NEW APPROACHES TO SECURING BASIC SERVICES

Graham S. Stubbs
Vice President, Science & Technology

OAK Communications Inc.
San Diego, California 92127

ABSTRACT

The shift towards increased revenue generation from basic services (and a corresponding decrease in multi-tier pay revenues) strengthens the need for means to protect those basic services from signal piracy. In the past, scrambling and addressability have been used primarily to protect pay services. Now there is clearly a need for a cost effective method to secure basic channels without rendering existing equipment, especially plain converters, obsolete.

This paper discusses converter compatible solutions to the problem, and describes two specific examples, each of which is capable of being overlaid on an existing system already equipped with converters.

The more secure of the approaches described applies encryption technology to provide a very high degree of security. The other approach is an add-on decoder, examples of which have been available for some time.

INTRODUCTION

Signal security techniques, as applied in cable today, are designed primarily to control the delivery of pay services and to protect revenues. Addressable methods have been introduced to enhance Pay TV operations by making the changing of subscription packages less costly to the operator and more convenient to the subscriber. Addressability is almost a pre-requisite for most forms of PPV. Security in scrambled signals has been enhanced by the use of addressability for delivery of decryption keys.

While it is true that a few cable systems scramble basic service channels, the fact is that encoding of television signals has been directed primarily at pay services. Yet the greater part of cable systems' revenues in 1986 are projected to come from basic subscriptions, and in future years the percentage of income from basic service is expected to increase. Most cable operators admit to some degree of theft of basic service, but few have taken steps to make "basic" signals more secure.

Some pay program material has to be scrambled for obvious reasons. And yes, of course it's simplest to deliver basic programs in the clear, either directly to the television receiver or through an inexpensive converter. However, there can be some interesting challenges for cross-innovation in security methods.

In an existing addressable system it is possible to scramble some or all of the basic channels in the same manner as pay channels. However this means supplying converter/decoders (with their attendant capital costs) to all subscribers, which can place a greater burden on the security of older and less sophisticated scrambling techniques.

Most cable subscribers today are supplied with non-addressable converters of either the programmable (converter-decoder) variety, or non-programmable (plain-vanilla) type. This paper focusses on methods to secure basic services in systems, which today are non-addressable, without rendering the non-addressable converters obsolete.

Functional Requirements

Before discussing the details and merits of specific approaches, it is as well to review some observations regarding "basic" requirements.

- Security -- As the value of the entertainment product continues to increase so will the ingenuity and determination of pirates. Defeating secured "Basic" as well as scrambled "Pay" could be looked upon as twice as rewarding by the pirate.
- Compatibility -- A successful approach should not obsolete existing subscriber terminal equipment.
- Cost -- No technique will be acceptable unless there is a financial pay-off.
- Addressing -- Individual device control is a necessary component of a secure system. However the multi-tier/multi-function controls, usually incorporated into addressable pay systems, are not necessary for basic services.

Two Proposed Methods

In order to illustrate the possibilities of using Pay TV security techniques to protect basic services, two methods will be outlined having in common the use of an addressable device located on the subscribers premises, inter-faced with an existing converter (or non-addressable converter/ decoder). There are significant differences between the two approaches related to:

- o adaptability to other uses
- o security

Post-Converter Addressable Decoder

Devices of this kind have been offered for several years by a number of manufacturers of addressable systems. These devices have been marketed primarily for the addition of pay services to systems equipped with non-decoder type converters. Usually they have been designed for system compatibility with converter/decoders designed to decode the same scrambled signals.

A representative block diagram (Fig. 1) is shown of one of these devices (OAK TCM-1) which employs out-of-band addressing. The decoder is equipped with four connectors. The signal from the drop cable loops through the decoder to permit access to the out-of-band FSK addressing channel, and is connected to the converter input. After channel selection, the converter output signal loops again through the decoder in order to accomplish program tag recognition and decoding. The decoder output is connected to the television receiver.

The FSK receiver, similar to that used in other addressable devices, extracts serial addressing control data. The control data contains, in decoder specific messages, the identity of authorized program levels which are stored in the decoder. The output signal of the converter passes through the decoder tag detection circuit. If the selected channel is scrambled, the decoder automatically extracts program level information from the tag signals which are transmitted in the vertical blanking interval. Control circuits compare the tag levels with stored authorized program levels, and if there is a match, activate the decoding circuit. The TCM-1 uses the same dual-mode sine-wave sync suppressed scrambling as OAK's Total Control system.

This type of decoder can be used in a system presently employing a mixture of plain converters and converter/decoders (either addressable or non-addressable) to permit scrambling of all channels, including, of course, basic channels. Any scheme involving encoding of basic channels naturally requires all basic subscribers in the system (or section of the system in which scrambling is employed) to be provided with appropriate decoding devices.

Once installed, the same decoder can be used to extend Pay coverage without additional investment in converter/decoders.

As the decoder utilizes signals which have already passed through a converter, particular attention must be paid in this type of decoder to the effect of converter fine tuning. In the device described, frequency sensitive portions of the decoding detection and tag detection circuits operate at a special intermediate frequency. AFC is used to maintain accurate frequency control of this IF. The decoder is designed to be system compatible with the addressing commands of its converter/ decoder counterpart.

