Marconi
Electronic Devices

DVS200

SPEECH ENCRYPTION PROCESSOR

Features

- Complete data encryption system on a chip.
- Excellent voice 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 upto 4.8Kbits/sec.

General Description

The DVS200 is a digital speech encryption processor, on a single custom-designed VLSI chip, that implements a 'TDM' (Time Division Multiplexing) encryption algorithm enabling encryption of data at upto 4.8kBits/sec. The device can be used to protect virtually any vulnerable speech 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.

The DVS200 is a complete system on a chip that only requires a DRAM, SRAM and a few additional passive components for basic operation.

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

The 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.

The information presented herein is to the best of our knowledge true and accurate. No warranty expressed or implied is made regarding the capacity, performance or suitability of any product. You are strongly urged to ensure that the information given has not been superseded by a more up to date version

Marconi Electronic Devices Ltd.
IC Division,
Doddington Road,
Lincoln LN6 3LF, **England**
Tel: (0522) 500500
Telex: 56380
Fax: (0522) 500550

Marconi Circuit Technolgy Corp.
45 Davids Drive,
Hauppauge,
New York 11788, **USA**
Tel: (516) 231 7710
Telex: 275801
Fax: (516) 231 7923

Marconi Electronic Devices, s a
2 Rue Henri Bergson,
92600 Asnières
France
Tel: (1) 4 7 33 51 45
Telex: 612850
Fax: (1) 47 33 11 31

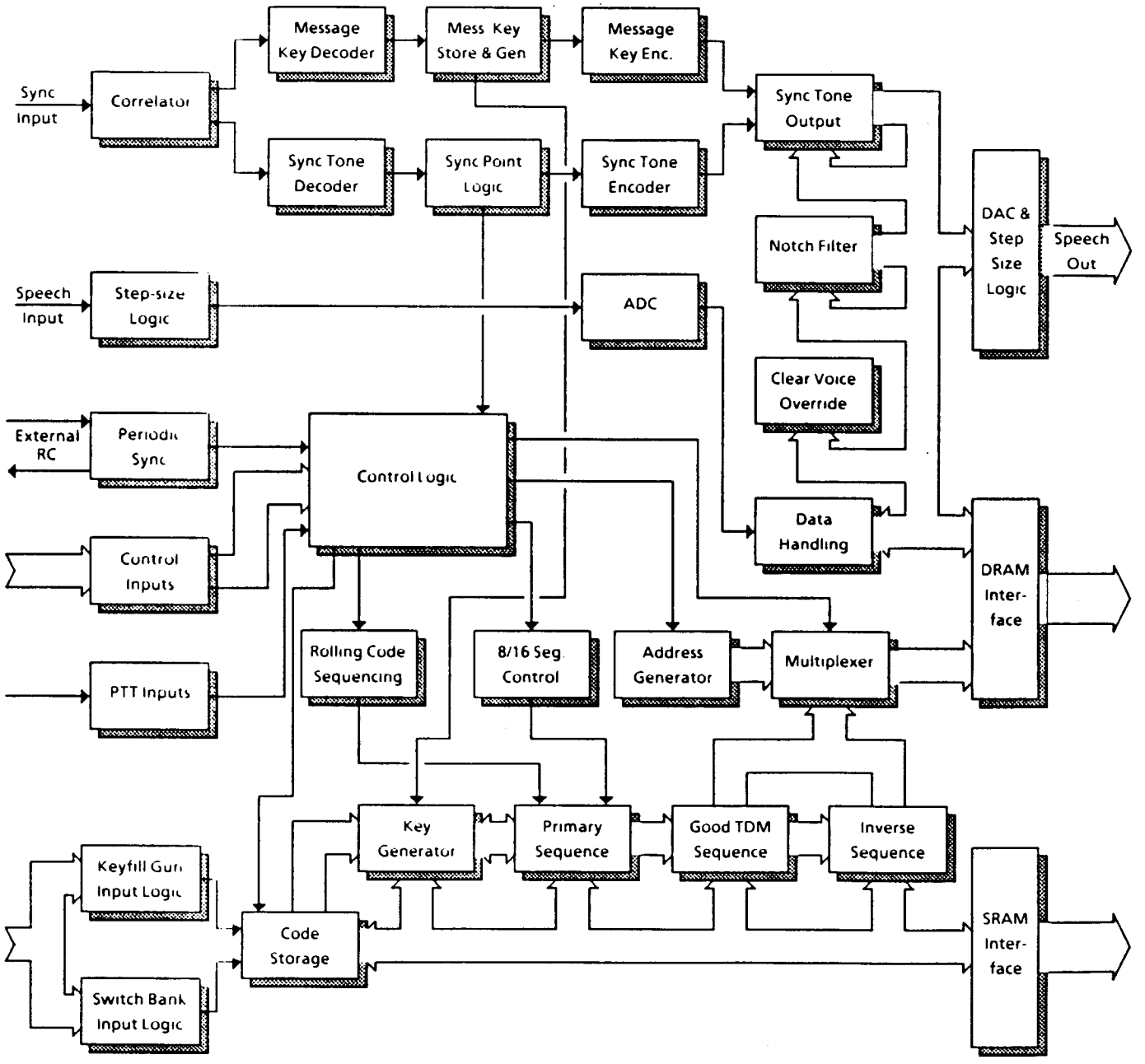
Marconi Electronik
Landsberger Strasse 65
8034 Germering
Germany
Tel: 089/849 36-0
Telex: 5 212 642
Fax: 089/841 91 42

C754D Iss 1 May' 89

DVS200

SPEECH ENCRYPTION PROCESSOR

Block Diagram



PIN	NAME	TYPE	DESCRIPTION
1	RND	I	Input for the source of the message key data.
2	CVOICE	IP	Clear voice override pin. When a logic 1 is applied the device is in secure mode. When a logic 0 is applied, the device outputs unencrypted speech.
3	MKEY	IP	Used for selecting the message key option. A logic 1 enables the device, a logic 0 disables it.
4	NRND	O	This is a latched, inverted version of pin 1 (RND. It can be used, together with pin 1, to provide a random data stream for the message key.
5	CRES	O	Test pin - Pulses low when the device synchronises.
6	NPTT	O	Inverted version of pin 7 (PTTPOUT).
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 pin 9 (CLKOUT). Used for setting the device's clock frequency.
9	CLKOUT	O	Used, together with pin 67 (CLKIN), to form the device's clock oscillator.
10	VDD	I	+ 5V
13 14	PERIOD PEROUT	SI O	These two pins are used to form the oscillator that determines the period of the periodic sync.
15	SYNCIN	SI	Received sync tone input.
16 17	ADCOUT ADCIN	O I	The analog to digital converter is formed around these two pins
18 19 20 21 22 23 24 25	DRAMA0 DRAMA1 DRAMA2 DRAMA3 DRAMA4 DRAMA5 DRAMA6 DRAMA7	O O O O O O O O	DRAM Address bus
26 27 28	DRAMRAS DRAMCAS DRAMRW	O O O	DRAM Control bus
29	DRAMD	O	Connect to DRAM data input.
30	DRAMQ	I	Connect to DRAM data output.
31	VSS	I	0V
34 35 36 37 38 39 40	SRAMA6 SRAMA5 SRAMA4 SRAMA3 SRAMA2 SRAMA1 SRAMA0	O O O O O O O	SRAM Address bus
41 42	SRAMCE SRAMRW	O O	SRAM Control bus.
43 44 45 46	SRAMDO SRAMD1 SRAMD2 SRAMD3	BP BP BP BP	SRAM Data bus.
47	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.

KEY TO PIN TYPE
I-Input, IP-Input with pullup, SI-Schmitt input, O-Output, TO-Tri-state output, BP-Bidirectional output with pullup

Table 1. Pin Description

PIN	NAME	TYPE	DESCRIPTION
48 49 50 51	KGD0 KGD1 KGD2 KGD3	O O O O	Key generator output port
52	VDD	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	SSTB0 SSTB1 SSTB2 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	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 (ie 0 or 1) is determined by pin 84 (PTTP).
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	Used, together with pin 9 (CLK-OUT), to form the clock oscillator
68	FRES	SI	Device reset (active low).
69	KGREQ	I	When in data encryption mode, this pin is strobe (active high) to request a key generator word.
70 71 72 73	DACA DACB DACC DACD	O O O O	Digital to analogue converter outputs.
74	VSS	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 funciton. This enables seed data already present in the SRAM, due to battery back-up for example, to be retained. So the device can 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.

KEY TO PIN TYPE
I-Input, IP-Input with pullup, SI-Schmitt input, O-Output, TO-Tri-state output, BP-Bidirectional output with pullup
Note: Please tie all unused inputs to either VDD or VSS.

Table 1 Pin Description (continued)

PIN	NAME	LOGIC 0	LOGIC 1
2	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 pin 63-KINJ) have internal pullups. So, if a logic 1 is desired, the pin should simply be left unconnected.

Table 2. Summary of Options

1.0 Overview of Operation

1.1 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 Figure 1 demonstrates the effect that the DVS200 would have on a signal that had a ramped envelope.

You will notice two things from figure 1. First, that the signal is delayed by an equivalent of one frame, i.e. 236msec (this figure is valid for the nominal device clock of 4.43MHz). This means that there will be a system delay of 472msec (236msec for encrypt and 236msec for decrypt). The second thing to notice, is that, in figure one, 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.

1.2 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 in the sequence, is determined by the seed data (code) that has been entered by the user. This code can be any one of approximately $3x10^{38}$ 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 figure 1 (A5,A8,A2,A4,A6,A1,A7,A3) is eminantly suitable.

