MX•COM, INC. MiXed Signal ICs

APPLICATION NOTE

Variable Split-Band Scrambling (VSB)

Variable Split-Band Scrambling (VSB) Furnishes Voice Security

Introduction

Voice scrambling offers tactical security for radio dispatch communications. It takes so long, even for a dedicated eavesdropper, to unscramble your transmissions that the information would be worthless by then.

Unwanted consequences of third-party radio communications eavesdropping include foiled drug busts, unsolved burglaries and pirated business opportunities. Some mobile radio users employ voice privacy and voice security devices to scramble their communications. Most users who need voice security continue to communicate in the clear, however, for several reasons:

(1) Cost --They cannot justify the capital expense.

(2) Technology -- The poor quality of recovered audio and the radio range reduction common to many voice security systems discourage their use.

(3) Availability -- Two principal scrambling alternatives, frequency inversion and digital encryption, are not suitable for many applications. Frequency inversion offers privacy but not security; digital encryption offers high security but with a high price tag.

Semiconductor technology advances have reduced costs and improved the quality of voice security products. Variable Split-Band (VSB) scrambling has become economical because of such advances.

How it works

Filters separate the voice band (400Hz to 2700Hz) into a pair of subbands (32 pairs are possible). (See Figures 1A, 1B and 1C.) A mixer fed with a carrier signal inverts the subbands; a summing amplifier recombines them. Ordinary radio transceivers transmit the resulting variable split-band-scrambled output via an ordinary radio communications channel.

Microprocessor outputs control the split point (the frequency at which the voice band is subdivided) and change it from 4 to 60 times per second. Figure 2 reveals the “rolling code” nature of VSB scrambling. One of more than 65,000 unique user-programmable code keys initializes the pseudorandom sequence of split points. User programming commands the split point's rate of change, or “hop rate,” to vary pseudorandomly or in a fixed fashion.

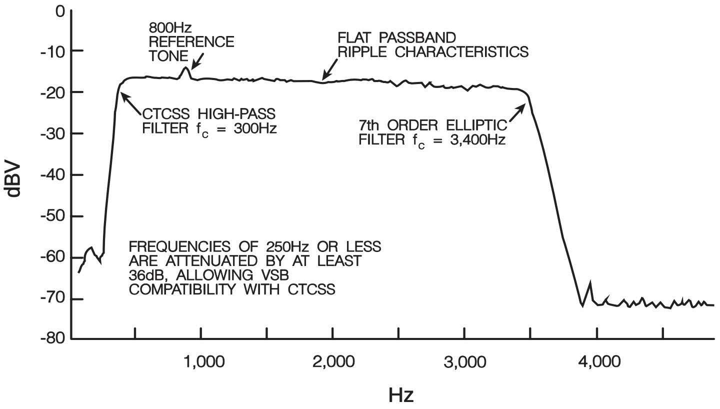

Figure 1A: Audio output of VSB filter array IC in clear mode

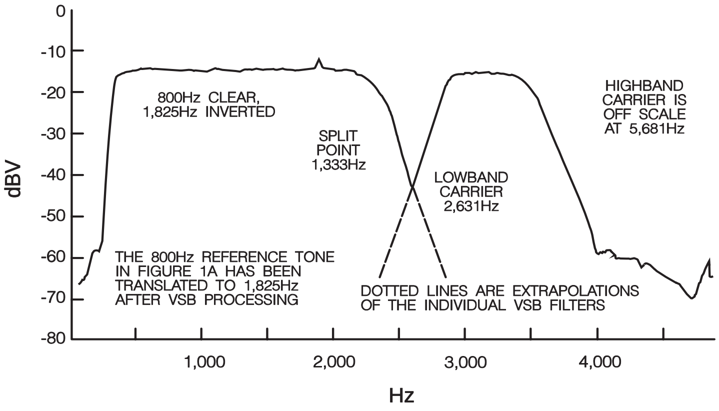

Figure 1B: Audio output of VSB filter arrray IC in "scramble" mode with split point at 2,333Hz

