United States Patent [19]

Wechselberger et al.

[11] **Patent Number: 4,531,020**

[45] **Date of Patent: Jul. 23, 1985**

[54] **MULTI-LAYER ENCRYPTION SYSTEM FOR THE BROADCAST OF ENCRYPTED INFORMATION**

[75] Inventors: **Anthony J. Wechselberger,** San Diego; **Leo I. Bluestein,** Rancho Bernardo; **Leo Jedynak,** San Diego; **David A. Drake,** Escondido; **Larry W. Simpson,** Poway, all of Calif.

[73] Assignee: **Oak Industries Inc.,** Rancho Bernardo, Calif.

[21] Appl. No.: **401,258**

[22] Filed: **Jul. 23, 1982**

[51] **Int. Cl.**[3] **H04K 1/02**

[52] **U.S. Cl.** **178/22.08;** 358/122; 358/123

[58] **Field of Search** 178/22.08, 22.09, 22.13–22.16; 375/2.2; 455/26–28; 358/114, 122, 123

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,193,131	3/1980	Lennon et al.	178/22.08
4,203,166	5/1980	Ehrsam et al.	178/22.09
4,288,659	9/1981	Atalla	178/22.08
4,292,650	9/1981	Hendrickson	358/114
4,323,921	4/1982	Guillou	358/114
4,337,483	6/1982	Guillou	358/114
4,348,696	9/1982	Beier	358/114
4,354,201	10/1982	Sechet et al.	358/114
4,388,643	6/1983	Aminetzeh	358/114
4,460,922	6/1984	Ensinger et al.	358/114
4,464,678	8/1984	Schiff et al.	358/122

FOREIGN PATENT DOCUMENTS

WO81/02961	10/1981	PCT Int'l Appl.	358/122
WO83/01881	5/1983	PCT Int'l Appl.	358/122

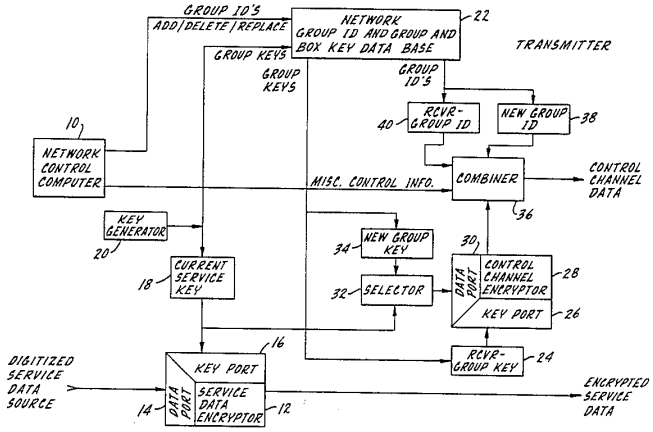
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—Kinzer, Plyer, Dorn & McEachran

[57] **ABSTRACT**

A method of controlling the simultaneous broadcast of enciphered digital information signals, for example in a radio or television broadcast environment, to a plurality of subscribers provides several levels of enciphering keys. The broadcast digital information signal is in a broadcast common service enciphering key and communication between the transmitter and subscribers may take place in a box key or in a group enciphering key common to a group of subscribers having a common interest in the reception of broadcast signals of a particular type. Each receiver will decipher the broadcast digital information in a specific service key which is common to that broadcast. The service key may be changed at one or more subscribers by communicating the change in the service key to the subscribers by means of the group enciphering key. Further, the group enciphering key may be changed at one or more subscribers or new groups may be formed among subscribers by communicating to the subscribers in one or more group enciphering keys.