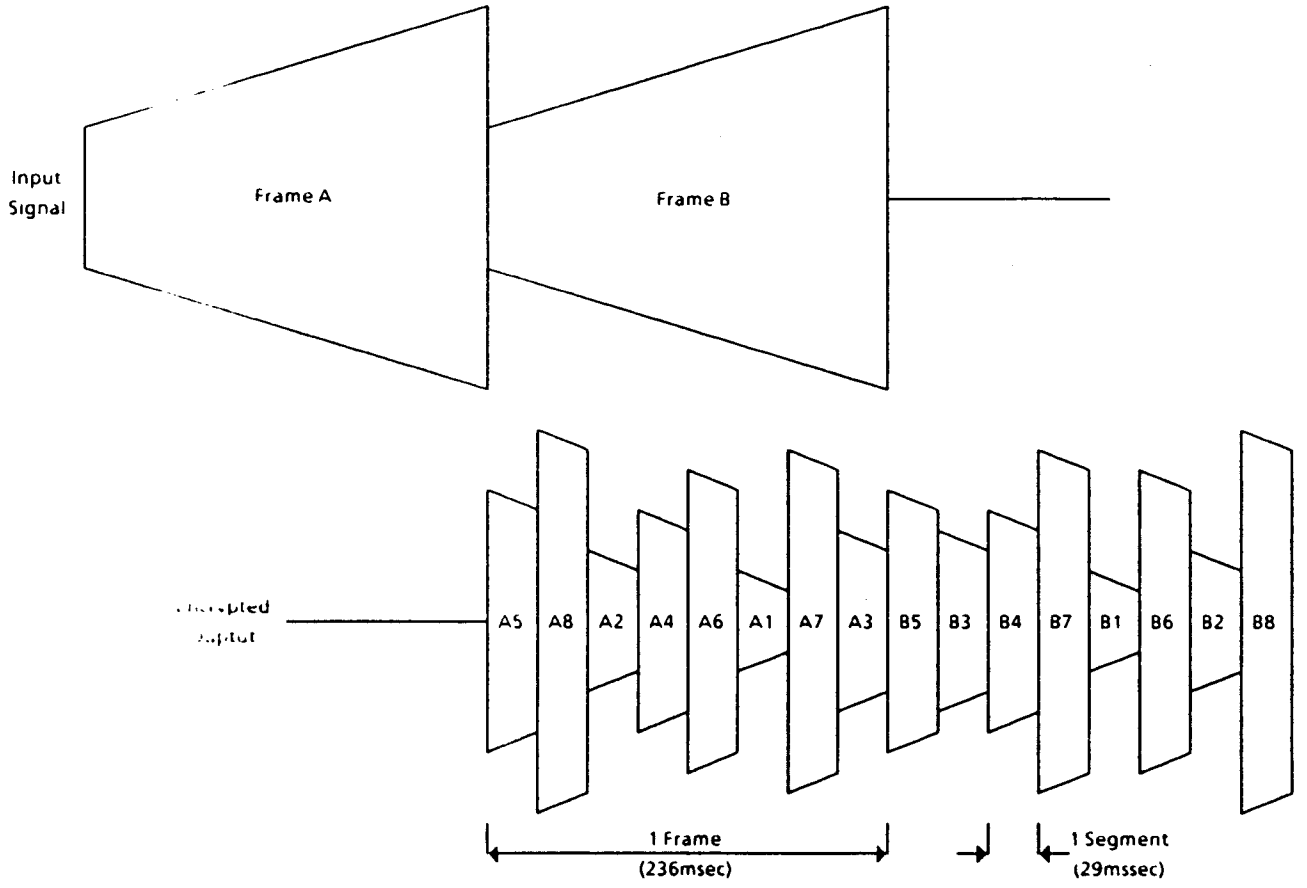


Figure 1. Segmentation

1.3 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 (using the nominal device clock of 4.433MHz) that is transmitted across the transmission channel by the Tx DVS200. When the Rx DVS200 receives the sync tone it recognises it (using a form of correlation) and extracts a sync point from it. 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 figure 4a).

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. Please note that in figure 2a, the DAC output is shown with only sync tones present. Normally encrypted speech is also present, but this has been ommitted for clarity.

1.4 Synchronisation - Message Key

The message key facility is an option, selected by means of an external pin (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 in section 1.3, the DVS200's 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

When the message key option is selected, the DVS200's key generator is set to a different point each time the device synchronises The point to which the key generator is set to 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 section 2.6). 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 figure 4b) This pre-cursor is of the same length and frequency as that of the sync tone discussed in section 1.3. The DVS200 temporarily synchronises to the pre-cursor, loading only user code into the key generator. So, between the pre-cursor 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 pre-cursor; if it is in phase it represents a logic 0, anti-phase a logic 1. The first bit, D1 in figure 4b, is always a logic 1; i.e. it anti-phase to the pre-cursor. The DVS200 detects this phase change and switches over to message key decode mode. The example shown in figure 4b has the second data bit (D2) as a logic 0, and you can see that at the junction of D1 and D2 the tone reverts back to being in phase with the message key pre-cursor.

The final sync point always occurs at the final edge of the message key tone. In the case of figure 4b, the last bit, D32 is a logic 0 (in-phase), so the final edge is negative-going. If D32 was a logic 1, the final edge would be positive-going.

1.5 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 CVOICE pin (pin 2).

The second possibility is that the DVS200 has automatically invoked the clear speech mode because the encryption facility is not being utilised. 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 with 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, you will notice that the speech is always transmitted encrypted unless the CVOICE pin is active. A logic 1 on the output CLEAR (pin 55) indicates that the DVS200 is in clear speech mode.

Application Notes

2.1 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 64Kx1 and an access time of no greater than 150nsec. The minimum timing requirements are shown in figure 6a; 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 128x4, and a maximum access time of 200nsec. The minimum timing requirements are shown overleaf in figure 6b; the PCD5114 satisfies this specification, though again, any SRAM whose performance is within the specification shown in figure 6b 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 section 2.10.3 for details.

2.2 Device Reset

Each time the DVS200 is powered up, the device must be reset so that the internal logic is set to a known state. This is achieved by taking the FRES input (pin 68) low for a period of time not less than 2 microseconds. A simple circuit for achieving this is shown in figure 9

2.3 Clock Oscillator

The DVS200 has a nominal clock frequency of 4.433619MHz, though it can run at clock frequencies of upto 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 figure 10.

2.4 Analogue to Digital Converter

The DVS200's analogue to digital converter (ADC) is a serial adaptive delta modulator (ADM) that runs at a sample rate of 139Kbit/sec. The average input signal level should be approximately 1.7 volts (peak to peak); the ADC input should be driven by an impedence of less than 1Kohm. The external circuitry required, together with the recommended component values, are shown in figure 11.

2.5 Digital to Analogue Converter

The DVS200 has four outputs which, together with a few external passive components, go to form the Digital to Analogue Converter (DAC); these outputs are DACA (pin 70), DACB (pin 71), DACC (pin 72) and DACD (pin 73). Figure 12 shows the connection details. It is recommended that the values shown in figure 12 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 100Kohm. If the input impedance of the interface circuitry is less than 100Kohm 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 these is selected by the control logic of the DVS200. A description of each mode, together with what signals are present on each of the DAC outputs follows:

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 section 2.8), or the periodic sync circuitry. The operation consists of two phases. The main phase involves the transmission the sync tones During this phase encrypted speech data outputs 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 1.06sec or 118msec (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 (again by a factor of two) output from the DAC for a period of 118msec. 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). This attenuation is achieved by replacing the sync tone on DACC and DACD with the device clock.

d) Rx Excrypted - The DVS200's normal receive operation. The thing to note about this mode is 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 section 1.5): so if there is clear speech on the ACD, 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. Unfortunately, the filter attenuates other frequencies as well as the sync tone frequency, so the notch filter is only selected whenever a sync tone has been received. When the DAC is in this mode, the speech outputs from the DAC at the same level as it was on the input to the ADC. As the speech was transmitted at half its normal level during Tx sync (see c) above) the level will be consistent throughout the receive mode of operation.

Table three 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.

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 Analogue Converter Operation

2.6 Message Key

2.6.1 Basic Circuitry

The operation of the message key option is described in section 1.4; it is selected by leaving the MKEY pin (pin 3) unconnected (internal pullup pulls the input to a logic 1). There is a small amount of external circuitry required for the message key operation. This is shown in figure 13. This external circuitry is inserted between the DVS200 and SRAM on the D0 connection (please note that the circuit in figure 13 is for PTT active low - if PTT is active high, the NPTT 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.

2.6.2 Message Key Derivation

While the DVS200 is in message key mode, thirty two 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/sec. 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 NRND (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 figure 11). Any of these methods, or indeed any other, can be used to derive the message key.

2.6.3 Message Key Mute

When the Rx DVS200 receives a sync tone (with or without message key) the notch filter at the DAC is activated (see section 2.5); 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 (see section 1.4). At these data boundaries the sync tone will not be a 50% duty cycle square wave (see figure 4b). The notch filter will not be able to eliminate this from the channel; this will result in a glitch on the final speech waveform. This glitch 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 1msec pulse each time a glitch is present is shown in figure 14. This logic output (Mute Out) can then be connected to a FET, or analog switch, that will shunt the channel (post-DVS200) 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.

2.7 Sync Input

The receive analogue 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 square with a 50% duty cycle. You will have noticed in figure 4a 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 figure 15.

2.8 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).

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 I will assume, 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 PTT 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 118msec 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).

Please 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 figure 16. The resultant timing is shown below in figure 2.

Because of the nature of the encryption technique, there is a time delay, of approximately 236msec, 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 figure 2, ranges from 236msec (one frame length) to 450msec, 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 NPTT output (pin 6) is an inverted version of PTTOUT, and can be used to control any analogue switches that are needed to switch between the Rx and Tx speech channels.

2.9 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, this user will be unable to recover encrypted speech correctly until another transmission has been initiated, ie. 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 figure 17. 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 VDD or VSS.

Please 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 460msec, depending on what point in a frame the periodic sync operation is completed.

