COMMERCIAL APPLICATIONS OF ENCRYPTED SIGNALS

M. Davidov, V. Bhaskaran, T. Wechselberger

OAK Industries Inc., Rancho Bernardo, California

ABSTRACT

The use of encryption technology in the delivery of premium television is described. Signal security concepts such as scrambling, encryption, key-management etc. as applied in the ORION and SIGMA systems are discussed*. In order to asess the effects of transmission link and system induced impairments, an analytical procedure is developed for the encryption method used in ORION/SIGMA. System performance curves obtained from the analysis are presented. Finally, potential applications of ORION, SIGMA systems in the secure transmission of non-video information is discussed.

1. INTRODUCTION

In recent years, we have evidenced increasing concern for privacy and security of information. Information is now being viewed as a commodity with commercial value and hence, like material goods, security measures must be taken to protect it from theft. In the commercial arena, there are several instances, wherein, security measures are essential for the system to be commercially viable e.g. electronic funds transfer systems, software distribution, pay-TV broadcasts. Cryptographic techniques are being applied in such systems to realize high levels of information security. Development of such crypto-systems has been motivated by recent technological advances in LSI/VLSI systems and this in turn has led to the implementation of cost-effective cryptographic protection schemes.

Cryptographic methods used in ORION and SIGMA systems (for the secure transmission of TV programs) is the focus of this paper. By a judicious mix of analog scrambling, digital encryption and effective key-management, a high level of security at low-cost is achieved in these systems. This paper is organized as follows. In Section 2, factors affecting the design of secure transmission scheme for TV programs are discussed. Signal security methods used in ORION and SIGMA are described in Section 3. In Section 4, we provide a simple analysis which takes into account the specific encryption method used in ORION/SIGMA; this analysis is used to derive performance curves for ORION/SIGMA systems in the presence of typical transmission link and system impairments. Examples of potential applications using ORION/SIGMA systems for secure transmission of non-video information are discussed in Section 5 and concluding remarks are made in Section 6.

*ORION and SIGMA are manufactured by OAK Ind.

2. TV SIGNAL SECURITY CONSIDERATIONS

In the past, TV systems transmitted only video and audio. TV systems today (e.g. ORION, SIGMA) however can handle diverse information sources such as program video, audio (monoaural/stereo/second-language), control data (is used to control the communication network and provide the receiver with the commands needed for it to function properly) and auxilary data services (e.g. video-text, home-banking, two-way interactive communications). There is considerable expense incurred in providing such diverse services; thus the system operator has to resort to direct subscriptions to pay for these services (referred to as "Pay-TV"). In order to ensure the revenue generating potential and to prevent unauthorized access to such services, a secure transmission scheme is needed.

There are several considerations which strongly affect the design/selection of signal security methods for TV:

1. Level of security
2. Network attack scenarios
3. Network compatibility
4. Human factors, and
5. Cost

Let us briefly examine each of these issues.

Level of security The type of information handled by the TV system and the medium over which the information is transmitted influence the level of security desired.

Major objective of TV systems is to deliver video programs; for these sources, entertainment value is contained in video and audio. Hence, any security scheme which denies unauthorized access to any one of these signals is considered acceptable (a "medium" security video scheme and a "high" security audio scheme is used in several commercial systems today e.g. ORION, SIGMA). As observed earlier, TV systems also transmit control data; this channel contains decoder and program specific information and hence is a vital communication

84CH2069-3/84/0000-0307 $1.00 © 1984 IEEE

link. Its contents must be conveyed in a highly secure manner. If a TV system provides non-entertainment services, different levels of security may have to be applied to each of these services e.g. home banking may require a higher level of security than video-text.

TV signals are transmitted over terrestrial, cable and satellite links (C-band, Ku-band). There are differing opinions on the level of security needed in these links. The operator of a cable distribution network, in lieu of a high-cost, high security scheme, may opt for a low cost system that offers lower signal security. Selection of the lower security scheme may be justifiable; a cable system provides some protection against piracy because such a network is difficult to tap into without detection and in such a system, non-paying subscribers can be denied the service by having their link to the system isolated. In a terrestrial link, risk of detection is low since there is no direct contact between subscriber and system operator unlike the cable distribution network; hence a high security scheme would be preferred in this environment. In distribution of TV signals by satellite, the signals are potentially available to a large number of homes and signal piracy on a large scale is feasible. Systems offering high security are preferred here.

