

Istituto Professionale di Stato per l'Industria e l'Artigianato
MORETTO
Via Luigi Apollonio, 21 BRESCIA

Lo Scrambler ed il Teorema di Shannon

Relatore

SANTIAGO VALTERNILO

classe 5BZ TIEN 2000-01

corso per Tecnici delle Industrie Elettroniche

Docenti :

prof. Cleto Azzani

prof. Vitonofrio de Trizio

PREMESSA

Quando dobbiamo trasmettere informazioni riservate o personali quasi sempre non riusciamo a trovare una via sicura, scegliendo così, la classica chiacchierata a porte chiuse.

I vari mezzi di comunicazioni non sono sicuri abbastanza per trasmettere informazioni segrete. Le comunicazioni via radio, così come i messaggi registrati possono essere facile “preda” di ascoltatori indiscreti. Il telefono sembrerebbe il mezzo più sicuro, ma può sempre capitare delle interferenze fra due linee telefoniche.

L'alternativa a questa drastica soluzione è data da un circuito elettronico capace di “Criptare”, cioè rendere incomprensibili, le informazioni via radio, per telefono o registratore a nastro magnetico.

Le informazione vocali potranno essere ascoltata o meglio compresa da chi possiede un circuito uguale programmato con lo stesso codice prestabilito, mentre altre persone sentiranno solo parole indecifrabile e discorsi assolutamente incomprensibili.

Questo circuito è lo “SCAMBLER”, esso rende le frasi ma anche le singole parole indecifrabili invertendo

La gamma delle frequenze acustiche e modificando il suono e il significato delle parole. Così uno che ascolta la conversione, anche se poliglotta non comprenderebbe la frase detta.

Le possibilità di scelta del codice di criptaggio sono 16 perché l'impostazione di questo codice avviene tramite quattro dip-switch; che secondo l'algebra Booleana le combinazione possibile sono con 4 interruttori sono 16, di conseguenza potremo avere fino a questo numero di corrispondenti di messaggi segrete, ogni uno con un codice diverso.

Nel circuito sono presenti sia la codifica che la decodifica utilizzando così un unico apparato per trasmettere e ricevere informazioni, così si ha più praticità di utilizzo ed un risparmio in termini di componenti elettronici, infatti alcuni dispositivi che interagiscono con la codifica e la decodifica, sono in comune eliminando così anche eventuali discrepanze tra i codici di criptaggio dovute alle interferenze.

Inoltre con questo circuito possiamo verificare il teorema di Shannon aggiungendo un ulteriore circuito che possa generare delle frequenze.

1° – blocco : **PREAMPLIFICATORE A GUADAGNO VARIABILE**

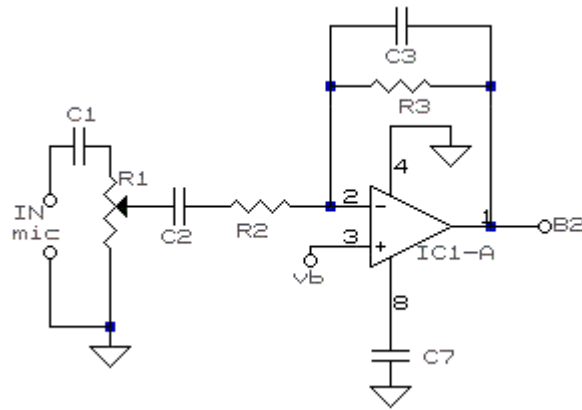


Figura 1

Questo blocco è costituito da un stadio d'ingresso ed un filtro passa-banda attivo del 2° ordine, che funziona da pre-amplificatore. La presenza del Trimmer R1 fa sì che l'amplificatore sia a guadagno variabile, a seconda della regolazione d'ampiezza del microfono. Dove la sua caratteristica di trasferimento è:

$$Z_2 = R_2 + \frac{1}{sC_2} = \frac{1 + sC_2R_2}{sC_2}$$

$$Z_3 = \frac{R_3}{1 + sC_3R_3}$$

$$A_v = F(s) = -\frac{Z_3}{Z_2} = -\frac{sC_2R_3}{(1 + sC_2R_2) \cdot (1 + sC_3R_3)}$$

Sulla base della teoria dei filtri passa- banda è stato calcolato anche la frequenza di taglio inferiore e superiore. Frequenza ricavata da una rete RC.

$$f_T = \frac{1}{2p \cdot CR}$$

$$f_{Ti} = \frac{1}{2p \cdot C_2 R_2}$$

$$f_T = \frac{1}{2p \cdot C_3 R_3}$$

Si ricavata dalle formule che il range di frequenza è compreso fra 73-2823Hz

Il range della banda passante del circuito in questo blocco si può riportare a quello vocale che è di: 300-3000Hz.