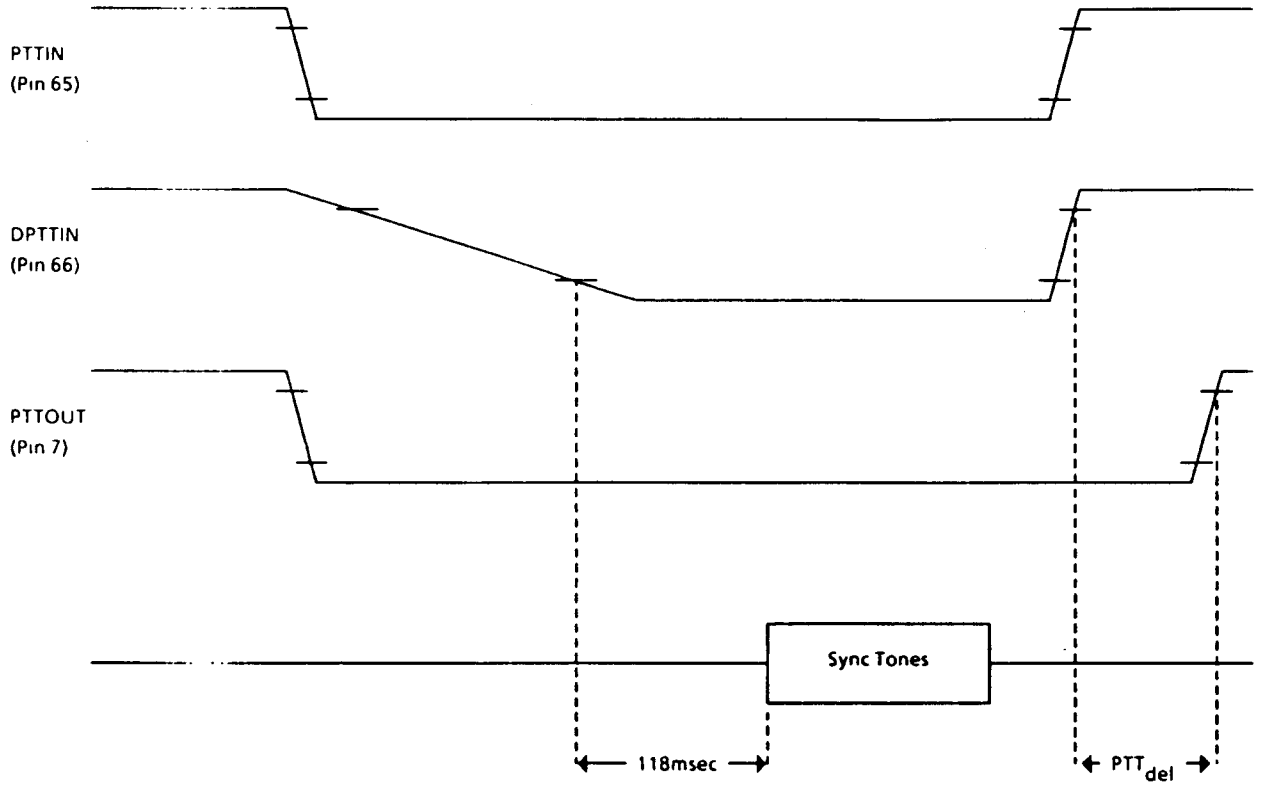


Figure 2. PTT to Sync Delay Timing

As mentioned in section 1.5c), 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 CVOICE pin is not active). If this automatic override is not required, then the periodic sync option should not be selected in Rx.

2.10 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 (FRES active).

2.10.1 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 VSS. 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 figure 18a) The inverse is true of the sixteen switch configuration; it offers greater security (65336 possible codes), but this occupies greater board area. So, the decision about the number of switches to be used for code entry is 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 figure 18). 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. SSTB0-SSTB3 (pins 59, 60, 61, 61); otherwise these terminals should be connected to VSS (see figure 18a). 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 SSTB outputs should be connected together, ensuring that the number of strobe nodes is equal to the number of switch banks (see figure 18b). The timing diagram for automatic seed data entry is shown in figure 7.

2.10.2 Seed Data Entry - External Strobe

This method of seed data entry is selected by tying the KINJ input (pin 63) to VDD. 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 ISTRB input (pin 64 - active on the negative edge). This is repeated for each of the thirty two 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 section 2.10.4).

There are two ways to implement this. The first is to use a key fill gun (the SP100 for example); 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 (32x4 min) each time the DVS200 is reset. The necessary timings for strobe controlled seed data entry are shown in figure 8.

2.10.3 Seed Data Paging

When an SRAM with excess capacity is used (i.e. greater than 128x4), 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 128x4 (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 of course, means 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 figure 3.

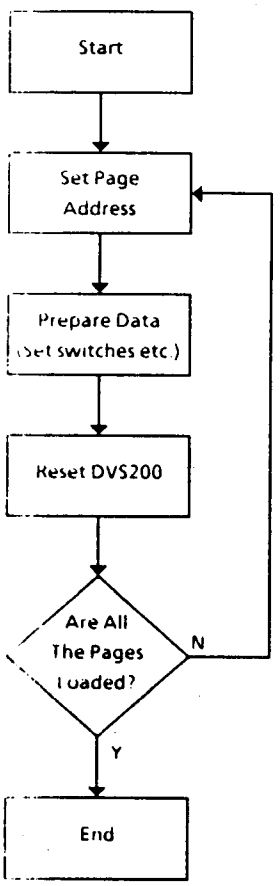


Figure 3 Loading Paged Seed Data

If the seeding is being done using the external strobe option, the 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 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 utilised, the automatic seeding option (described in section 2.10.1) 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.

2.10.4 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 sections 2.8.1 and 2.10.2). 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.

3.0 Timing Diagrams

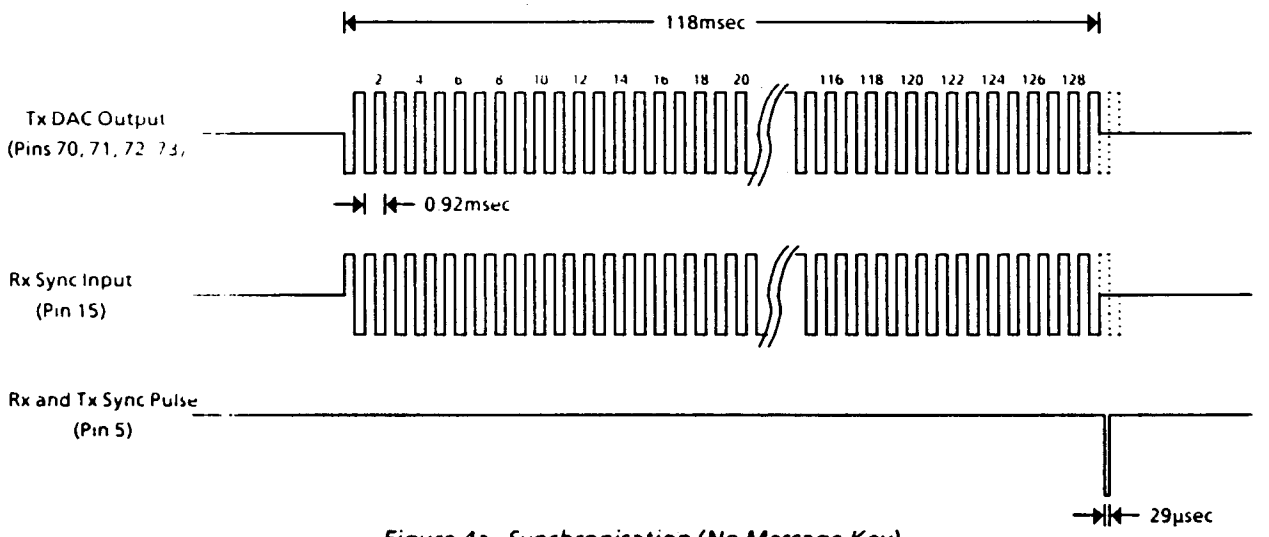


Figure 4a. Synchronisation (No Message Key)

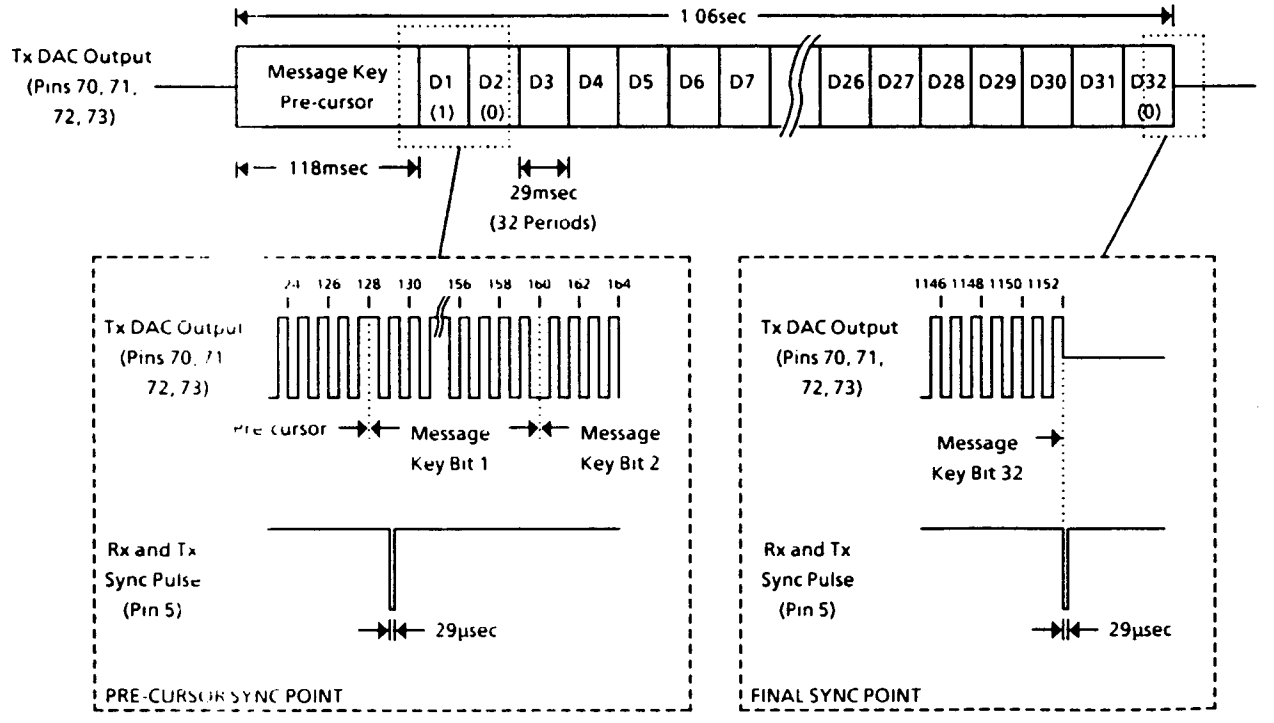


Figure 4b. Synchronisation (With Message Key)