Network attack scenarios The security method must take into account possible system attacks. Potential network attack scenarios in CATV transmissions is shown in Fig. 1. These schemes include simple circuit changes in the receiver, local synthesis of valid control signals and add-on hardware to decode the signals and to tamper with the cable link. To thwart such network attacks, the security scheme should be devised in a manner such that (1) unauthorized access to transmitted signals must offer no entertainment value, (2) one-time system defeats must not be possible - implies that a time-varying signal security scheme must be used, (3) observation of transmitted signals must not offer any clues about the actual signals, and (4) there must be contact between sender and receiver via a control channel. The information in the control channel must be such that interruption of this channel must disable decoder and this channel must provide decoder with information not merely as to when to decode but how to decode.

Network compatibility The security scheme must not impose excessive requirements on the network and for wider acceptability, it must posess the same bandwidth and other signalling requirements as conventional TV systems e.g. signals transmitted using the secure transmission scheme must be capable of being transmitted in 6MHz RF bandwidth in CATV/terrestrial links employing VSB-AM, and must fit in a 27-36MHz (C-band) and 22-24MHz (DBS) satellite link employing FM modulation. The security scheme employed in these links must be resistant to the impairments dominant on the link e.g. in CATV links, multipath is dominant; hence signal security methods which rely on information smearing for its security (output feedback schemes) can result in degraded system performance when multipath is present.

Human factors In a commercial environment, the end user must not be inconvenienced when system penetrations occur since long-term survival and profitability are based on favorable consumer attitudes. Hence, Draconian methods such as closing down the link, changing security procedures and widespread investigations etc. in the event of suspected system intrusions must be avoided.

Cost Schemes offering very high security are presently being realized at high cost and thus are not amenable to commercial applications. In a TV environment, cost constraints are very severe since the security scheme is only one aspect of the overall system required by the consumer. In a CATV system since risk of detection is high, desired level of security can be low and hence a low-cost security scheme is preferred (low-cost usually implies lower security). The signal security method should be such that the cost to derive useful information is low for an authorized user, whereas, the cost to derive useful information from the intercepted signal must be prohibitive.

Prior to describing the signal security techniques used in ORION/SIGMA, let us examine basic signal security concepts.

Signal security concepts Signal security methods which meet one or several of the design considerations can be realized with analog scrambling or digital encryption. Analog scrambling or digital encryption is an invertible transformation T

$$T : A \longrightarrow S \qquad (1)$$

Here, A is the scrambler(encryptor) input and S is the output. By analog scrambling, we imply A and S to be analog signals and the transformation T is implemented in analog or digital domain. By digital encryption, we imply A and S to be digital signals and T is a digital process (typically a bit oriented process). Transformation T is controlled by another process and T is represented as T(k). For correct descrambling/decryption, decoder must posess k, transformation T and S.
Note that analog scrambling can be achieved at RF or baseband. RF systems have traditionally been implemented at low-cost; however, presently, the trend is towards baseband systems due to the flexibility offered by baseband signals (such signals can be easily transmitted over different transmission media).

The control process i.e. the mapping from k to T(k) is typically a digital process and k is referred to as the "key". Several factors must be considered in the design and handling of the key:
1. The key must be used to inform decoder not merely when to descramble/decrypt but how to descramble/decrypt - this makes unauthorized key-less descrambling expensive.
2. Key must be made time-varying to prevent one-time system defeats.
3. Scrambling or encryption by itself does not ensure signal security. In order to maintain the integrity of the scrambling/encryption process, the key must be handled in a secure manner (referred to as the "key-management" problem). The key must not be available via a fixed algorithm in the decoder. In a TV environment, due to the large number of subscribers, traditional means of

delivering keys e.g. courier, mail etc. are not feasible. Instead, an electronic key distribution scheme could be used e.g. the keys can be made part of the information to be transmitted and by encrypting these keys under some master key, a secure key distribution scheme is achieved.