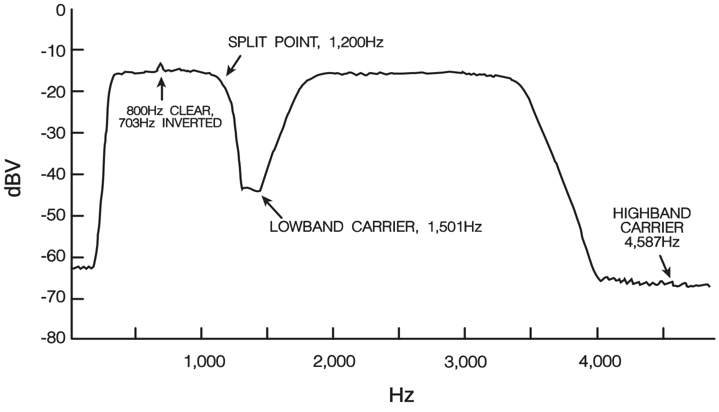

Figure 1C: Audio output of VSB filter array IC in “scramble” mode with split point at 1,200Hz

Filtering Accuracy

Optimum recovered audio quality depends upon highly accurate voice filtering. Two pairs of 7th order, switched-capacitor, elliptic filters in the VSB filter array integrated circuit (IC, on-chip) accomplish all the filtering (See Figure 3).

The transceiver's mic. audio pre-amplifier or receiver audio demodulator output feeds the VSB filter array IC's highband and lowband inputs. Within the IC, audio from each subband passes through a lowpass filter, a frequency inverter and another lowpass filter. A summing amplifier recombines the subbands. The chip includes a highpass filter that permits VSB scrambling to be used with continuous-tone controlled squelch systems (CTCSS) and other sub-audible signaling schemes.

On-chip programmable dividers with a 5-bit logic address control the 32 split points and their highband and lowband carrier frequencies. The VSB microprocessor uses the 5-bit address to generate a rapidly changing sequence of split points. Table 1 shows the exact relationship between each split point and its associated carrier frequencies.