L'utilità è una prima limitazione di frequenza dato che è la voce che dovrà essere modificata e tutte le altre frequenze, soprattutto i disturbi, sarebbero d'impiccio al normale funzionamento dello Scambler; le frequenze vocali vengono poi amplificate per fare in modo che raggiungano gli altri dispositivi senza problemi.

2- blocco: **FILTRO PASSA-BASSO (ANTI-ALIASING)**

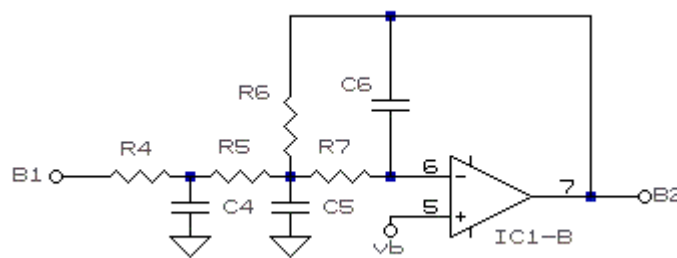


Figura 2

Il blocco rappresentato in figura è un ulteriore filtro passa- basso del 2° ordine a reazione multipla. Trattandosi di un filtro passa- basso , il guadagno in banda è determinato dal rapporto Uscita/Ingresso in corrispondenza dei valori di frequenza inferiori a quella di taglio, per i quali risulta trascurabile l'effetto delle reattanze.

In tale ipotesi, il circuito del 2° blocco si configura come un amplificatore operazionale in configurazione invertente, pertanto:

$$A_0 = -\frac{R_6}{R_5}$$

$$A(s) = - \frac{\frac{R_6}{R_5} \cdot \frac{1}{C_5 C_6 R_7 R_6}}{s^2 + s \frac{C_6}{R_5} \cdot (R_6 R_7 + R_5 R_6) \cdot \frac{1}{C_5 C_6 R_7 R_6} + \frac{1}{C_5 C_6 R_7 R_6}}$$

$$w_0 = \frac{1}{\sqrt{C_5 C_6 R_7 R_6}}$$

$$2x = C_6 w_0 [R_7 (1 - A_0) + R_6]$$

$$f_T = \frac{w_0}{2 \cdot p}$$

Il filtro antialiasing può limitare la banda dello spettro del segnale d'ingresso per frequenze non maggiore alla frequenza di Nyquist.

Nel sistema di campionamento dei dati il limite di banda è compiuto dalla attenuazione delle frequenze maggiori alla di Nyquist per un livello non analizzabile o invisibile per il convertitore analogico- digitale (A/D).

