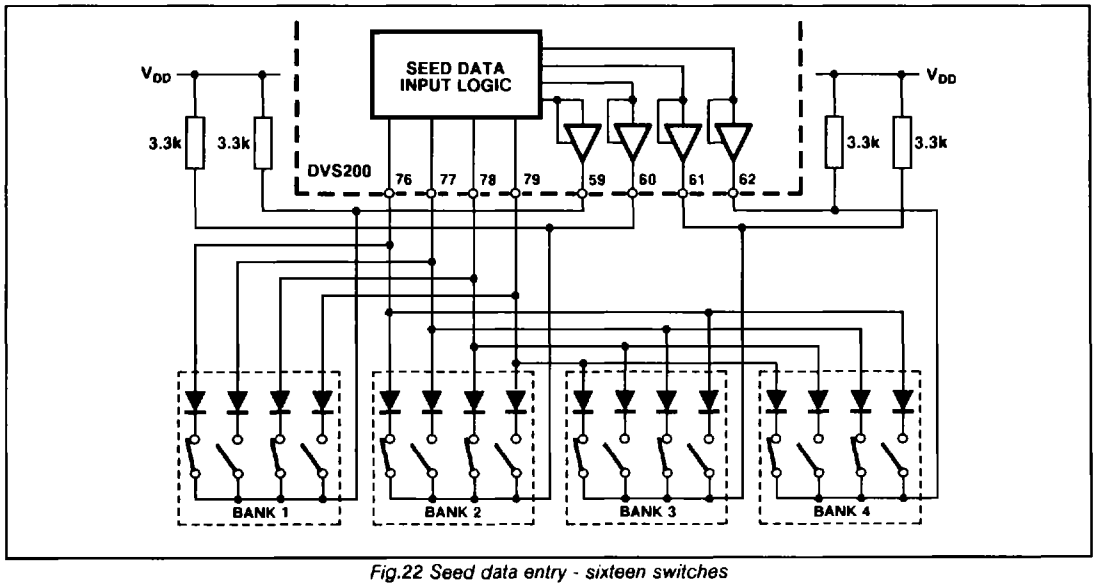


Fig.22 Seed data entry - sixteen switches

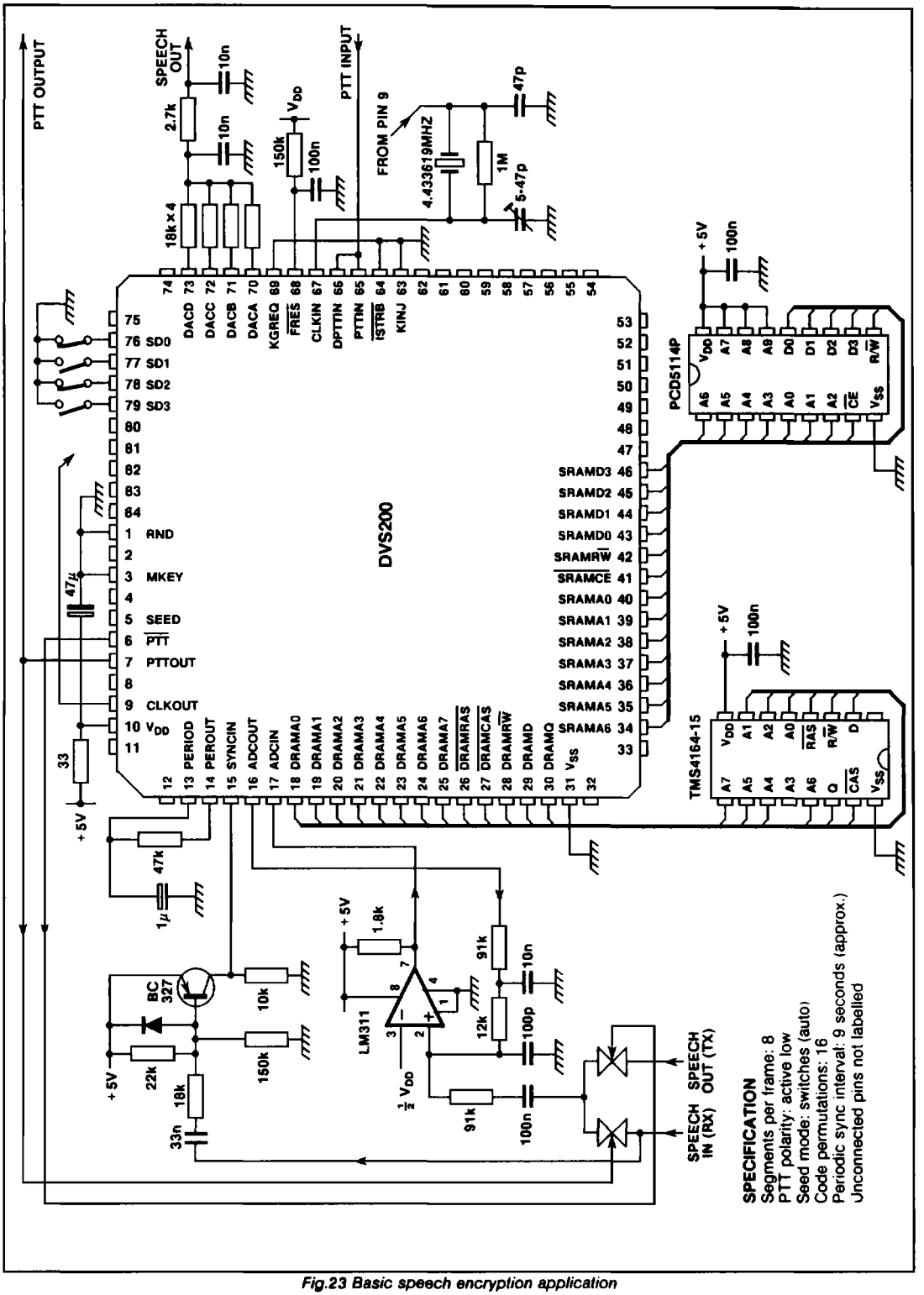


Fig.23 Basic speech encryption application

DATA ENCRYPTION

OVERVIEW

The DVS200 has a data encryption mode which can be selected by connecting the option pin KGOP (pin 83) to V_{SS}. When in this mode, the output of the DVS200's on-chip key generator can be used to encrypt a low-bandwidth data stream.

The data stream is encrypted by modifying each bit of data before it is transmitted. The modification of the bit is determined by the pseudo-random output of the DVS200's key generator, and is usually achieved with the modulo-2 addition of the data stream to the key generator output, using an EXOR gate. The output of this gate is the encrypted data stream and can, therefore, be transmitted over the vulnerable network or link. The data is recovered by simply repeating the procedure at the receive end.

BASIC OPERATION

Before data encryption can begin, there are three operations that need to be performed. The first requirement is that the DVS200's is reset by activating the $\overline{FRES}$ pin (see page 4-9). The second phase is that the code storage registers are loaded with the seed data; this happens automatically whenever the DVS200 is reset. The details of this operation are described on page 4-12. Once this has been done the seed data in the code storage registers needs to be transferred to the key generator. In the speech encryption mode this is usually done when synchronisation occurs. In data encryption mode this can be simulated by taking the PTTIN and DPTTIN pins low (see pages 4-10 and 4-11) for at least 240ms. Each time the DVS200's key generator is reseeded (i.e., the key generator is reset) it is essential that the first and third phases of the initialisation process (device reset and synchronisation) are performed. If the seed data has already been entered, the second phase can be omitted by activating the SEED option pin (see Seed Data Override, page 4-12). The flow diagram of Fig. 24 shows the key generator initialisation sequence.

Just before a data bit is ready to be transmitted, a word should be requested from the DVS200's key generator. This is achieved by strobing KGREQ (pin 69). A number of clock cycles after the falling edge of KGREQ, the key generator will indicate the presence of a valid four bit word on the key generator output port (KGD0-KGD3) with a logic '0' on the $\overline{KGRDY}$ output. The timing for the signals involved with a request for a word from the key generator is summarised in Fig. 25.