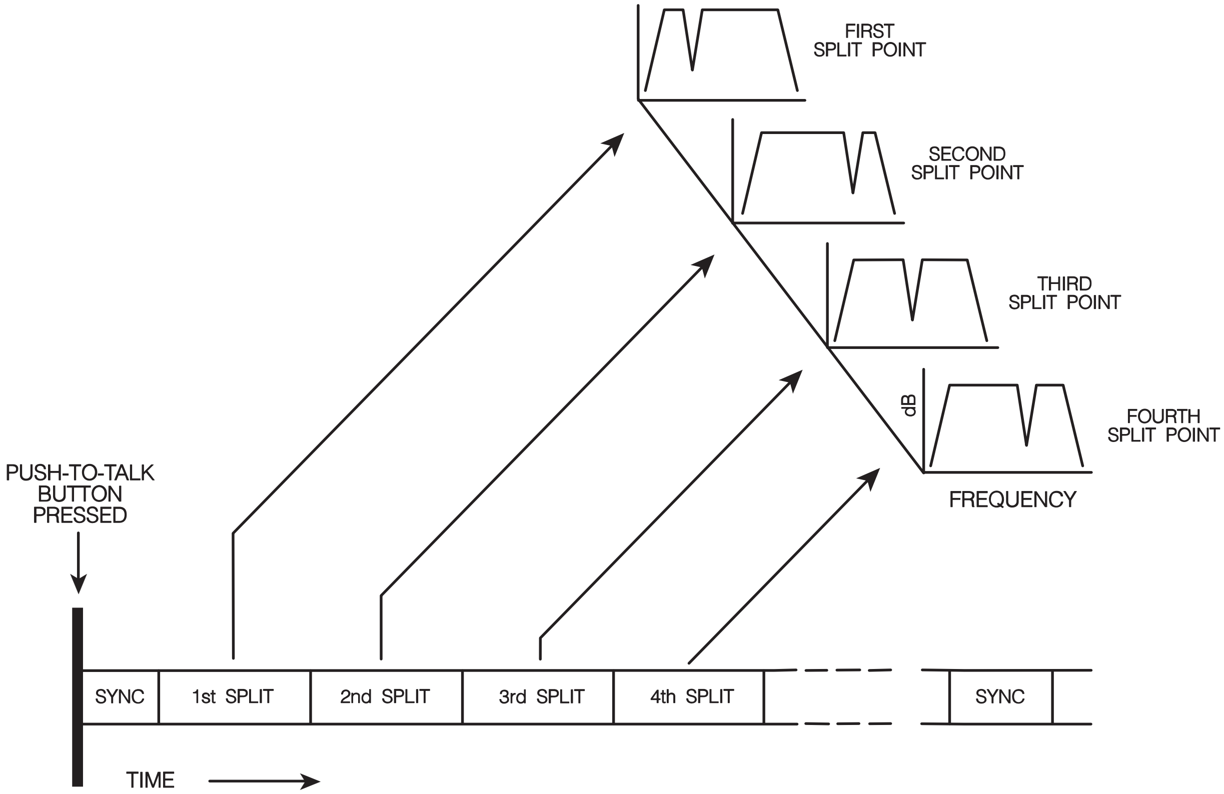

Figure 2: The effect of rolling code split points on the transmitted radio spectrum

Microprocessor Control

The VSB microprocessor performs scramble system control functions, including:

generation of split-point sequences
control of system synchronization
monitoring of the push-to-talk (PTT) line
code key selection
code key loading
selection of the secure or clear mode.

The microprocessor generates pseudorandom strings of split points initialized by one of four user-programmable code keys. Non-volatile, electrically erasable, programmable read-only memory (EEPROM) stores the code keys and other user-programmable system information (see Figure 4).

To decode a rolling, VSB-scrambled message properly, the receiver(s) must “hop” in unison with the transmitter from one split point to the next. A continuous synchronization scheme accomplishes this task. The scheme transmits 1200-baud minimum-shift keyed (MSK) data bursts every three seconds. Authorized parties can descramble transmissions even if the beginning of the message is missed, preserving mobile radio's inherent “late joining” feature.

In the absence of valid synchronization bursts, receivers revert to clear mode. The automatic reversion to clear mode (“clear voice override”) makes scrambling easier to use in systems that include some radios not equipped for scrambling.