3- blocco: MIXER CODIFICATORE

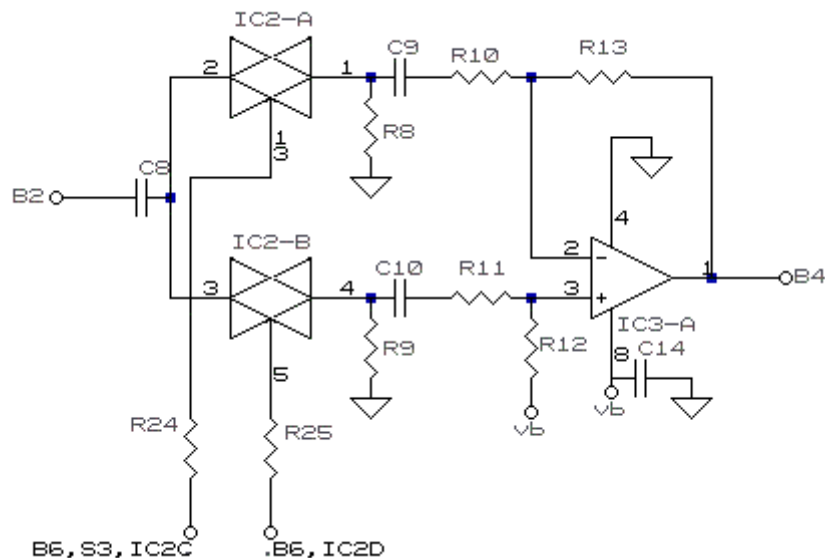


Figura 3

In questo blocco è rappresentato lo schema elettrico del mixer codificatore che è costituito da due interruttori elettronici (IC2-A e IC2-B) e da uno amplificatore() che a seconda da dove passa il segnale, secondo l'abilitazione dei piedini 13 e 5 (IC2-A e IC2-B) comandati dall'oscillatore locale che stabilisce la frequenza con la quale il segnale originario viene modificato e ricostruito nella decodificazione, se il segnale arriva all'ingresso invertente il segnale viene sfasato di 180°, mentre

se il segnale arriva all'ingresso non invertente il segnale non subisce nessuno sfasamento inoltre all'uscita non si ha amplificazione dovuto i valori delle resistenze che fa si che il guadagno sia 1. All'uscita dell'amplificatore differenziale (IC3- A) sono presenti le frequenze ottenute dalla miscelazione, cioè la somma e la sottrazione del segnale microfonico e quello dell'oscillatore locale chiamato anche codice di criptaggio.

4- blocco: **TEOREMA DI SHANNON**

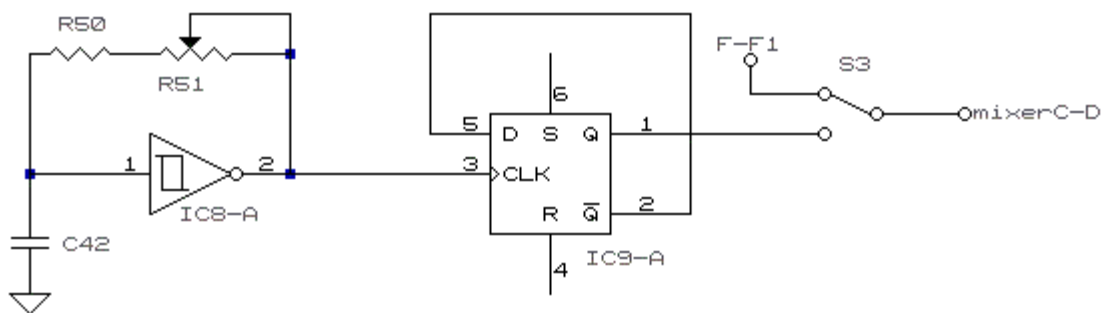


Figura 4

Questo blocco è di estrema importanza per la teoria del campionamento o Shannon, noi abbiamo voluto utilizzando lo scambler provare la frequenza di campionamento che secondo Shannon è di :

$$f_c \geq 2 \cdot f_{MAX}$$

Infatti variando il potenziometro al minimo della frequenza di campionamento che è 4.4 Khz all'uscita audio esce un segnale disturbato secondo un fenomeno denominato aliasing, mentre variando verso il massimo superando i 4.4 Khz il segnale può essere campionato, perché il segnale non è sovrapposto. Per evitare questo fenomeno a vale del circuito Semple-Hold si mette un filtro passa- basso.

Per scegliere la modalità Shannon, basta attraverso un deviatore selezionare tale modalità. Il blocco è costituito da una porta logica not triggerata con una rete RC e da un flip-flop D per aver un dc del 50%, che possa permettere che il tempo di chiusura del mixer S1 sia uguale al tempo di apertura di S2 e vice versa.