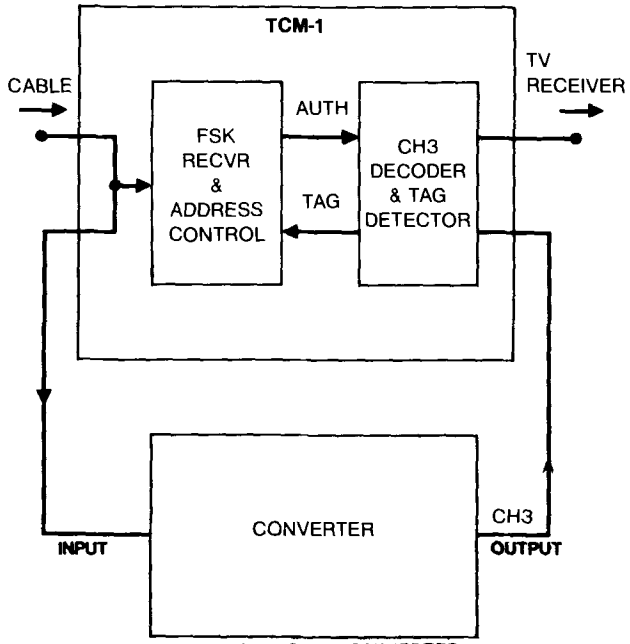

FIG. 1. POST-CONVERTER ADDRESSABLE VIDEO DECODER

Devices of this type are relatively inexpensive (approximately one half the cost of a converter decoder), and are already developed and available. They employ, however, relatively unsophisticated analog scrambling.

Post-Converter Audio Restorer

This section describes a concept, not a product already developed for low cost manufacture.

Security of basic channels is achieved by digital encoding and encrypting the audio portions of each channel for transmission through the cable system in portion of the cable spectrum dedicated to the high speed data transmission of audio (for example a single 6 MHz channel could easily carry 10 stereo channels).

Each controlled television channel is transmitted with clear video but with no analog audio modulation. Instead a tag signal, identifying the channel, is transmitted on the sound carrier.

The equipment provided to the subscriber is connected in the configuration shown in Fig. 2. Again a four connector device is used. The cable signal loops through the decoder allowing the high speed program-audio data to be extracted. The high speed data channel comprises digital encryupted audio, error protection, and control signals.

After television program selection by the converter, the signal passes to the tag detector section of the decoder (Fig. 3). If the channel selected is "tagged," the decoder's tag receiver identifies the tag signal, and seeks a matching digitized audio signal from the receiver of high speed data by control of the demultiplexer (DEMUX).

The audio data is decrypted and converted to analog audio in the DECRYPTER/DAC circuit. It then modulates a Voltage Controlled Oscillator (VCO) used to generate a restored audio carrier.

The signal from the converter is converted to an IF, passes through a filter to remove the sound carrier transmitted through the cable system, and is recombined with the restored audio carrier. Precise phase lock loop techniques are used in the frequency conversion and VCO circuits to assure maintenance of intercarrier frequency accuracy and to minimize incidental FM noise.

As shown the signal passed to the television receiver is a conventional monaural signal, however this scheme is readily extendable to BTSC (MTS) audio.

The concept described here is based on the encryption concepts already employed in the SIGMA product and has the potential to be extremely secure. It is compatible with existing converters and can be used to supplement the security of a wide variety of existing analog scrambling techniques.

This device also is estimated to be approximately one-half the cost of a new converter/decoder of similar security.

The principle can be extended to use without a converter. Used with an IS-15 compatible receiver, a device of this kind could recognize tag information in the broadband IS-15 audio output, and supply audio derived from the high speed data stream directly to the television receiver.