5 Claims, 3 Drawing Figures



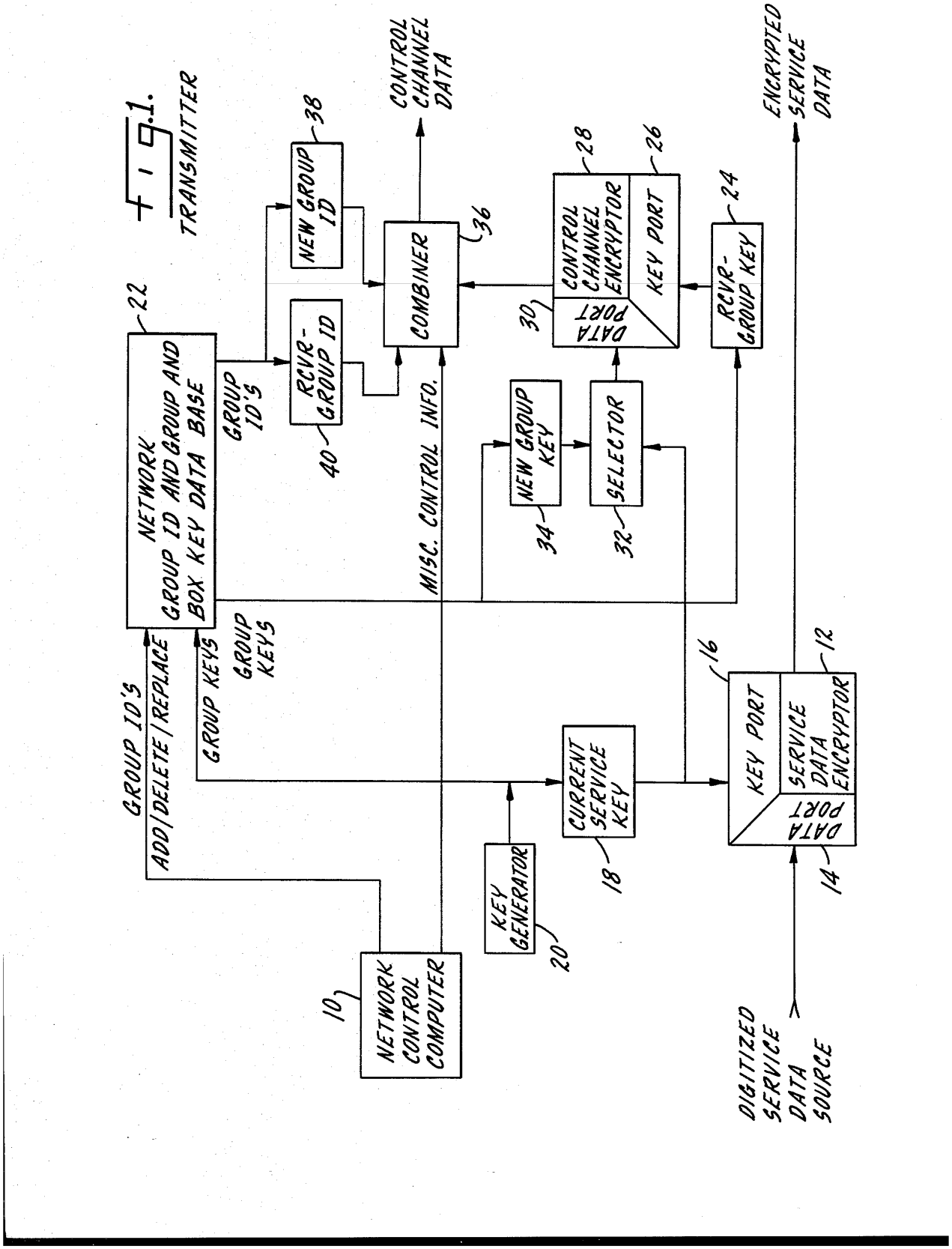


FIG. 1.