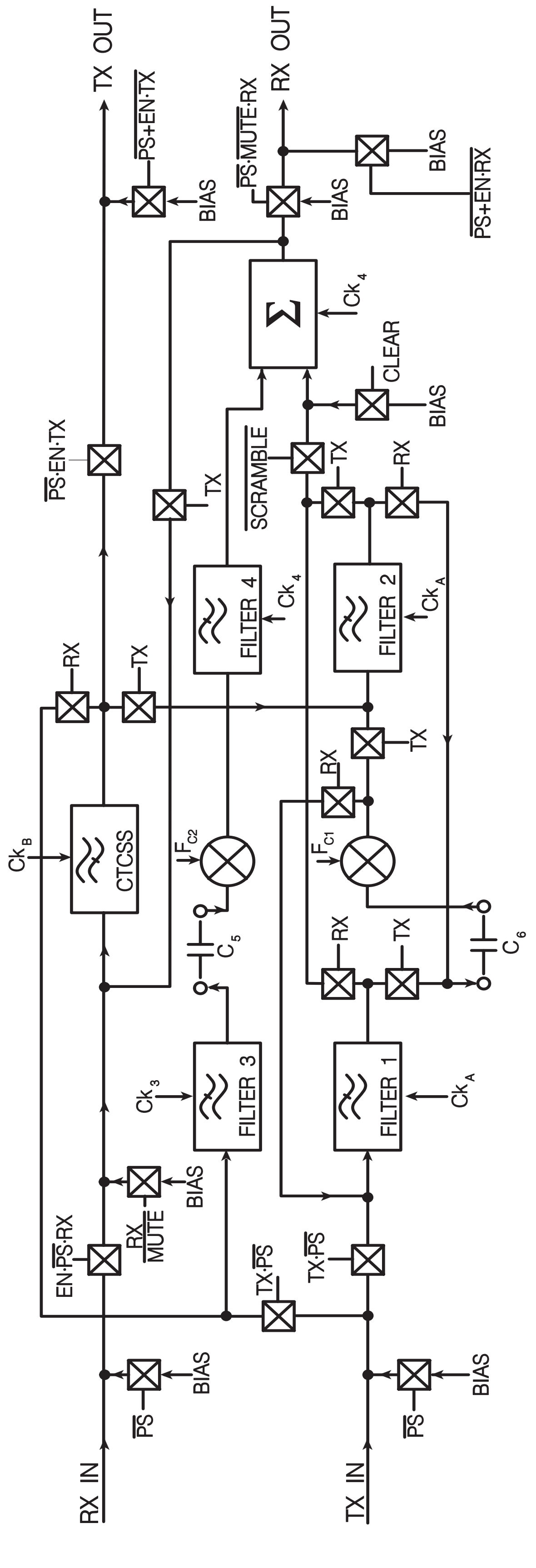

Figure 3 - Functional block diagram of the VSB filter array

Figure 3: Functional block diagram of the VSB filter array

ROM Address A_4-A_0	Split Point Hz	Low Band Carrier, Hz f_{C1}	High Band Carrier, Hz f_{C2}
00000	2800	3105	6172
00001	2625	2923	6024
00010	2470	2777	5813
00011	2333	2631	5681
00100	2210	2512	5555
00101	2100	2403	5494
00110	2000	2304	5376
00111	1909	2212	5263
01000	1826	2127	5208
01001	1750	2049	5102
01010	1680	1984	5050
01011	1555	1858	4950
01100	1448	1748	4807
01101	1354	1655	4716
01110	1272	1572	4629
01111	1200	1501	4587
10000	1135	1436	4504
10001	1050	1351	4424
10010	976	1278	4347
10011	913	1213	4310
10100	857	1157	4273
10101	792	1094	4166
10110	736	1037	4132
10111	688	988	4065
11000	636	936	4032
11001	591	891	3968
11010	552	853	3937
11011	512	813	3906
11100	471	772	3846
11101	428	728	3816
11110	388	688	3787
11111	350	650	3731

Table 1: ROM Address Programming

Only transmitting VSB units generate synchronizing data bursts, so the system resynchronizes at the transmitting station's command. Transceivers automatically transmit 80ms data bursts every three seconds after beginning a transmission. Each data burst includes:

Unit System Address -- Identifies the scrambler as part of a designated group.

Code Key File Number -- Identifies which of the four stored code keys to use.

Time Of Day -- When mixed with the secret code key, which never is transmitted, time of day tells the receiver on which part of the 50-hour long split-point sequence to begin “hopping.”

Synchronization Cue -- Tells the receiver when to change split points.

In the standby mode, VSB scrambling units scan continuously for incoming synchronization bursts that have the proper system address and file number. After receiving one such data burst, a VSB unit uses the time-of-day signal and synchronization cue to descramble the incoming message properly. Unless the receiving unit receives the proper address and file combination, it processes incoming transmissions as though they were unscrambled.

A robust error-detection algorithm, based on the British MPT 1317 signaling protocol, minimizes synchronization errors. As a safeguard, VSB scramblers retain synchronization even if a single synchronization burst is missed. If the scrambler misses two synchronization bursts in a row, the system reverts to the standby mode and scans once again for synchronization burst data.