In the next section we describe the ORION and SIGMA systems from a signal security viewpoint. A possible solution to the key management problem as implemented in ORION/SIGMA systems is also discussed.

3. ORION/SIGMA SYSTEM SECURITY

ORION and SIGMA systems provide secure transmission of video, audio and control data. Block diagram of a transmission scheme employing the ORION system is shown in Fig. 2a; in Fig. 2b, use of the SIGMA system in a CATV scheme is shown. In general terms, ORION and SIGMA systems are similar; however, individual system parameters have been optimized for the specific transmission environment.

Signal security methods used in ORION/SIGMA is illustrated in Fig. 3. Digital encryption was ruled out for video due to bandwidth and cost constraints (bit rates around 80 - 120 MBps are generated when color signals are digitized. It is not possible to transmit this high rate information over 6MHz CATV/terrestrial links without some form of data compression. Compression schemes cannot be realized inexpensively). Instead, of digital encryption, a low-cost, analog scrambling method capable of offering good scrambling depth is used (for a discussion of the scrambling method see ref. 1). The scrambling function is controlled by a key as shown in Fig. 3.

Audio security is achieved by encrypting the digitized audio signals. Digitization causes bandwidth expansion; however the encrypted audio signals can be easily transmitted in the available bandwidth of CATV/terrestrial/satellite links using a TDM scheme (encrypted audio bits are transmitted during video line blanking interval).

A digital control channel is also transmitted. This control channel contains descrambling and decryption keys, decoder and video-program specific information. Control channel information is encrypted. In SIGMA, the control channel consists of two channels (1) a GLOBAL channel transmitted using FSK and all decoders tune to this channel, (2) a LOCAL channel transmitted using TDM by inserting this channel in the vertical blanking interval. In ORION, only the local channel is available.

The encryption method used for audio and control data is the cipher-feedback scheme. This method is chosen over the bit-by-bit encryption method due to its good synchronization properties and its ability to provide message authentication (e.g. in a bit-by-bit encryption scheme for audio, if intruder has knowledge of sampling frequency, bits/sample etc., by merely altering few of the encrypted audio most significant bits, intelligible audio may be obtained). From a transmission viewpoint, a cipher-feedback scheme causes error propagation; a bit error probability analysis for the cipher-feedback scheme used in ORION/SIGMA is performed in Section 4.

As observed earlier, keys used in scrambling and encryption are transmitted in the control channel. In Section 2, it was noted that these keys must be transmitted in a secure manner. The ORION/SIGMA solution to this key management problem is illustrated in Fig. 4. A multi-level key distribution scheme is used in which there are three key variables. These include a decoder specific key (unique to each decoder), a variable second level key common to all legitimate users and the encrypted service keys (used for descrambling/decryption). The service keys are time-varying.

4. ORION/SIGMA SYSTEM PERFORMANCE

Due to transmission link and system imperfections received control and/or audio bits (encrypted) will be in error. In this section, it is our intent to estimate the effects of these bit errors on descrambled video, decrypted control and decrypted audio.

Error enhancement due to cipher-feedback The cipher-feedback scheme causes error propagation (a bit in error at decryptor input can cause several bit errors at decryptor output). The encryption/decryption system is modelled as shown in Fig. 5. Due to transmission errors $E(i)$, $B(i) \neq \hat{B}(i)$. If For the decryptor, we can write

$$\hat{B}(i) = B(i) \oplus \hat{E}(i) \quad \oplus \text{ is Mod-2 addition} \qquad (2)$$

$$\hat{E}(i) = E(i) \oplus \sum_j T(j)E(i-j) \quad \sum \text{ is Mod-2 addition} \qquad (3)$$

$$\begin{aligned} Pr^*[B(i) \neq \hat{B}(i)] &= Pr[\hat{E}(i)=1] \\ &= Pr[E(i)=1]Pr[\textstyle\sum T(j)E(i-j)=0] \text{ OR} \\ &\quad Pr[E(i)=0]Pr[\textstyle\sum T(j)E(i-j)=1] \end{aligned} \qquad (4)$$