5- blocco: **FILTRO PASSA- BASSO (SMOOTHING)**

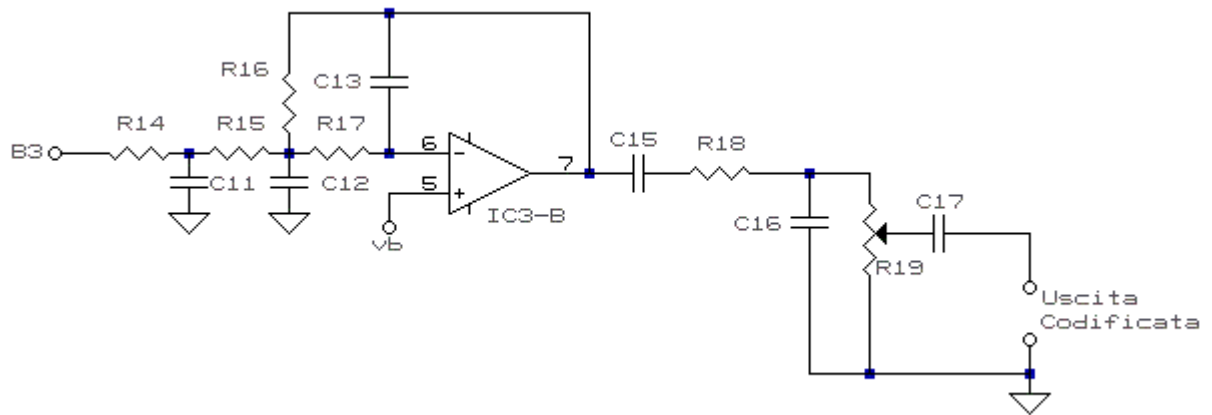


Figura 5

Questo blocco è l'ultima fase di "filtreggio" del segnale, infatti l'amplificatore è stato configurato per funzionare come filtro passa- basso attivo del terzo ordine, simile a quello del 2° blocco, con frequenza di taglio pari a 3000Hz.

Il segnale proveniente dal blocco precedente è costituito da due frequenze ottenute dalla somma e dalla sottrazione del segnale vocale e dell'oscillatore locale, è necessario eliminare il segnale ottenuto dalla somma. Per fare questo si utilizza un filtro passa- basso attivo del terzo ordine in modo da poter amplificare il segnale oltre che condizionarlo a transitare solo sotto una frequenza di 3000Hz.

Le resistenze e i condensatore costituiscono eventuali filtri passivi per un filtraggio più efficiente, Il trimmer R19 si può considerare un adattatore di impedenza quasi identico a quello dello stadio di ingresso; l'utilità è l'adattamento della resistenza dell'utilizzatore per l'uscita codificata che può essere di diverso tipo, ad esempio può essere un alto parlante come l'ingresso di un amplificatore audio.