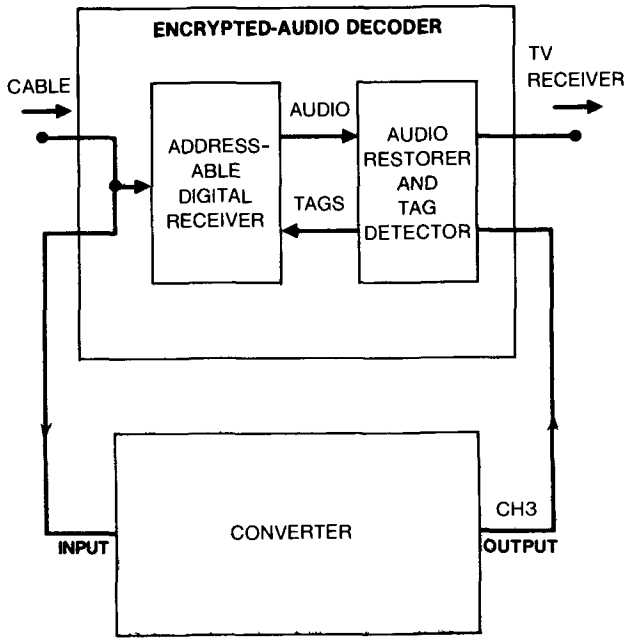

FIG. 2. POST-CONVERTER AUDIO RESTORER

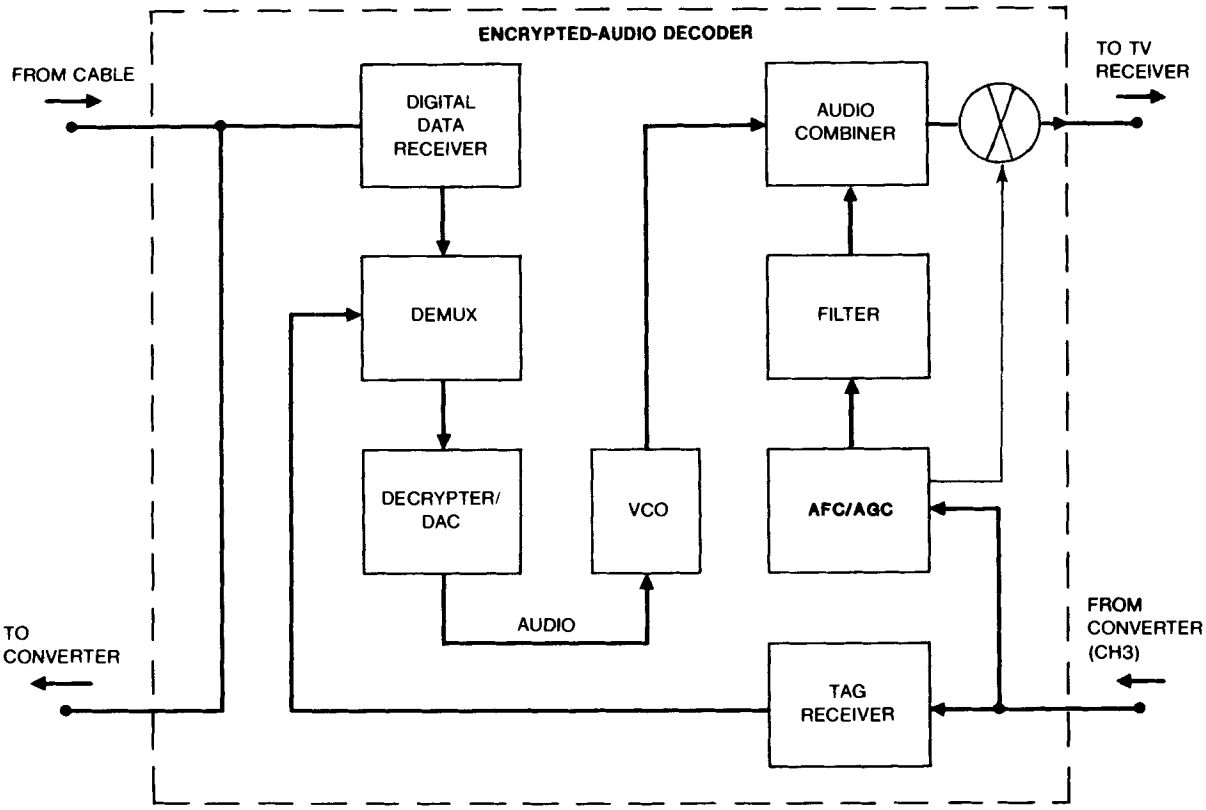

FIG. 3. AUDIO DECRYPTOR/RESTORER

Comparison of the Two Methods

Both proposed methods employ addressable devices, using time-proven tag-matching methodologies. In both cases basic service can be authorized as a single tier, or split into subtiers.

The post converter-decoder can be used to control pay services without the use of additional scrambling equipment. The audio denial method, on the other hand, cannot be used to protect all pay services without some additional means of assuming visual privacy. It can be used to enhance the security of analog scrambling methods used to protect pay services.

In both cases, the home terminal device costs about the same -- about half the cost of a converter-decoder. Both techniques are designed around the use of existing converters with the assumption that the converters still have significant remaining useful lives.

The decoder method has limitations in relation to stereo. Inherent in the audio denial method, however, is the ability to deliver a stereo signal.

The greatest contrast between the two techniques is the degree of security. Analog video scrambling techniques such as sine wave or gated sync suppression are relatively unsophisticated. Digital encrypted audio, on the other hand, is now well established as the state-of-the-art in securing cable television signals.

Conclusions

In the cable industry scrambling and addressable techniques have in the past been applied primarily to protect Pay signals. The financial indicators suggest, moreover, that cable is becoming even more dependent upon revenue from basic services. It is time to consider the application of the developments in program security technology to the protection of these "basic service" revenues.

Two converter-compatible methods of securing basic services have been outlined and compared. Regardless of the specific advantages or disadvantages of these particular techniques, it is clear that Pay TV technology can already provide some useful tools to protect cable's primary revenue stream from piracy.

It is timely to re-examine our priorities and determine whether all our efforts to secure signals within cable should be directed at Pay TV and PPV -- or whether perhaps some of this ingenuity is better re-directed to securing "basic!"