Note that $T(j)$ is binary valued and time-varying. At any given instant, let N be the number of '1' valued $T(j)$ and let P be the probability that $E(i-j)$='1'. Then,

$$Pr[\textstyle\sum T(j)E(i-j)=0] = Pr[\#\text{ of } E(i-j)=1 \text{ is even among N } E(i-j)=1] \qquad (5)$$

(5) can be shown to be

$$\frac{1 + (1 - 2P)^N}{2}$$

Using (5) in (4), we obtain

$$\begin{aligned} Pr[\text{decrypted bit error}] &= (P/2)[1+(1-2P)^N] + \\ &\quad ((1-P)/2)[1-(1-2P)^N] \\ &= (1/2)[1-(1-2P)^{N+1}] \end{aligned} \qquad (6)$$

Decrypted control channel errors, video descrambling errors due to wrong descrambling key and decrypted audio error probabilities can be derived from (6) as will be shown now.

Control channel errors Control channel information including decryption keys is transmitted in encrypted form (cipher-feedback encryption). A 6 x 8 row-column parity scheme is used on the encr-

*Pr is abbreviation for Probability.

ypted bits. In the decoder, a 2 out of 3 majority voting scheme is used to accept/reject control channel messages. Thus,

P = Pr[bit error at decryptor input]
  = Pr[2 out 3 control channel messages in error]

and

$$\Pr[\text{message in error}] = \binom{48}{2} Pb^2 (1-Pb)^{46} \quad (7)$$

Pb is the transmission link bit error probability. Depending on the modulation format, transmission link carrier-to-noise ratio versus Pb relationship is usually available. Decrypted control channel bit error probability (henceforth denoted as Pd) can be easily computed using (7) in (6) for given Pb and N.

Video descrambling errors Erroneous descrambling keys can result in descrambled video errors. Using (7) in (6), descrambling key error probability Pd can be computed. Assuming one descrambling key controls upto 30 frames of video descrambling and assuming a key change every second, number of seconds between video frame errors can be computed as

$$1/(30 \times Pd) \quad (8)$$

Decrypted audio errors Audio errors are caused by wrong decryption key and/or wrong decryptor input audio bits. Using (6), decrypted audio bit error probability can be written as

$$[(1-Pd)/2][1-(1-2Pb)^{N+1}] + (Pd/2)[1-(1-2Pd)^{N+1}] + (Pd/2)[1-(1-2Pb)^{N+1}] \quad (9)$$

Calculated error probabilities Various error probabilities determined from (6)-(9) are summarized in Fig. 6,7. For the calculations, we account for the time-varying nature of T(j) by assuming a uniform distribution on N, where the N values are distributed between 2 and 32 (determined from the key-size and decryptor shift register size).

Calculations in Fig. 6 were performed for a SIGMA system. Here, curve labelled IDEAL is for the case of no encryption and no multipath. Curve labelled ACTUAL includes multipath effects, receiver imperfections (5deg RMS phase error in demodulator, data detector peak timing jitter = 5% of bit duration) and no encryption. In all cases, gaussian noise effects are included. Curve for Pd (control channel decrypted bit error probability; also descrambling/decryption key error probability) is derived using ACTUAL, (7) and (6). Decrypted audio bit error probability is derived using (9) with Pb as per ACTUALand Pd as computed. From these curves, it is seen that cipher-feedback degrades audio performance by atmost 1.5dB at error probabilities around 1E-5. In CATV systems, worst case C/N (around 34dB) and poor multipath yields acceptable performance in audio and control channels even with the error propagating cipher feedback scheme.

In Fig. 7, we show performance results for the ORION system with discriminator and PLL type demodulation (ref. 2 contains details on these demodulators). Typical operating conditions are C/N 10dB for discriminator and 8dB for PLL. From Fig. 7 and actual observations, it is concluded that the cipher-feedback scheme yields negligible degradations while ensuring high levels of security.

5. APPLICATIONS FOR NON-VIDEO SOURCES

The basic ORION/SIGMA transmission scheme can be used to handle non-video sources. One can envision a host of applications, wherein, the signal security methods and the transmission schemes as embodied by the ORION/SIGMA systems can be radily used. Video-text for instance, can easily be incorporated as part of the control channel. Other digital data sources depending on their bit rate can also be time-division multiplexed with the existing control channel data. In an application where there is no need to transmit video, the entire video signal duration can be used to handle non-video information. For instance, in a commercial application concerning the secure delivery of music (a pay-music analogue of pay-TV), analog music channels could be digitized and encrypted as per the ORION/SIGMA method and be transmitted using these systems so that secure transmission of music is achieved - upto 11 stereo channels can be transmitted using such a scheme .