6- blocco: **OSCILLATORE**

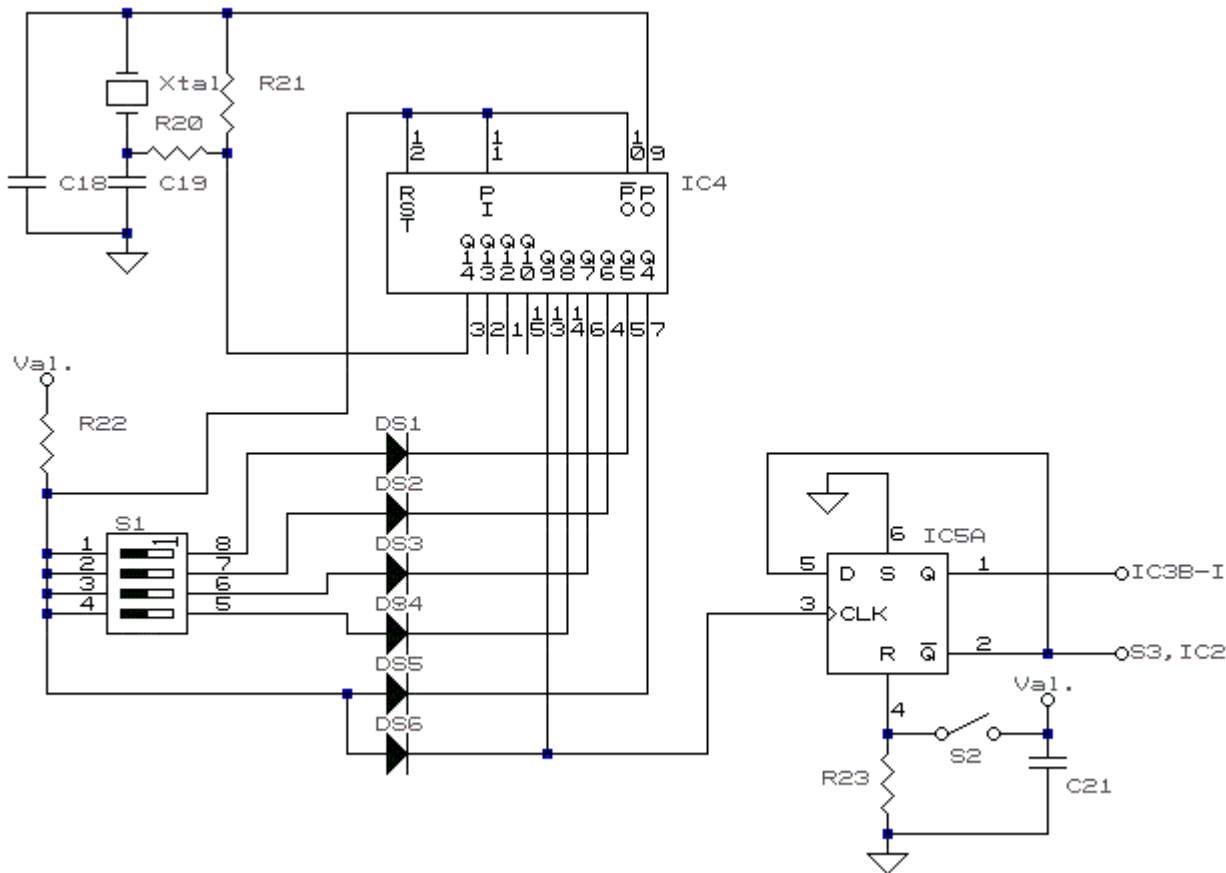


Figura 6

L'oscillatore è la parte di circuito che, secondo l'impostazione dei dip-switch, stabilisce il codice di criptaggio del segnale ovvero la frequenza da fornire al mixer per modificare il segnale originario dell'informazione.

L'integrato IC4 è un contatore binario il quale funziona come divisore di frequenza. La frequenza di partenza è data dal quartzo Xtal 2MHz che viene divisa, a seconda della combinazione dei dip-switch S1, dal contatore.

In questo modo si ottiene una frequenza di clock, da fornire al flip-flop diversa per ogni combinazione possibile con gli interruttori del dip-switch.

7- blocco: FLIP-FLOP

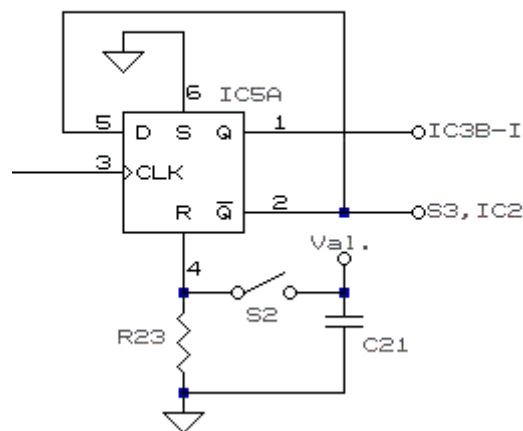


Figura 7

Il flip-flop dello scambler si può considerare come interfaccia di collegamento tra oscillatore del 5° blocco e i mixer che effettuano la modifica del segnale.

Il segnale di clock viene fornito dall'oscillatore tramite un contatore e si inserisce nel piedino n° 3 dell'integrato IC5; il flip-flop contenuto in questo integrato è di tipo D che commuta solo sui fronti di salita del clock.

Il flip-flop di tipo D, ad ogni fronte di commutazione, riporta, sull'uscita Q l'ingresso ed è per questo che, come ingresso D è stato utilizzato il segnale dell'uscita Q negato.

Ad ogni fronte di salita il flip-flop commuta le sue uscite da 0 a 1 e viceversa comandando i mixer di codifica e di decodifica.

Nello schema di fig. 7 dove è rappresentato il blocco del flip-flop, si può notare la presenza di un interruttore, S2, che, a seconda della sua posizione, setta il piedino 4 dell'integrato IC5 con un livello logico 0 o 1. La funzione di S2 è di abilitare o disabilitare la codifica o la decodifica dello scambler senza doverlo collegare e scollegare ogni volta che serve.

Quando l'interruttore S2 è aperto il piedino 4, cioè il reset del flip-flop, è condizionato a massa quindi ad un livello logico 0 che permette il normale funzionamento di IC5. Nel momento in cui S2 viene chiuso sul piedino di reset si ha la tensione di alimentazione e quindi un livello logico 1 che inibisce il flip-flop settando le sue uscite di Q e Q negato rispettivamente a 0 e 1 mantenendole tali fino a che il livello logico 1 sul piedino 4 non verrà commutato a 0.