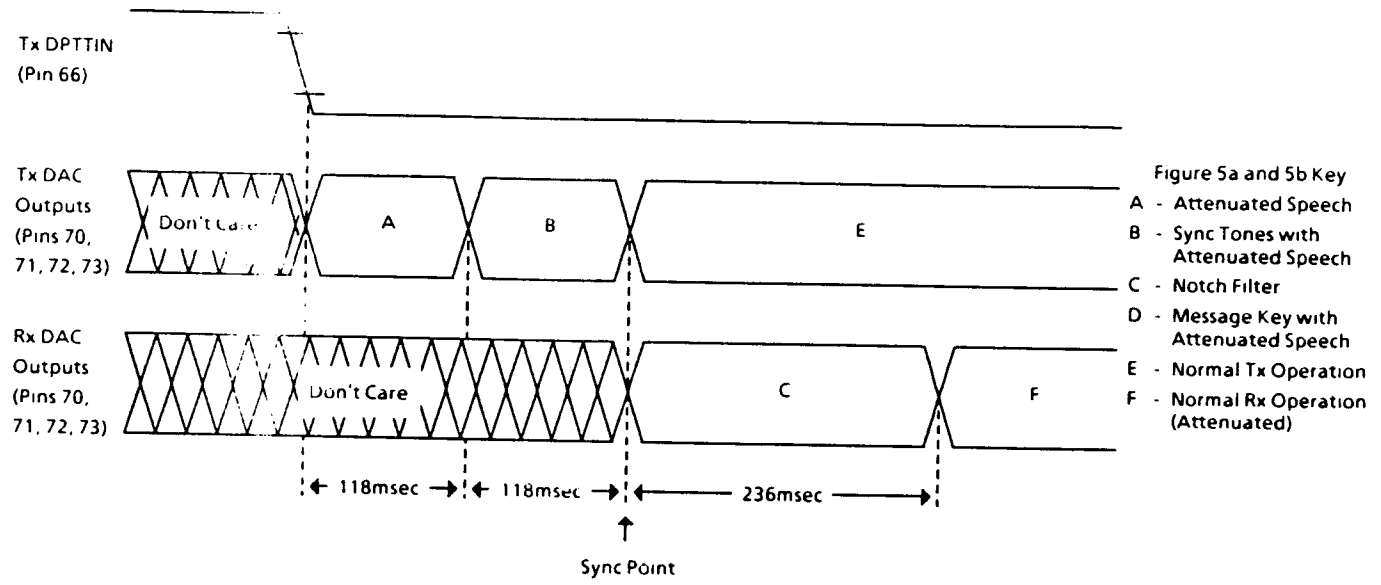


Figure 5a. DAC Operation (No Message Key)

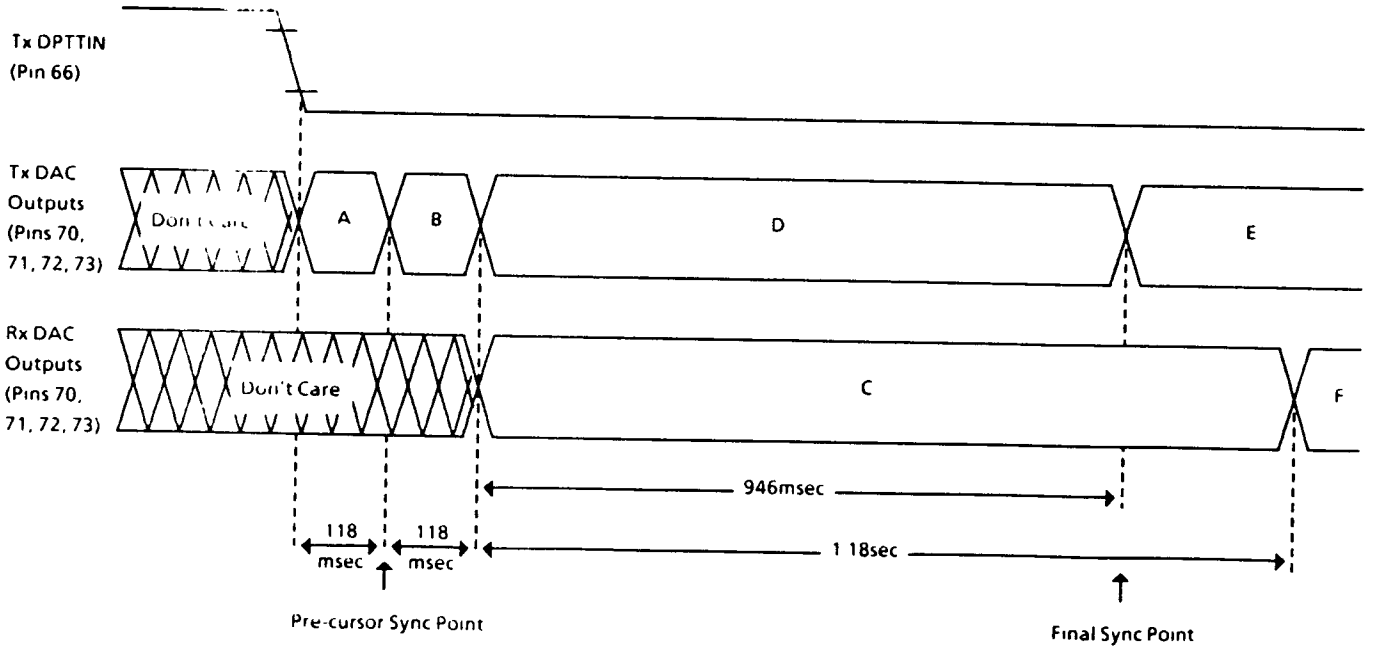


Figure 5b. DAC Operation (With Message Key)