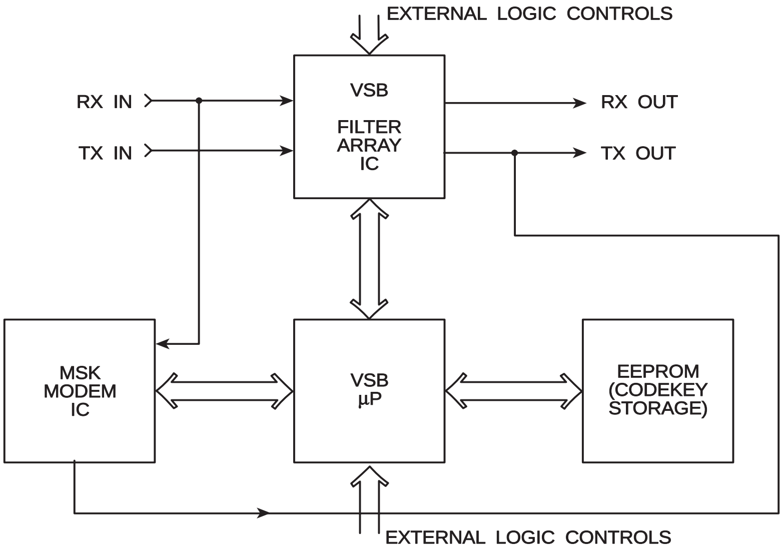

Figure 4: Block diagram of VSB Scrambler mode

Voice Security Market

Potential markets for economical voice security products include:

- *Tax*
- *Towtruck*
- *Marine and other dispatch operations whose managers have been unsatisfied with the price or performance of voice security products*
- *Municipal law enforcement agencies that lack voice security systems or that are committed to a digital encryption system that is too expensive to insall into every radio in the organization.*

Minimum-shift keyed modulation offers excellent narrowband transmission properties and superior noise performance. With MSK modulation, voice intelligibility and synchronization are lost more or less concurrently in fringe reception areas and without an appreciable loss in radio range.

An eavesdropper monitoring a VSB-scrambled transmission hears an unintelligible jumble, interrupted by bursts of digital “static” every three seconds. Consider VSB scrambling's security features:

(1) The split-point sequence permutation, which is based on a mixture of the secret code key and the time-of-day signal, changes automatically every three seconds. The code knowledge that may be obtained from one descrambled three-second sequence cannot be applied to descramble subsequent segments because they are based on different sets of pseudorandom permutations.

(2) The split-point “hop rate” may be varied pseudorandomly, further complicating the task.

(3) Each VSB-equipped radio can transmit and receive four programmed code keys, and VSB systems can accommodate as many as 16 unique code keys. Thus, a unit can transmit on one code key and receive on another.

(4) The code keys may be changed at any time. They never are transmitted. They cannot be deduced by visual or mechanical means.

VSB Scrambling Multiple Codekey Capability

Within a VSB network, up to 16 codekeys can be allocated. Four of the sixteen codekeys can be installed per radio. As illustrated below, this capability can create interesting subgroup segregation possibilities:

Scenario: Public safety departments of medium-sized cities need interagency, as well as private, intradepartmental secure communications.

Solution: A VSB Scrambling codekey allocation scheme allocates seven codekeys (A-G), four to the police force, and two each to the fire department, ambulance service, and detective unit.