Bloccando il flip-flop si bloccheranno anche i due mixer che non misceleranno la frequenza vocale con quella dell'oscillatore locale facendo in modo che all'uscita dello scambler si abbia lo stesso segnale d'entrata, cioè il segnale prelevato dal microfono che rimarrà inalterato.

Per quanto riguarda un installazione fissa dello scambler, l'interruttore S2, svolge una funzione molto importante perché permette la codifica di un segnale con il solo spostamento di una levetta.

DECODIFICA

1 - blocco : PREAMPLIFICATORE A GUADAGNO VARIABILE

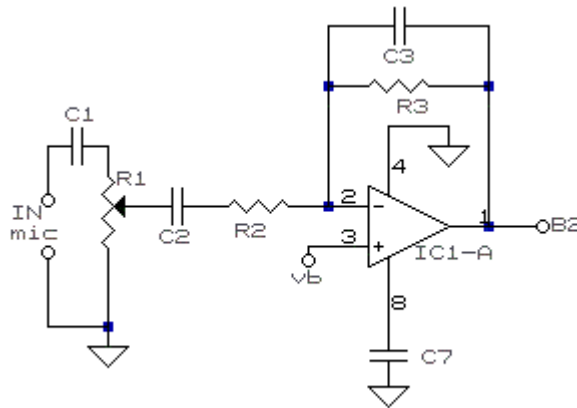


Figura 8

Il blocco funziona identicamente al blocco 1 di codifica, analogamente al preamplificatore della codifica, questo blocco si comporta da filtro passa-basso attivo del 2° ordine eseguendo un primo filtraggio del segnale da decodificare. L'unica differenza tra il circuito della codifica e quello della decodifica è l'aggiunta di una resistenza R28, che serve solo come supporto al trimmer R29, a limitare la tensione d'ingresso che, visto che proverrà quasi sicuramente da un preamplificatore o da un amplificatore, potrebbe essere di una tensione tale da danneggiare lo scambler. Come la codifica, la decodifica è un adattatore di impedenza.

2- blocco: **FILTRO PASSA-BASSO (ANTI-ALIASING)**

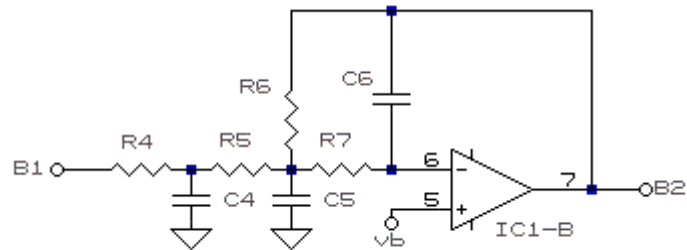


Figura 9

Il circuito di figura 9 è uguale, compresi i valori dei componenti elettronici, al circuito del 2° blocco (codifica) che rappresenta il filtro passa-basso del 2° ordine.

La sua funzione è di avere un ulteriore filtraggio del segnale in modo da eliminare ogni probabilità di segnali parassiti che potrebbero compromettere la corretta decodifica