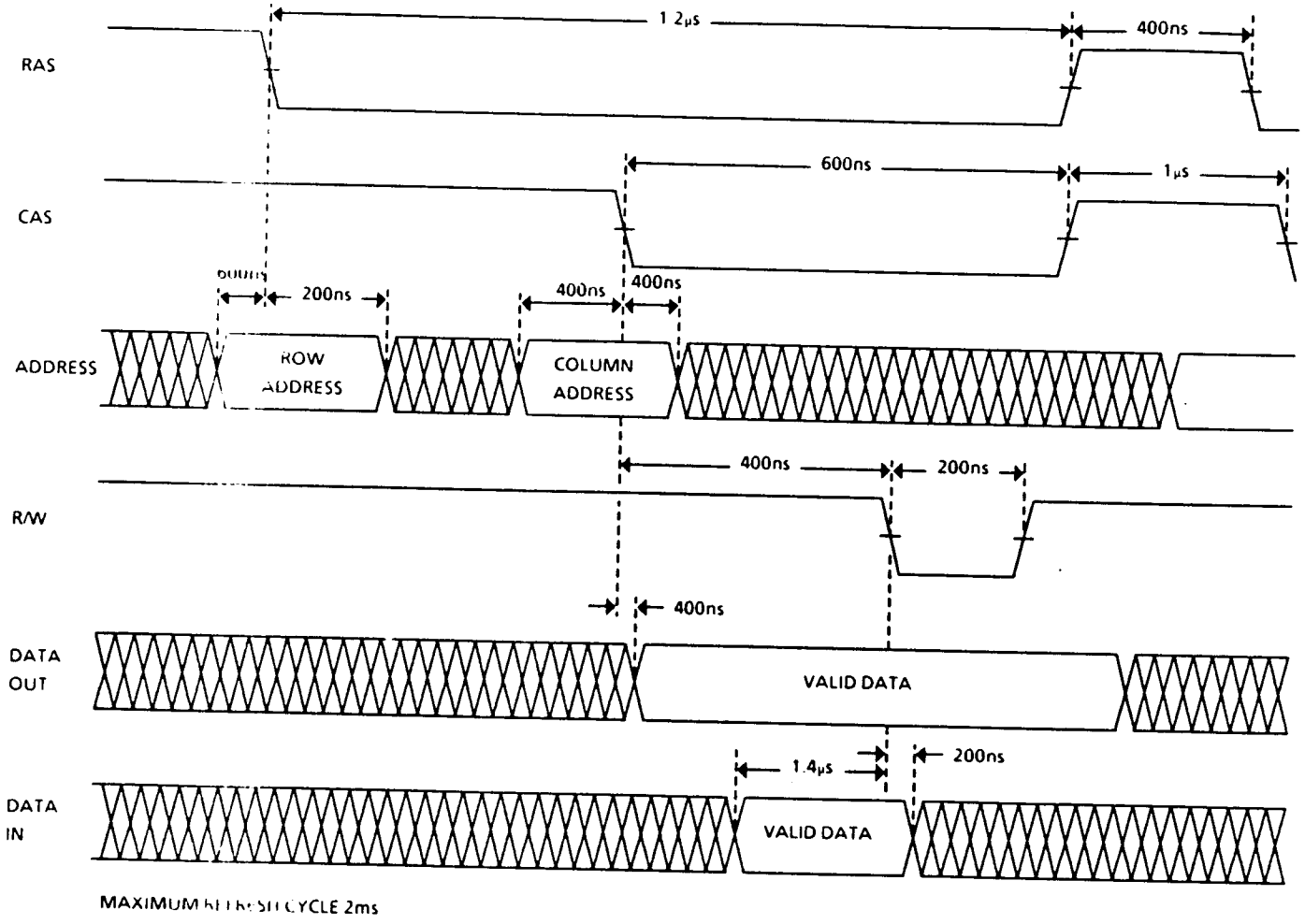


Figure 6a. DRAM Read/Write Cycle

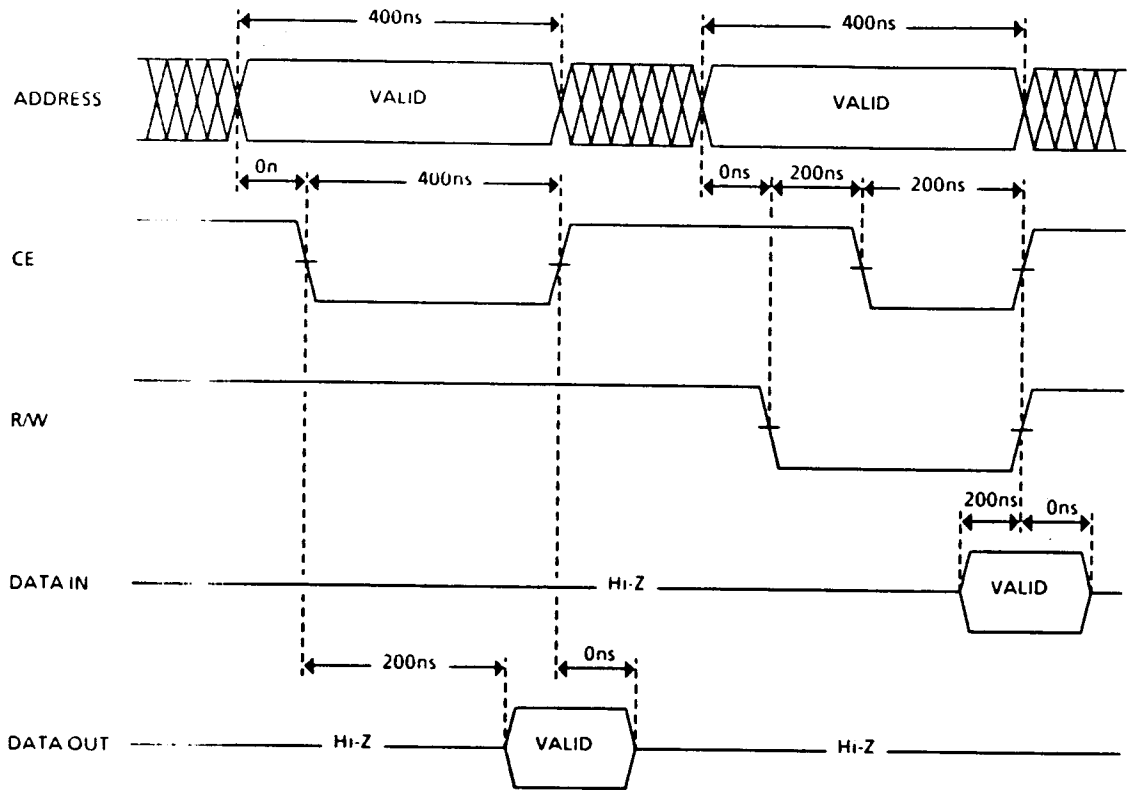


Figure 6b. SRAM Read/Write Cycle

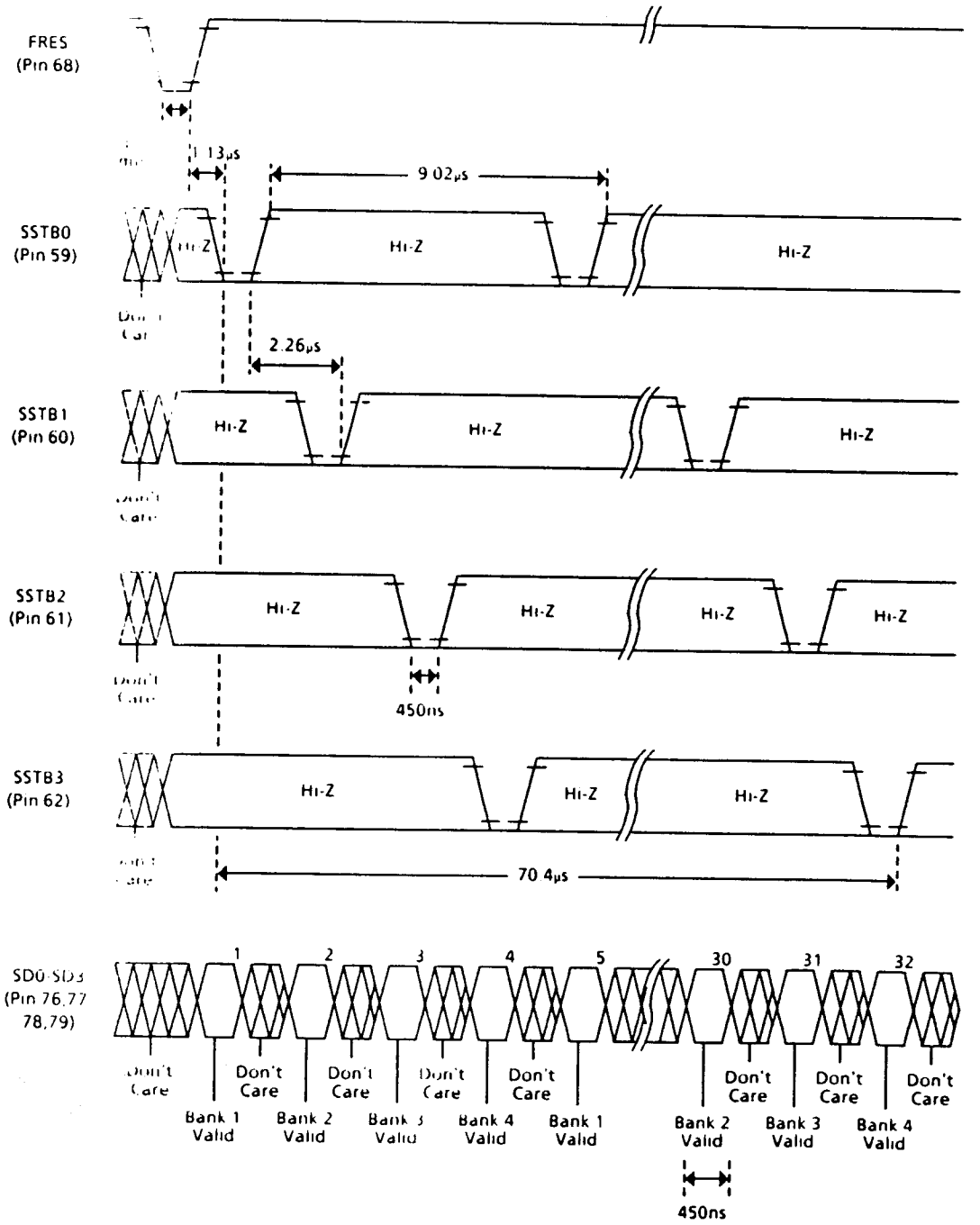


Figure 7 Automatic Seed Data Entry Timing

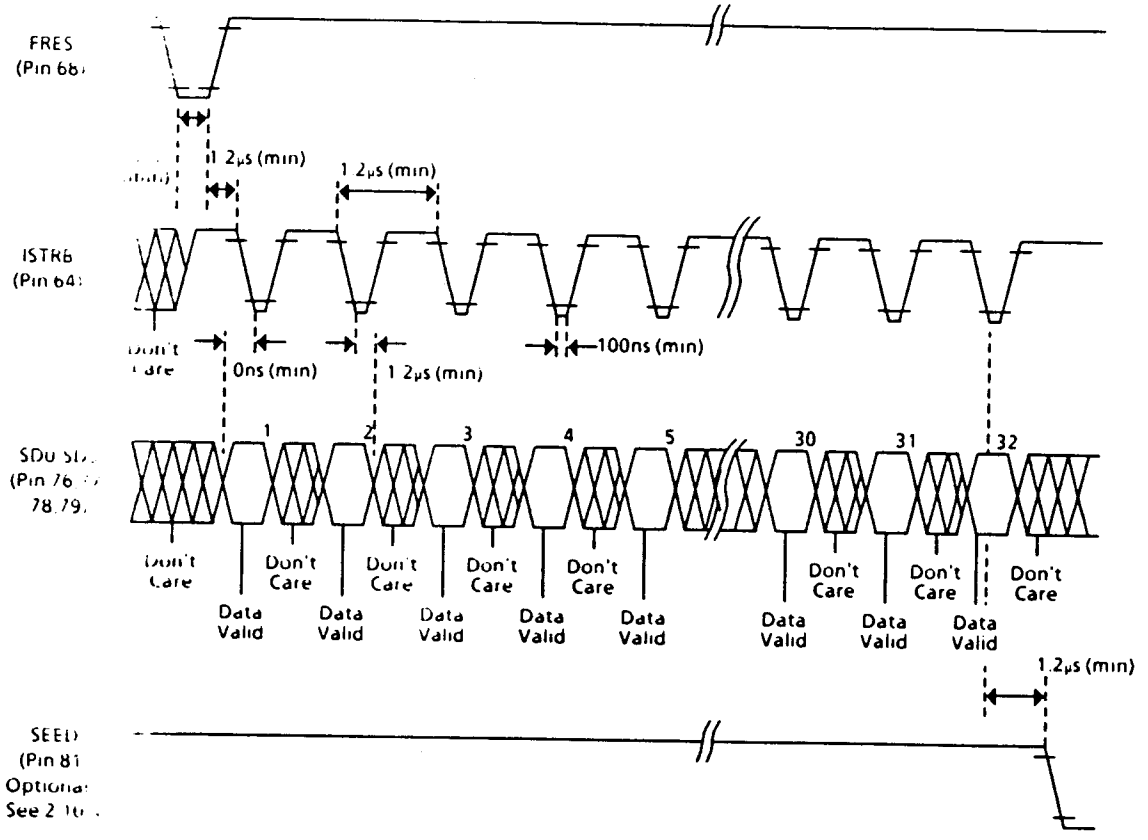


Figure 8. Strobe Controlled Seed Data Entry Timing

4.0 Circuit Diagrams

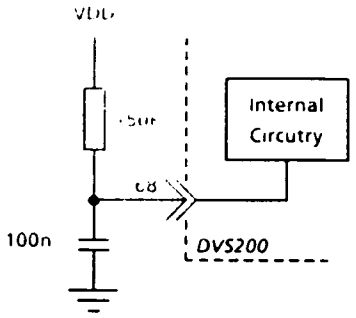


Figure 9 Device Reset

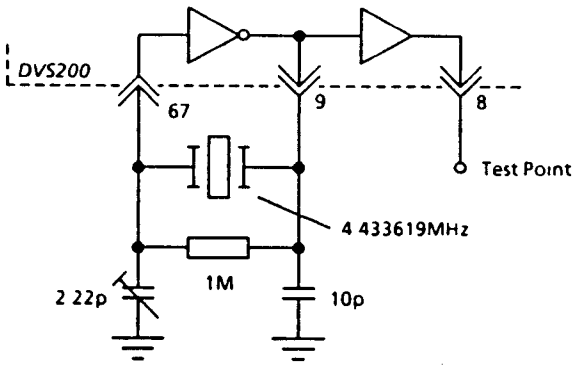


Figure 10. Clock Oscillator

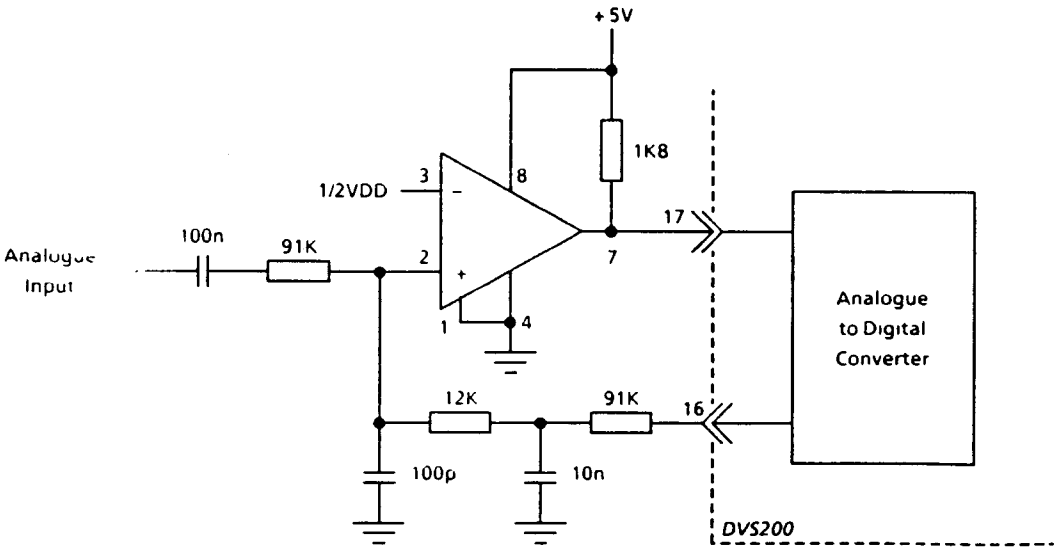


Figure 11. ADC External Circuitry

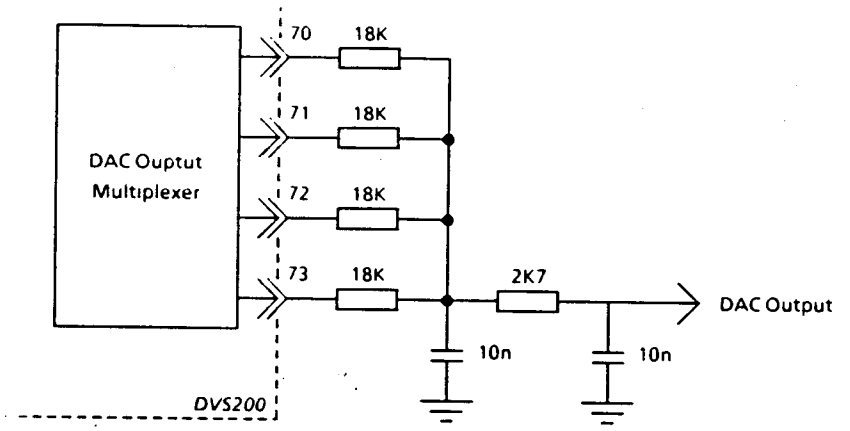


Figure 12. Digital to Analogue Converter

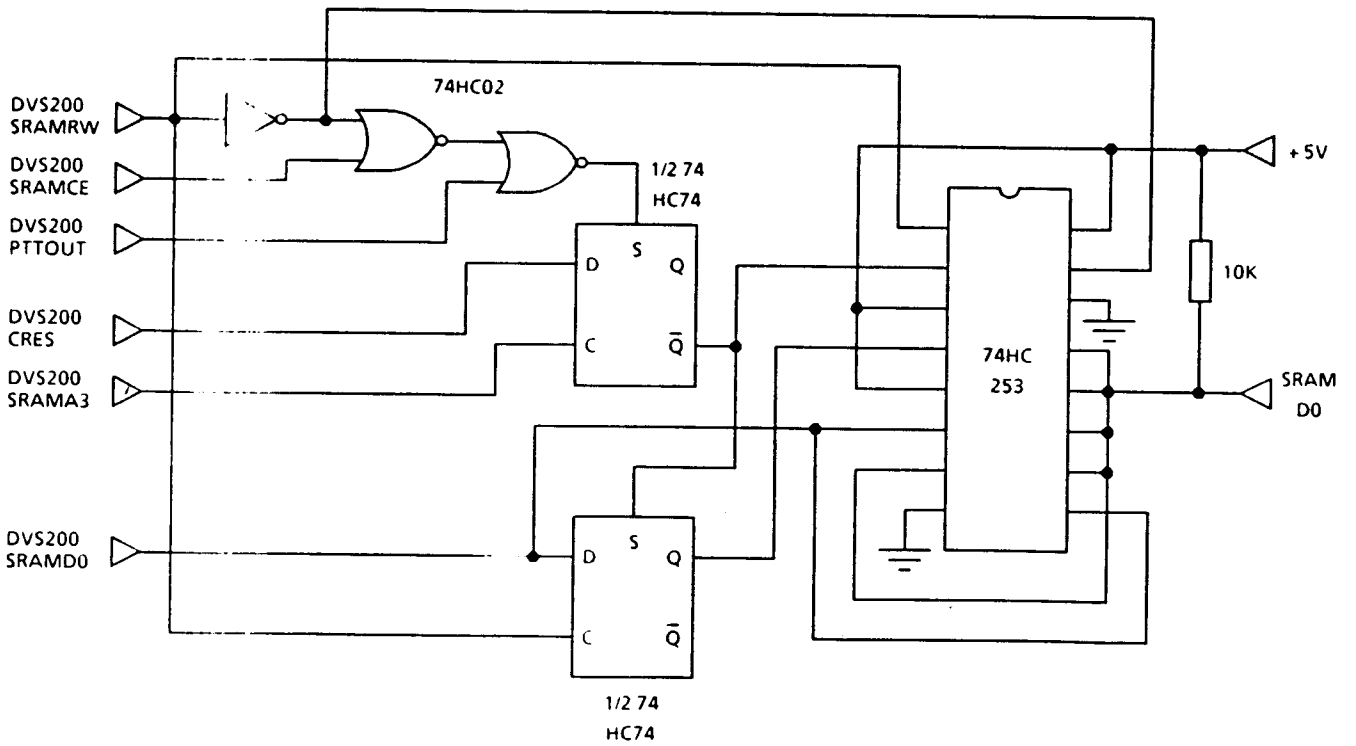


Figure 13. Tx Message Key Circuitry

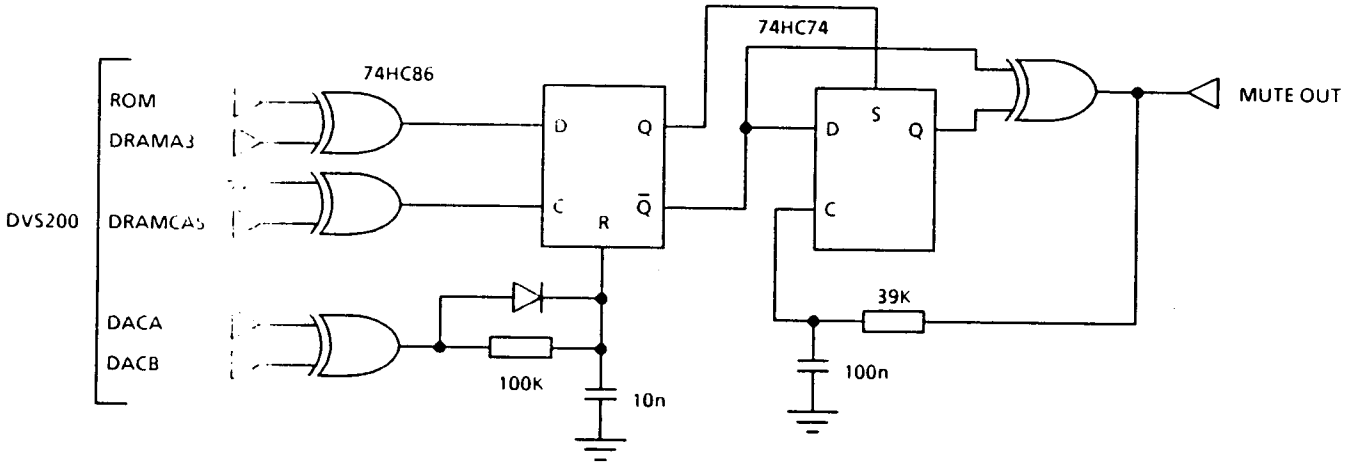


Figure 14. Rx Message Key Mute Circuit