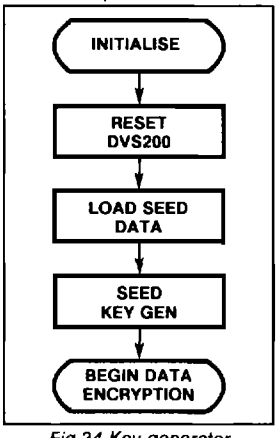


Fig.24 Key generator initialisation sequence

The key generator output is in the form of a four bit word; usually, the data to be encrypted is in serial form. If this is the case, the output of the DVS200's key generator should be loaded into a four-bit shift register; the shift register should then be clocked each time one of the bits from the nibble is required. It is, therefore, only necessary to request a word from the key generator every fourth bit in the data stream. A circuit diagram illustrating the implementation of this basic data encryption application is shown in Fig. 26. A timing diagram showing the relevant signals for this application is shown in Fig. 27. Note that in this application, the external DRAM is omitted as it is only required for storing sections of speech in the speech encryption mode. The DRAMQ input (pin 30) is therefore connected to V_{SS}.

DATA RATES

Unbuffered Key Generation

Because of the nature of the DVS200's key generator, the time that elapses between a KGREQ strobe and a valid output appearing on the key generator output port is variable. It is the time that elapses between these two events that determines the maximum rate at which the key generator can be accessed, and hence the maximum data rate that can be encrypted.

If a clock of fixed period is used to strobe the KGREQ pin, and no form of storage buffer is used (other than the four bit shift register), the minimum period of this clock must be equal to the maximum possible time taken to complete a key generator operation. If the four-bit shift register is loaded before $\overline{KGRDY}$ strobes low (key generator operation complete), erroneous data will be read from the key generator output port.

The maximum time taken to complete a key generator operation is equivalent to 9100 times the period of the device clock. So for a clock of 4.433619MHz:

Maximum time for Key Generator Operation
$= 9100 \times 225.5\text{ns}$
$= 2.05\text{ms}$
$\therefore$ Max number of Key Generator operations per second
$= (1/2.05) \times 10^3$
$= 487$
As the key generator outputs four bits:

Equivalent Data Rate
$= 4 \times 487\text{bits/s}$
$\approx 1.9\text{kbits/s}$

This means in this system the DVS200 can encrypt data streams operating at data rates of up to 1.948kbits/s. If the device clock were to be increased to 6MHz, the DVS200 could encrypt data streams at rates of up to 2.637kbits/sec.

Buffered Key Generation

Buffered key generation is a method of increasing the data encryption rate possible with the DVS200.

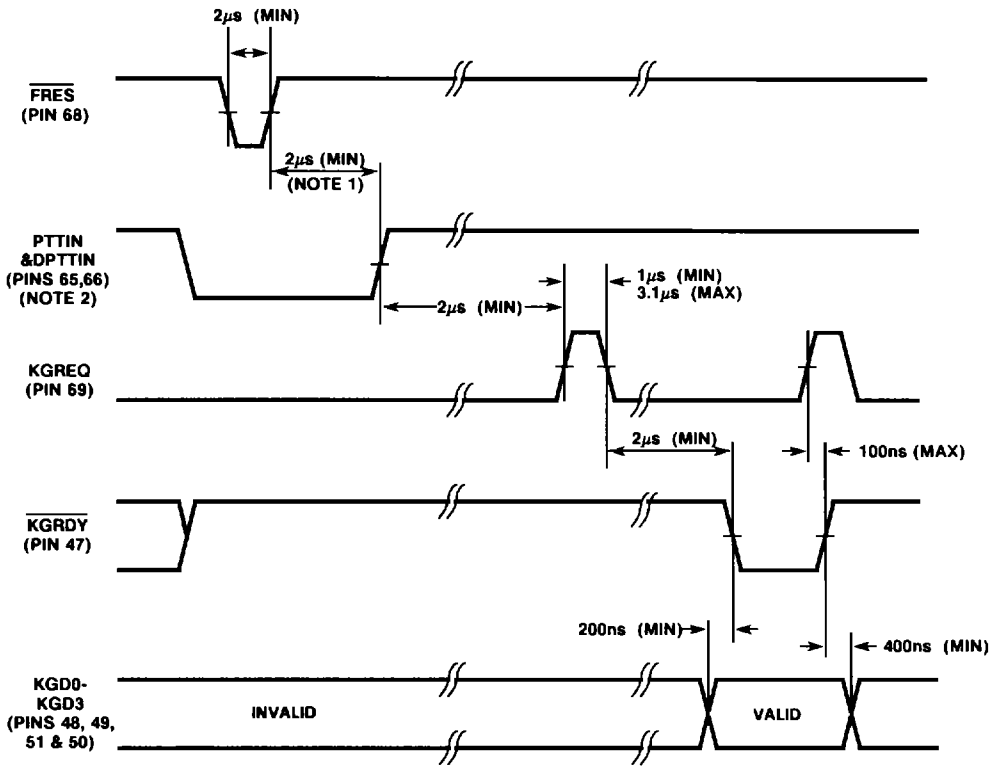
In this mode, the key generator is allowed to 'free-run' This is achieved by connecting the KGREQ input to the $\overline{KGRDY}$ output via an inverting gate. The 'free-running' mode is controlled by an externally supplied logic signal which is gated with $\overline{KGRDY}$. Once 'free-running', words will appear on the key generator outputs at variable intervals. These words can then be buffered externally and clocked out of the buffer at a fixed rate equal to the *average* time taken to complete the key generation cycle. This method gives an 86% increase in the equivalent data rate over the method described above for only a small increase in the amount of external logic required.