3- blocco: **MIXER DECODIFICATORE**

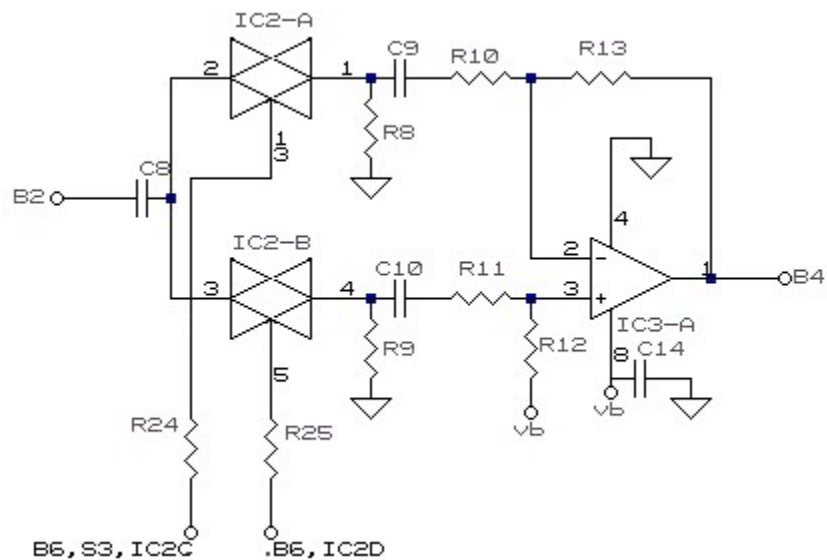


Figura 10

Il mixer decodificatore, funziona identicamente al mixer codificatore, questo spiegherebbe anche l'identità circuitale e dei valori dei componenti.

La differenza del mixer decodificatore rispetto al mixer codificatore, è che al suo ingresso è presente il segnale codificato ovvero incomprensibile che verrà decodificato e reso comprensibile con lo stesso metodo della codifica cioè miscelando il segnale con la frequenza dell'oscillatore locale.

Da questa miscelazione si otterrà, come per la codifica, due frequenze, una dovuta alla somma e l'altra alla sottrazione, che verranno filtrate in modo da eliminare la frequenza della somma.

4- blocco: **FILTRO PASSA- BASSO (SMOOTHING)**

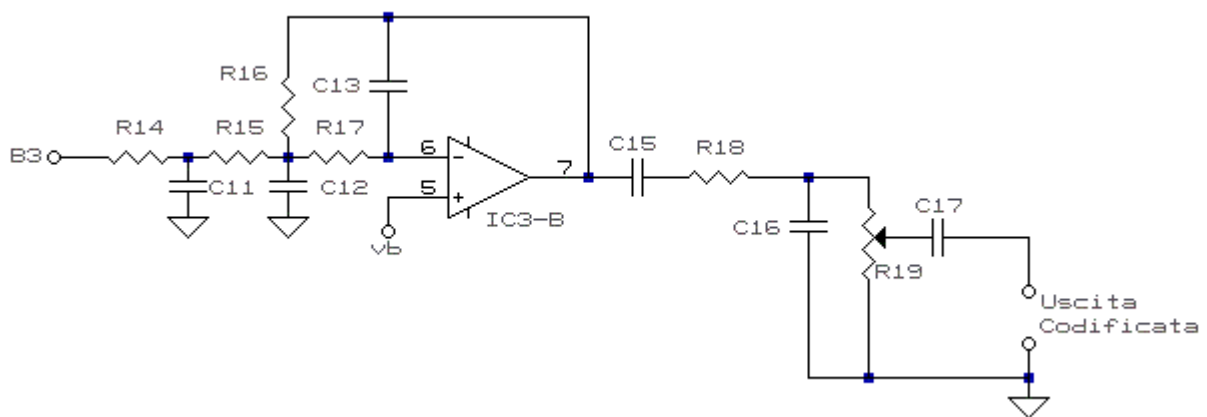


Figura 11

Il 4° blocco come tutti i blocchi che rappresentano il circuito di decodifica, uguale all'amplificatore differenziale del blocco 4 (codifica).

Anche il funzionamento è identico: si è utilizzato un amplificatore differenziale per creare un filtro passa- basso attivo del 3° ordine tarato in modo da non permettere il transito alle frequenze superiori a 3000Hz, così facendo si elimina la frequenza, in uscita del mixer decodificatore, ottenuta dalla somma del segnale vocale decodificato con quello dell'oscillatore locale.

In uscita a questo blocco, avremo il messaggio completamente comprensibile, come se nessuna modifica gli sia stata apportata.

Il trimmer R47 ed il condensatore C38 servono da adattatore di impedenza per non avere problemi con ciò che andremo a collegare all'uscita di B.F che potrà essere un altoparlante come un amplificatore di potenza ecc.

ALIMENTAZIONE

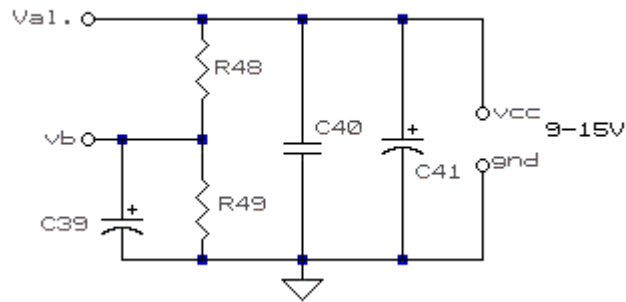


Figura 12

Questo blocco è stato creato per ottenere una tensione di riferimento V_b che sia l'esatta metà della tensione di alimentazione.