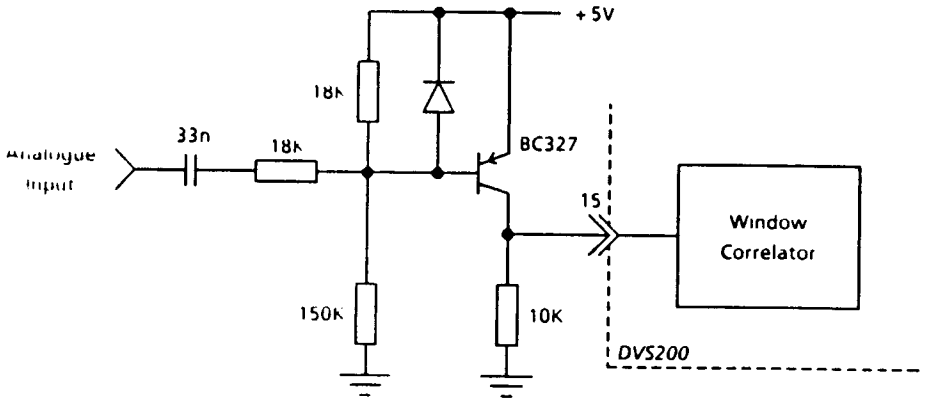


Figure 15. Sync Tone Inverter

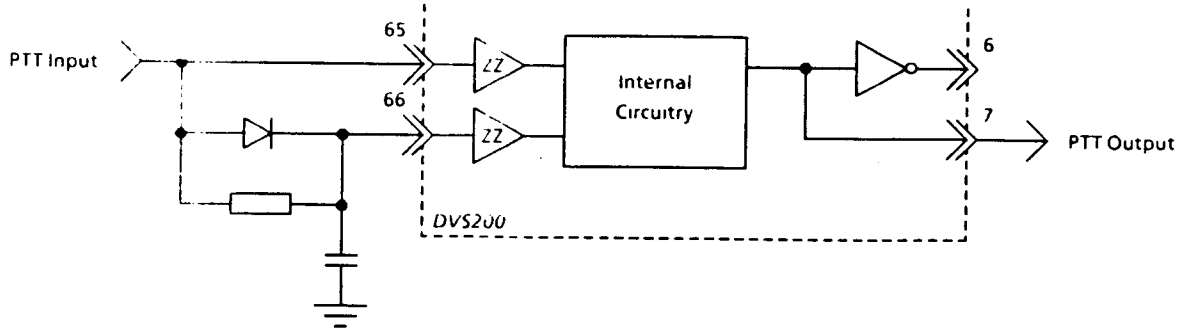


Figure 16. PTT to Sync Delay Circuit

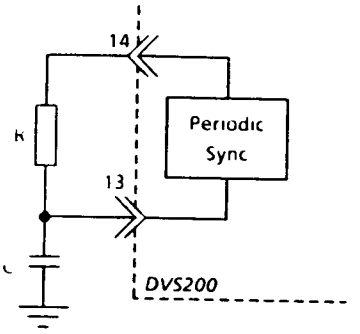


Figure 17. Periodic Sync Circuit

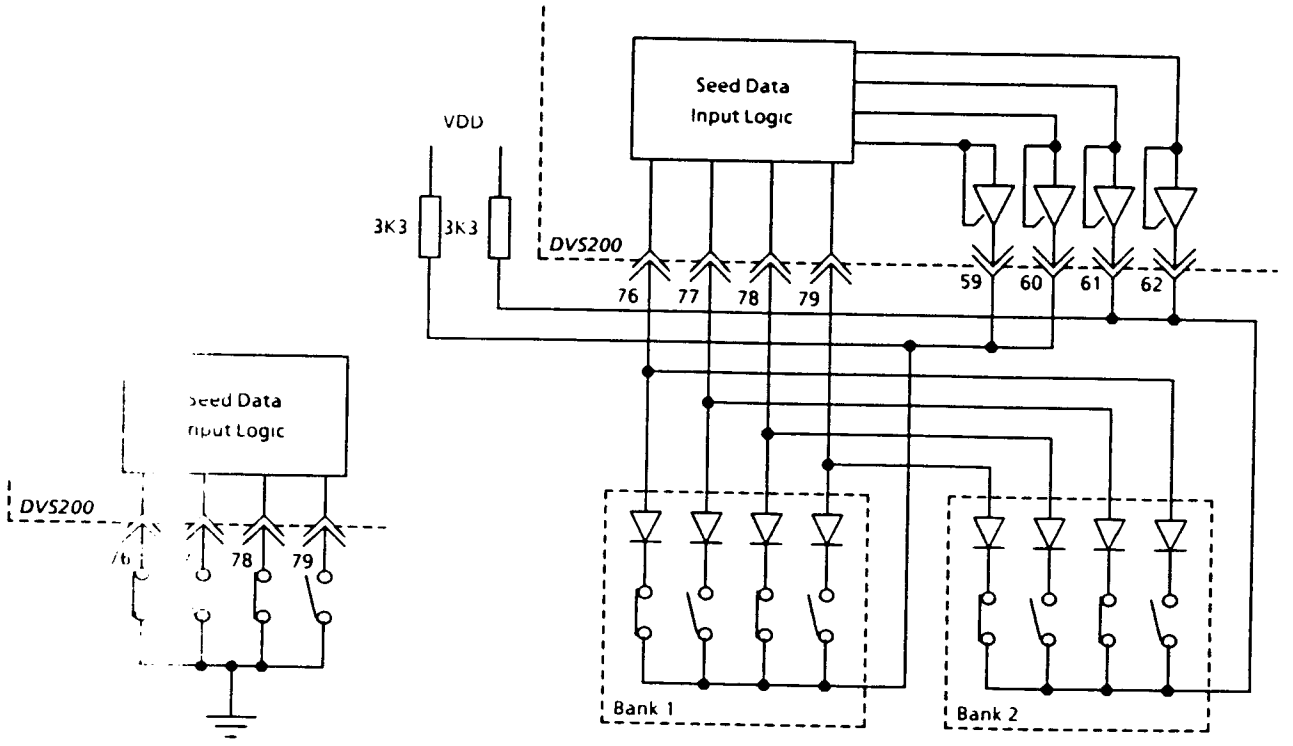


Figure 18a Seed Data Entry - Four Switches

Figure 18b. Seed Data Entry - Eight Switches

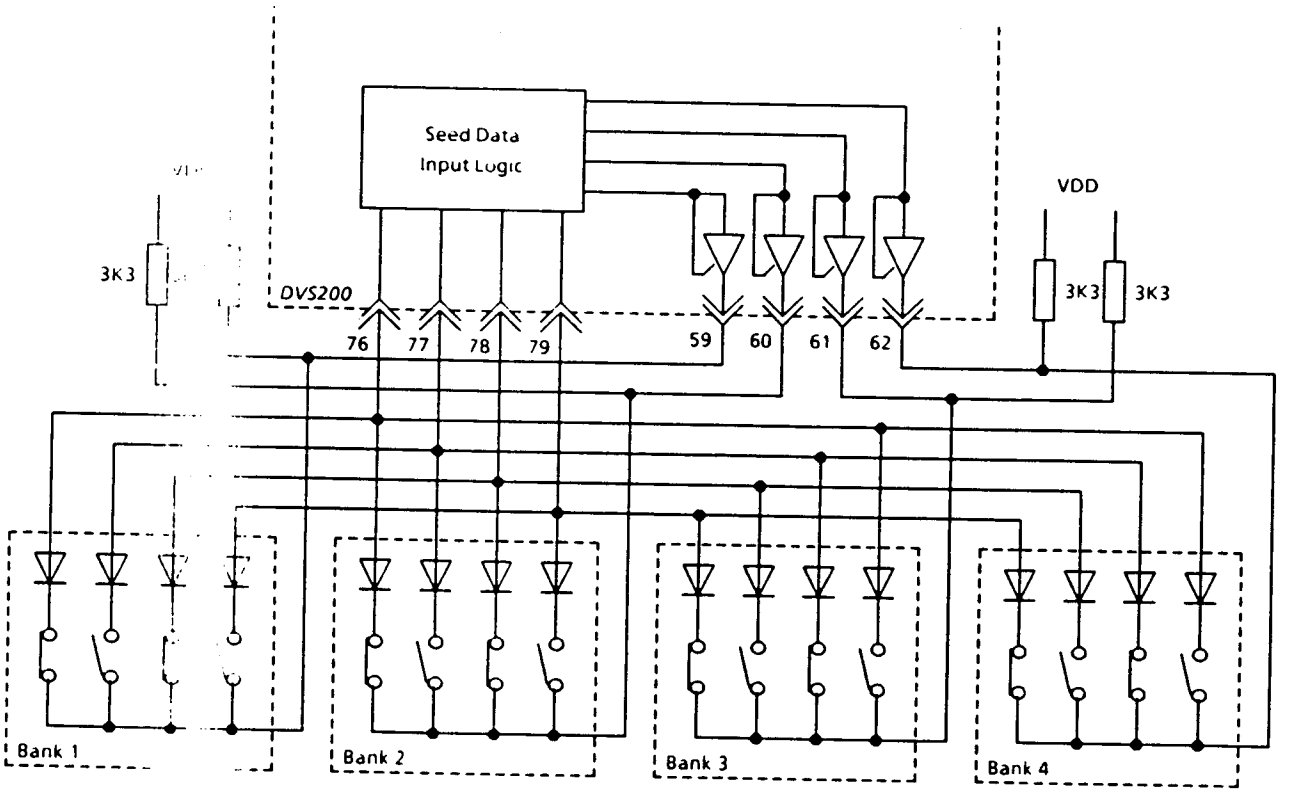


Figure 18c. Seed Data Entry - Sixteen Switches

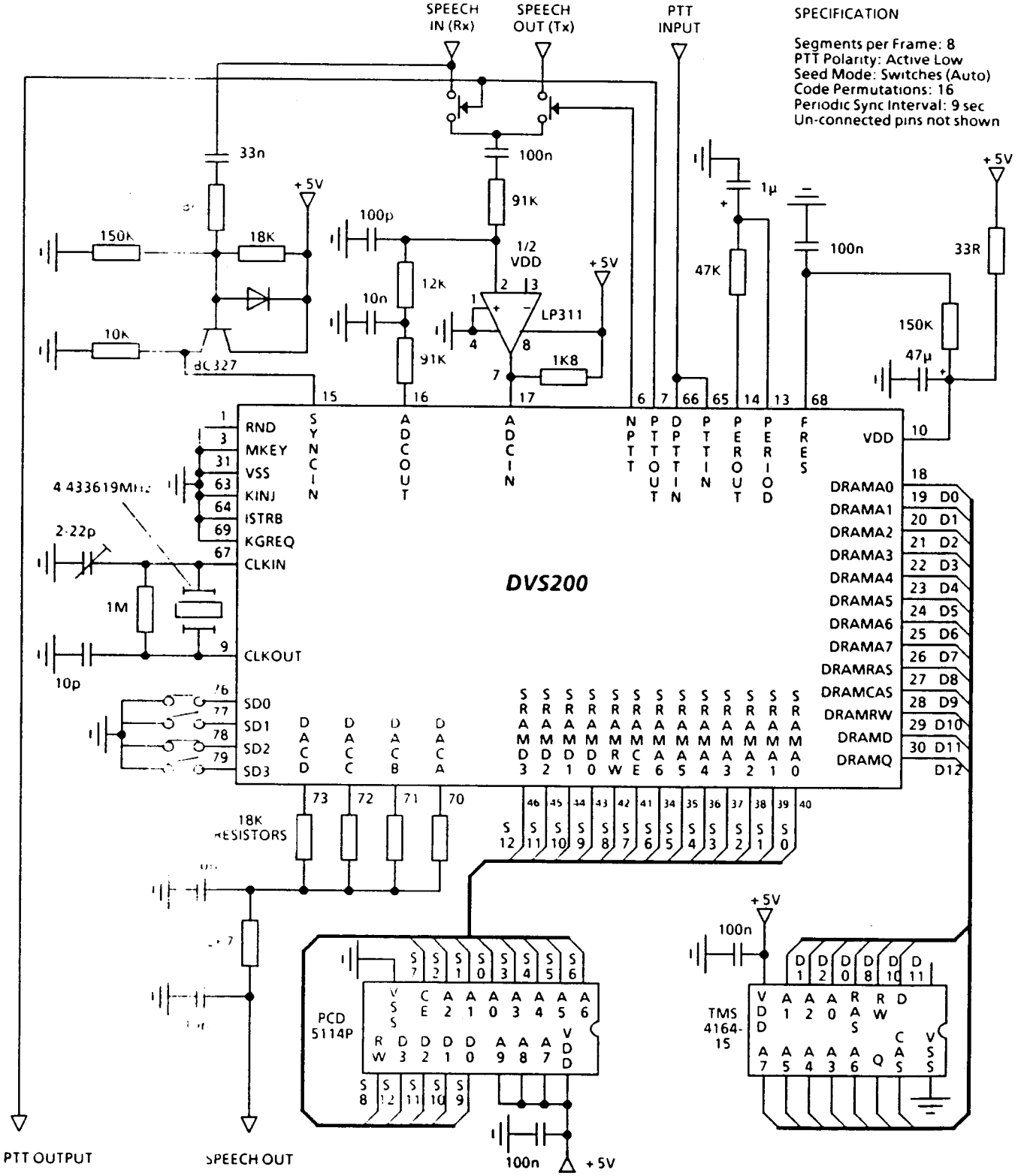
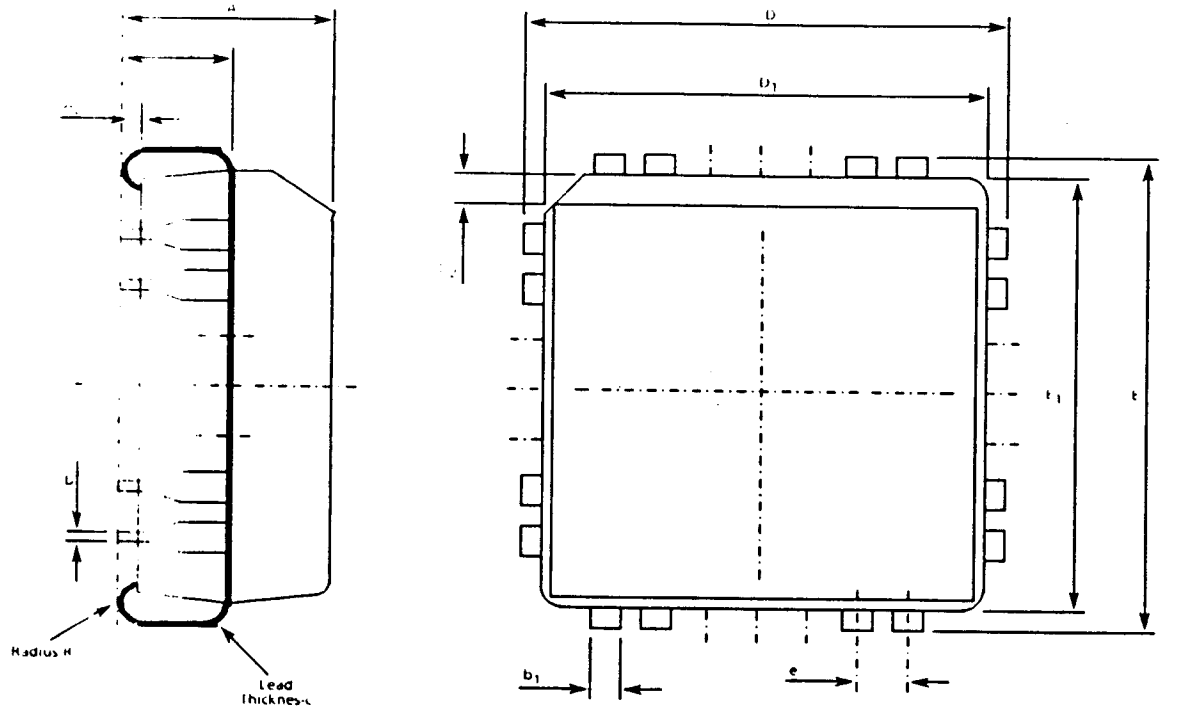


Figure 19. Basic Applications

5.0 Package Outline



DIM.	MIN	NOM.	MAX.
A	[illegible]		0 18
A_1	[illegible]		0 118
A_2	[illegible]		
b	[illegible]		0 21
b_1	[illegible]		0 032
c	0 009		0 0103
D	1 185		1 195
D_1	1 150		1 156
D_2	[illegible]		0 048
E	1 185		1 195