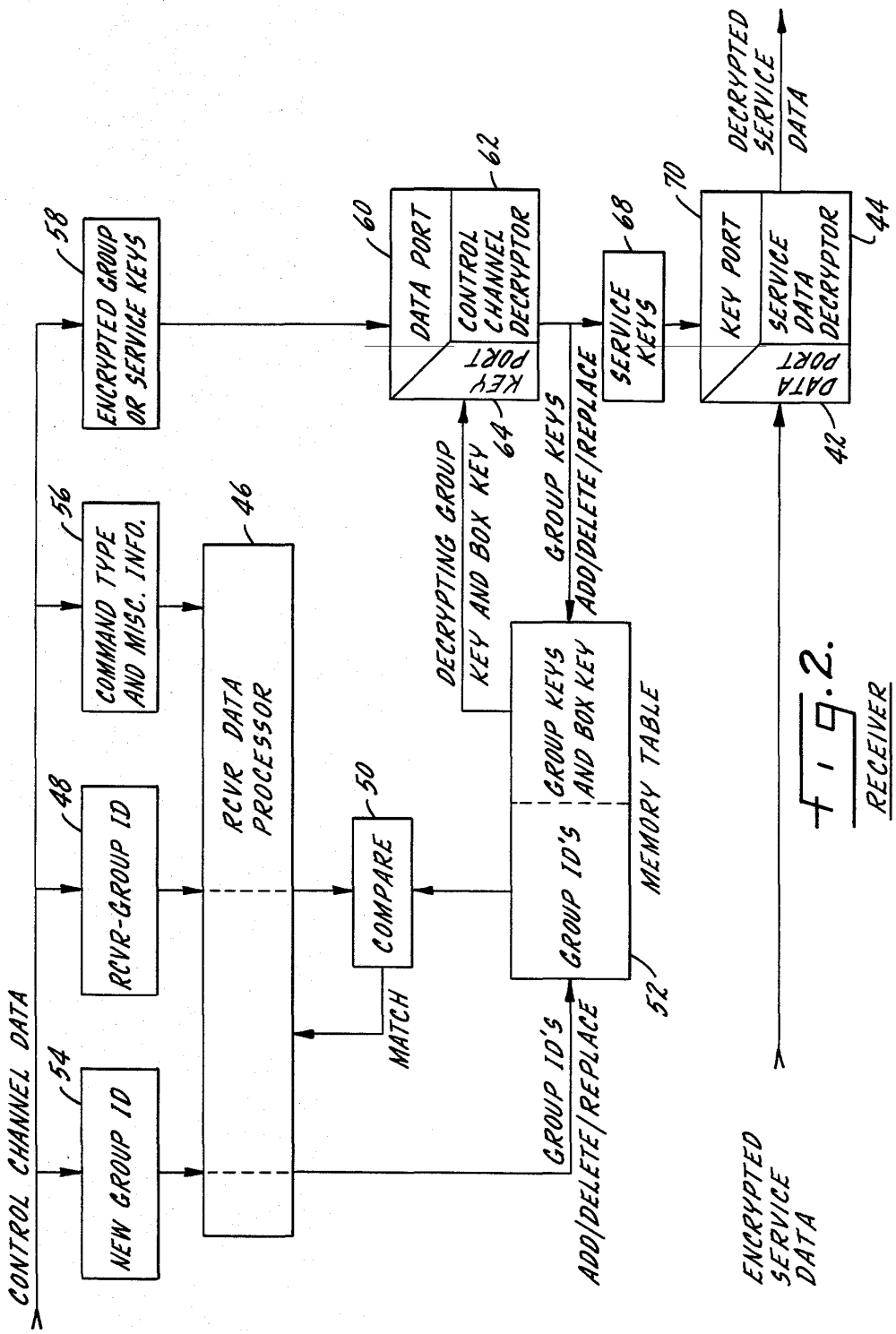


Fig. 2.

COMMAND TYPE	RCVR-GROUP ID	NEW GROUP KEY	NEW GROUP ID	MISC. INFO.

COMMAND TYPE	RCVR-GROUP ID	NEW SERVICE KEY	MISC. INFO.

Fig. 3.

TYPICAL MESSAGE STRUCTURE

MULTI-LAYER ENCRYPTION SYSTEM FOR THE BROADCAST OF ENCRYPTED INFORMATION

SUMMARY OF THE INVENTION

The present invention relates to a system for enciphering and deciphering digital information signals and has application in the field of broadcast television, although the principles disclosed herein should not be so limited. Specifically, audio information and/or text information for display on a video screen may be placed in digital form and enciphered. Such signals may be part of a cable television system (CATV), a subscription television system (STV) or a direct broadcast satellite television system (DBS).