Per fare questo abbiamo usato un semplice partitore di tensione formato da R48 ed R49; essendo queste due resistenze uguali la V_b sarà la metà della V di alimentazione. La formula matematica per spiegare il funzionamento del partitore di tensione applicato al nostro circuito è:

$$V_b = V_{al} \cdot R_{49} / (R_{48} + R_{49})$$

Essendo le resistenze uguali la formula diventa:

$$V_b = 0.5 \cdot V_{al}$$

I condensatori, in aggiunta al partitore, servono per rendere più stabile il valore di tensione in modo che non si verifichino sbalzi e variazioni che potrebbero danneggiare gli amplificatori operazionali visto che questa tensione di riferimento V_b andrà a collegarsi direttamente sui loro piedini.

La tensione di alimentazione dello scambler, può essere compresa da un minimo di 9V ad un massimo di 15V in modo da creare meno problemi per alimentarlo in quanto si potrebbe benissimo applicare una normalissima batteria da 9V e rendere così il circuito portatile.

Per quanto riguarda la tensione di riferimento V_b , se il circuito è alimentato con 15V sarà di 7,5. La tensione di alimentazione sarà di 12V e in corrente continua.

**ELENCO
COMPONENTI**

RESISTENZE	CONDENSATORI	I.C.	Xtal	INTERRUTTORI
R1= 47K trimmer	C1= 1mF	IC1= TL.082	Quarzo 2MHz	Dip-switch 4 vie
R2= 22K	C2= 100,000 pF	IC2= CD.4066		2- Interruttori
R3= 470K	C3= 120 pF	IC3= TL.082		
R4= 10K	C4= 22,000 pF	IC4= CD.4060		
R5= 10K	C5= 15,000 pF	IC5= CD.4013		
R6= 22K	C6= 1,500 pF	IC6= TL.082		
R7= 10K	C7= 100,000 pF	IC7= TL.082		
R8= 5,6K	C8= 470,000 pF	IC8= 40106		
R9= 5,6K	C9= 10,000 pF	IC9= 4013		
R10= 180K	C10= 10,000 pF			
R11= 180K	C11= 22,000 pF			
R12= 180K	C12= 15,000 pF			
R13= 180K	C13= 1,500 pF			
R14= 10K	C14= 100,000 pF			
R15= 10K	C15= 470,000 pF			
R16= 22K	C16= 10,000 pF			
R17= 10K	C17= 470,000 pF			
R18= 3,3K	C18= 33 pF			
R19= 4,7K trimmer	C19= 33 pF			
R20= 2,7K	C20= 100,000 pF			
R21= 1M	C21= 100,000 pF			
R22= 4,7K	C22= 1 mF			
R23= 10K	C23= 100,000 pF			
R24= 150K	C24= 120 pF			
R25= 150K	C25= 22,000 pF			
R26= 150K	C26= 1,500 pF			
R27= 150K	C27= 1,500 pF			
R28= 10K	C28= 100,000 pF			

R29= 47K trimmer	C29= 470,000 pF			
R30= 22K	C30= 10,000 pF			
R31= 470K	C31= 10,000 pF			
R32= 10K	C32= 22,000 pF			
R33= 10K	C33= 15,000 pF			
R34= 22K	C34= 1,500 pF			
R35= 10K	C35= 100,000 pF			
R36= 5,6K	C36= 470,000 pF			
R37= 5,6K	C37= 10,000 pF			
R38= 180K	C38= 470,000 pF			
R39= 180K	C39= 47 mF			
R40= 180K	C40= 100,000 pF			
R41= 180K	C41= 47 mF			
R42= 10K	C42= 3,3 nF			
R43= 10K	C43= 1 nF			
R44= 22K				
R45= 10K				
R46= 3,3K				
R47= 4,7K trimmer				
R48= 2,2K				
R49= 2,2K				
R50= 6,8K				
R51= 100K trimmer				
R52= 1K				
R53= 1K				