E_1	1 150		1 156
e		0 050	
R	[illegible]		0 045

Figure 20. 84 'J' lead Plastic Carrier

6.0 Absolute Maximum Ratings

Parameter	Min.	Max.	Units
Supply voltage	-	10	V
Voltage on any pin	V_{SS}-0.3	V_{DD}+0.3	V
Short circuit output current	-	10	mA
Power dissipation	-	1	W
Operating temperature	-40	85	°C
Storage temperature	-65	150	°C

Table 4 Absolute Maximum Ratings

Stresses above those listed may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these conditions, or at any other condition above those indicated in the operations section of this specification, is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

7.0 Electrical Characteristics

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

V_{DD} = 5V ± 10%, over full operating temperature range

Table 5. Electrical Characteristics

DVS200

SPEECH ENCRYPTION PROCESSOR

8.0 Functional Specification

All figures quoted at V_{DD} = 5V, clock = 4.433619MHz

Encryption

Technique	TDM and Time Inversion
Frame Length	236msec
Segments per Frame	8/16(option)
System Delay	236msec per end

Key Generator

Sequence Length	1.329x1036
Sequence Number	260
Key Variable Entry (Switches)	16 bits
Key Variable Entry (Keyfill; Gun)	1228 bits

Analogue to Digital Conversion

Conversion Method	Adaptive Delta Modulation
Sample Rate	139Kbit/sec
Average Input Signal Level	1.7Vpp
Dynamic Range	40dB
Idling Noise	10mV
SNR(1KHz@1.7Vpp)	45dB
Psophometric Noise	Better than -45Bm

Synchronisation

Sync Tone Frequency	1.082KHz
Sync Tone Decoding	Correlation
Periodic Sync	Period Variable (External RC)
Number of Message Key Bits	32
Message Key Modulation	Phase