The average key generation cycle time is equivalent to 4900 times the period of the device clock. For a clock of 4.433619MHz:

Average time for Key Generator operation
$= 4900 \times 225.5\text{ns}$
$= 1.1\text{ms}$
$\therefore$ Possible number of Key Generator operations per second
$= (1/1.1) \times 10^3$
$= 909$
As the key generator outputs four bits:

Equivalent Data Rate
$= 4 \times 909\text{bits/s}$
$\approx 3.6\text{kbits/s}$

Hence, with a storage buffer, the DVS200 can encrypt data streams at rates of up to 3.6kbits/s, (or up to 4.8kbits/s with a device clock of 6MHz).



NOTES
1. The figure quoted applies when no seed data is to be entered (battery back-up). If seed data is to be entered, this time should be equal to the time taken to enter the seed data (see Seed Data Entry, page 4-12).
2. PTT is selected to be active high (PTTP tied low).

Fig.25 Key generator timing diagram.

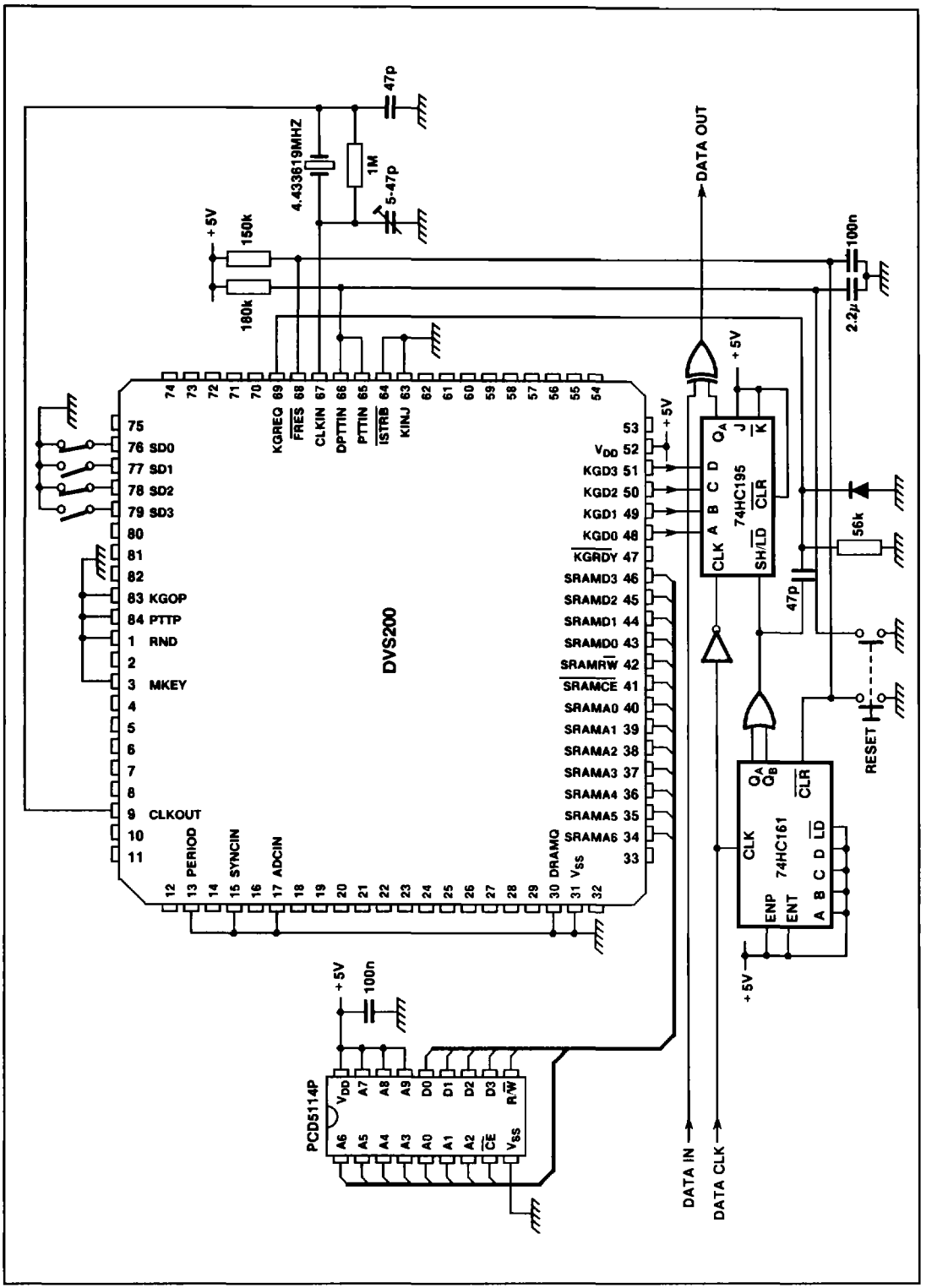
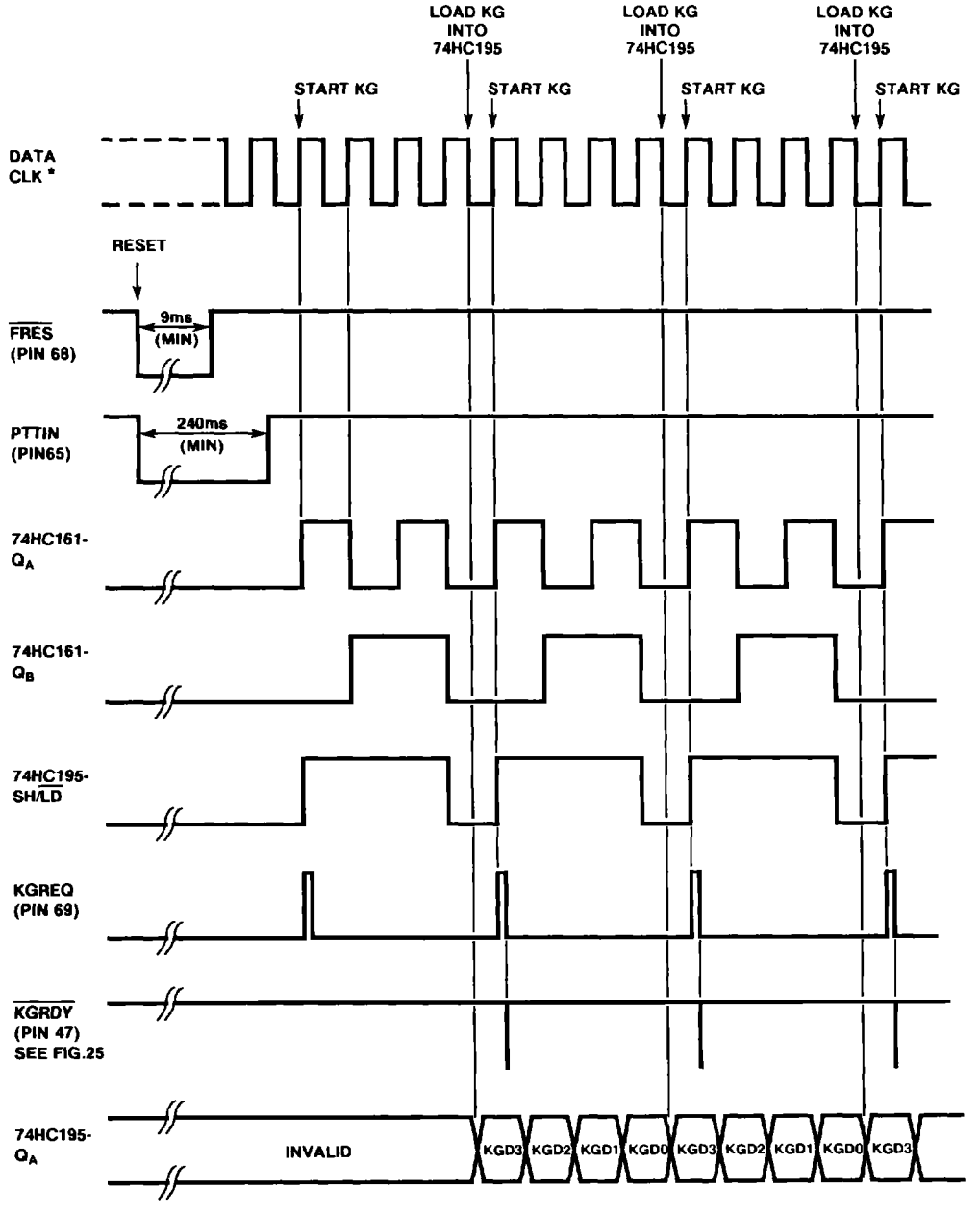