6. CONCLUSIONS

In this paper, we have described the signal security methods applied to the transmission of TV programs. Signal security methods used in two commercially available systems ORION and SIGMA were described. An analysis was developed to asess the effects of transmission errors on decrypted signals. From the performance curves derived from the analysis, it was concluded that the cipher-feedback scheme causes only marginal degradations under normal operating conditions; synchronization and message authentication benefits of such an encryption method make it more desirable than the simpler bit-by-bit encryption method. Potential uses of the ORION/SIGMA secure transmission format for non-video sources were briefly discussed.

REFERENCES

[1] V. Bhaskaran, M. Davidov , "Video-Scrambling, Overview", Intnl. Conf. Consumer Electron., 1984.

[2] M. Davidov, V. Bhaskaran, "Scrambled C-band DBS-Like Services", Intnl. Conf. Consumer Electron., 1984.

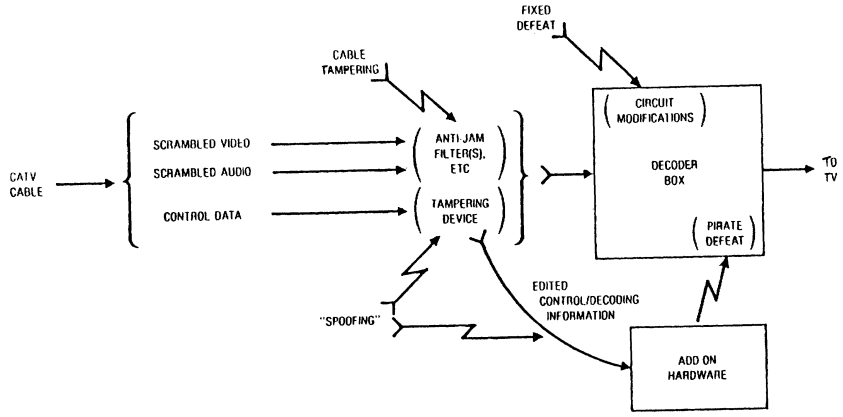

Fig. 1: CATV Network Attack Scenarios

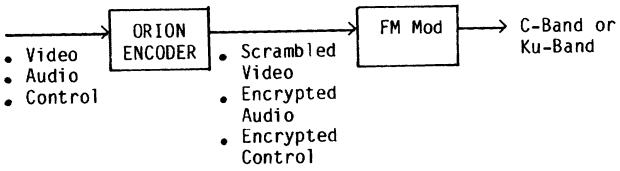

Fig. 2a: ORION System In Satellite Link

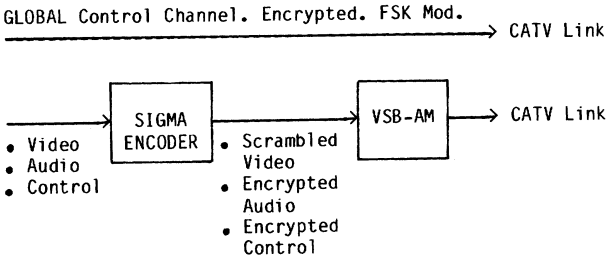

Fig. 2b: SIGMA System In CATV Link

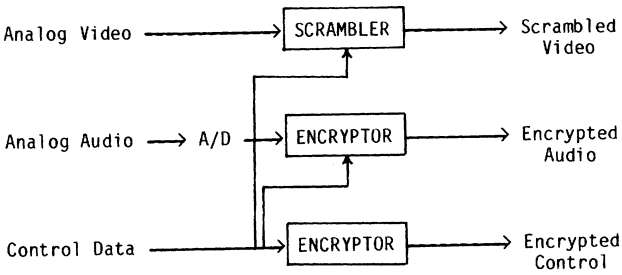

Fig. 3: ORION/SIGMA Signal Security Scheme (Encoder)

22.5.5

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.