A primary purpose of the invention is a system for enciphering digital information signals in the environment described in which there are multiple layers of enciphering keys to insure security of the broadcast information.

Another purpose is an enciphering and deciphering system of the type described in which communication between the broadcast station and a plurality of subscribers may take place in a box key peculiar to an individual subscriber, a group key peculiar to a group of subscribers having a common interest, or in a service key which is common for a specific broadcast and which may be changed from time to time through either the group or box keys.

Another purpose is a simply reliable and completely secure enciphering and deciphering system for use in the broadcast of digital information signals.

Another purpose is a method for controlling the broadcast of digital information signals in which there are layers or levels or tiers of keys to insure system security and in which the keys may be changed by communication to subscribers in one or more of the layers of keys.

Other purposes will appear in the ensuing specification, drawings and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is illustrated diagrammatically in the following drawings wherein:

FIG. **1** is a block diagram of a transmitter for use in the control system described herein,

FIG. **2** is a block diagram of the receiver, and

FIG. **3** is a diagrammatic illustration of typical message structures used in the system disclosed herein.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention has utility in CATV, STV and DBS television systems in which the video signal is coded. The specific enciphering and deciphering system disclosed herein is primarily applicable to the audio portion of the video signal as the audio signal is readily susceptible of being placed in a digital format. It is also applicable to those video signals in which alphanumeric text information is transmitted, such as the VIDEOTEXT system now in commercial use by Oak Industries Inc., assignee of the present application or other types of digital or digitized data such as computer software, games, radio programs, computer data bases, etc. which may be delivered via such communication system. Signals of that type are also readily susceptible to being placed in digital form and hence can be enciphered and deciphered by the control system described herein.

It is important in broadcast systems of the type referred to above to insure secrecy or privacy of the communications, as customarily such broadcasts are on a subscription basis and it is mandatory that privacy be retained or the concept of a subscription broadcast system is destroyed. To that end various schemes have been proposed to insure the security of those portions of the signals which can be placed in digital form. The present invention provides a first level of security by enciphering the digital information signals in what is termed a service key, which key is provided to all subscribers who are to receive a specific broadcast or a specific type of broadcast. For example, the service key may be peculiar to a specific program, but more commonly it will be used for a specific channel when the system is used in a television environment. To insure privacy and security the service key must be periodically changed. To change the service key it is necessary to communicate with each of the subscribers and this communication takes place in what is called the group key which is common to a group of subscribers, all of whom are to receive a specific type of broadcast. There may be a substantial number of groups associated with a specific communication system and an individual subscriber may itself belong to more than one or a plurality of groups. Specifically, to change the service key for a particular type of broadcast, the broadcaster will communicate to all of the subscribers in the group key and the group key is used to change the service key. As an alternative, a large number of service keys may be stored in each decoder and the broadcast station selects a specific service key by communicating with the subscriber in the group key.

From time to time subscribers' tastes and desires in programming change and thus it is necessary to change groups, to reform groups and to add or delete subscribers from a particular group. Again, this may be accomplished by communicating to the subscribers in the group key. The group key itself may be changed and subscribers may be added or deleted from the group, or in fact new groups may be formed by communicating to the subscribers in the group key.

In addition to communicating in the group key, it is necessary to have addresses which are peculiar to an individual subscriber and peculiar to a group. For example, each subscriber may have its own individual address which is peculiar to that subscriber. That address will be stored in the subscriber's decoder. In addition, the subscriber may belong to one or more groups, each of which will have a specific address for that group with these addresses being temporarily stored in the subscribers decoder. Thus, the broadcaster may communicate to the subscriber by providing the subscriber's group address or the subscriber's individual address and by communicating to the subscriber in the group key peculiar to the group with which the broadcaster is specifically concerned at that moment.

As a final means for insuring security and privacy, each subscriber will have what is known as a box key and that is a key peculiar to a specific subscriber. If the broadcaster wishes to communicate in complete privacy with an individual subscriber, it may do so in the subscriber's box key. For example, if the broadcaster feels that one or more groups of keys have been compromised and the only way to reform groups is to communicate to each individual subscriber in its box key,

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.