Fig.26 Basic data encryption application (unbuffered key generation - see text, page 4-22)



* NOTE: For a 4.433619MHz crystal, the data clock frequency must not exceed 1.9kHz (see page 4-22)

Fig.27 Timing diagram for data encryption application, Fig. 26

ELECTRICAL CHARACTERISTICS

Test conditions (unless otherwise stated):
V_{DD} = 5V ± 10%, T_{AMB} = – 40°C to + 85°C

Characteristic	Symbol	Value			Units	Conditions
		Min.	Typ.	Max.		
Supply voltage	V_{DD}	3	-	7	V	
Power supply current	I_{DD}	-	5	-	mA	V_{DD} = 5V
TTL input high voltage	V_{IH1}	2	-	-	V	
TTL input low voltage	V_{IL1}	-	-	0.8	V	
TTL Input leakage current	I_{IL1}	-	-	10	μA	$V_{IN} = V_{SS}$ or V_{DD}
TTL Tri-state leakage current	I_{OZ}	-	-	10	μA	$V_{IN} = V_{SS}$ or V_{DD}
Schmitt input high voltage	V_{IH2}	-	3.2	-	V	
Schmitt input low voltage	V_{IL2}	-	1.8	-	V	
Schmitt input leakage current	I_{IL2}	-	-	10	μA	
Output high voltage	V_{OH}	2.4	-	-	V	I_{OH} = – 2mA
Output low voltage	V_{OL}	-	-	0.4	V	I_{OL} = 4mA
Input pullup resistance	-	-	10	-	kΩ	

ABSOLUTE MAXIMUM RATINGS

Supply voltage, V_{DD}	10V
Voltage on any pin	V_{SS} – 0.3V to V_{DD} + 0.3V
Short circuit output current	10mA
Power dissipation	1W
Storage temperature	– 65°C to + 150°C
Operating temperature range	– 40°C to + 85°C

Stresses above those listed in the Absolute Maximum Ratings may cause permanent damage to the device. These are stress ratings only and functional operation of the device at these conditions, or at any other condition above those indicated in the Electrical Characteristics, is not implied. Exposure to Absolute Maximum Rating conditions for extended periods may affect device reliability.

FUNCTIONAL SPECIFICATION

All figures quoted at V_{DD} = 5V ± 10%, f_{CLK} = 4.433619MHz

Encryption	
Technique	TDM and time inversion
Frame length	236ms
Segments per frame	8/16 (option)
System delay	236ms per end
A to D Conversion	
Conversion method	Adaptive Delta modulation
Sample rate	139kbits/s
Average input signal level	1.7Vp-p
Dynamic range	40dB
Idling noise	10mV
SNR (1kHz at 1.7Vp-p)	45dB
Psophometric noise	Better than – 45dBm

Key Generator	
Sequence length	1.329 × 1036
Sequence number	260
Key variable entry (switches)	16 bits
Key variable entry (keyfill; gun)	1228 bits
Synchronisation	
Sync tone frequency	1.082 kHz
Sync tone decoding	Correlation
Periodic sync	Period variable (external RC)
No. of message key bits	32
Message key modulation	Phase