User Subgroup	Installed CODEKEYS	Communications Capability
1) HQ/Supv.	All	Monitor all channels
2) Police	A	Intradepartment Only
	B	Police and Fire
	C	Police and detectives
	D	Police and ambulance
3) Fire	B	Police and fire
	E	Intradepartment Only
4) Detectives	C	Police and detectives
	F	Detectives Only
5) Ambulance	D	Police and ambulance
	G	Intrasquad, ambulance and hospital

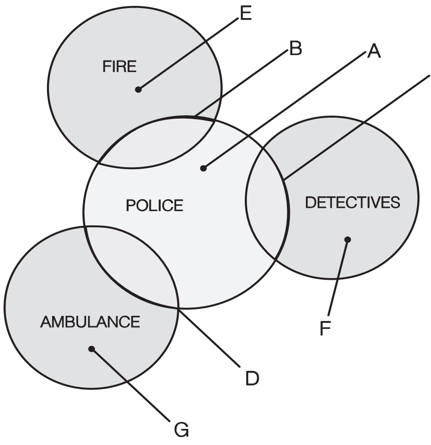

Figure 5: Multiple codekeys extend subgroup segregation possibilities in a medium-sized city's public safety

Given these security features, how difficult is it to descramble such a garbled transmission? According to two experts, it is not easy.

According to Michael Washvill, a voice and data security specialist with a federal agency, “VSB scrambling can be broken, but not in real time. The only practical attack is through trial and error. The scrambled speech must first be recorded, then divided into finite time segments according to the hop rate. Each segment is processed through a variety of split point combinations until clear speech results.”

A TRW systems engineer and former U.S. Department of Defense employee, Jim Walker, concurs: “The 'brute force' method of trial and error is the only way to break VSB-scrambled speech. Assuming that the 'bad guys' have a stolen VSB unit and no prior knowledge of the code key or code keys, 50 to 100 minutes of dedicated effort are required to descramble one minute of VSB-scrambled speech. A rule of thumb is 60:1 'grunt time to clear speech time'.”

Walker continued, “For most eavesdroppers, the potential rewards do not justify the time and effort. Two additional factors come into play. First, by the time the information is decrypted, will it still be of any use? Second, what percentage of the descrambled radio traffic will be of value?”

Given the time and perseverance required to break a VSB-scrambled transmission, two alternatives become much more attractive to those who want to eavesdrop: Steal a VSB-equipped radio or bribe someone who knows the codekey. Strict code key management procedures reduce system vulnerability to these attack methods.

To reduce the possibility of bribery, restrict code key knowledge to one person. To guard against stolen VSB units, change system code keys on a regular basis by using the VSB keyloader.

The keyloader is a portable tool that reprograms VSB-equipped radios in the field. A technician connects the keyloader's data-loading cable to a VSB-equipped radio and presses the load button to install as many as four new codekeys into each radio. Only the person with codekey management authority can program the keyloader or read its contents.

Tactical vs. Strategic

Voice security requirements can be divided into two broad categories: tactical and strategic. Tactical applications are those in which the secrecy of the message is time-dependent, such as battlefield tactical communications, most municipal police communications and nearly all dispatch communications. The tactical message retains its value for one or two hours at most. VSB scrambling serves tactical security requirements.

James Bramford, in his book The Puzzle Palace, defines strategic communications as “the high-level diplomatic, commercial and military communications that might give away a nation's foreign policy venture, where and with whom it was doing business, or what new weapons were being developed over the next few years.” Today's strategic applications demand some form of digital encryption.

In addition to the message security afforded by digital encryption or VSB scrambling, transmission security can be assured through spread-spectrum techniques, such as frequency hopping, which render the radio signal both undetectable and immune to jamming.

Most mobile radio users have tactical voice security requirements. For these applications, VSB scrambling offers a practical, economical alternative to digital encryption systems. VSB scrambling requires no modification of the installed communications network. It has little or no impact on radio range.

As dealers and users become more comfortable with VSB and other new scrambling technologies, foiled drug busts, unsolved burglaries and pirated business opportunities resulting from unauthorized eavesdropping will become things of the past.

Authors:

Steve Kelley and Hank Wallace

Reprinted with permission from the May 1988 issue of Mobile Radio Technology. Copyright 1988, Intertec Publishing Corp., Overland Park, KS. All rights reserved.