United States Patent [19]

Gilhousen et al.

[11] **Patent Number: 4,613,901**

[45] **Date of Patent: Sep. 23, 1986**

[54] **SIGNAL ENCRYPTION AND DISTRIBUTION SYSTEM FOR CONTROLLING SCRAMBLING AND SELECTIVE REMOTE DESCRAMBLING OF TELEVISION SIGNALS**

[75] Inventors: **Klein S. Gilhousen**, San Diego; **Charles F. Newby, Jr.**, El Cajon; **Karl E. Moerder**, Poway, all of Calif.

[73] Assignee: **M/A-COM Linkabit, Inc.**, San Diego, Calif.

[21] Appl. No.: **498,800**

[22] Filed: **May 27, 1983**

[51] **Int. Cl.**[4] **H04N 7/167**; H04L 9/00

[52] **U.S. Cl.** **358/122**; 178/22.07; 178/22.1; 178/22.16

[58] **Field of Search** 358/122; 178/22.07, 178/22.1, 22.14, 22.16

[56] **References Cited**

U.S. PATENT DOCUMENTS

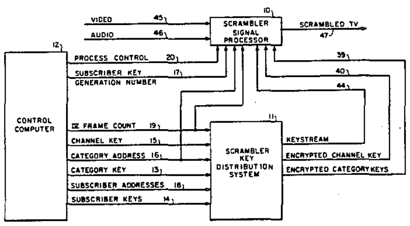
3,238,297	3/1966	Pawley et al.	178/22
3,668,307	6/1972	Face et al.	178/5.6
3,729,581	4/1973	Anderson	178/6.8
3,777,053	12/1973	Wittig et al.	178/5.1
3,798,359	3/1974	Feistel	178/22
3,803,491	4/1974	Osborn	325/53
3,886,302	5/1975	Kosco	178/5.1
3,894,176	7/1975	Mellon	178/5.1
3,899,633	8/1975	Sorenson et al.	178/5.1
3,916,091	10/1975	Kirk, Jr. et al.	178/5.1
3,919,462	11/1975	Hartung et al.	178/5.1
3,936,593	2/1976	Aaronson et al.	178/5.1
3,997,718	12/1976	Ricketts et al.	178/6.8
4,024,574	5/1977	Nieson	358/117
4,025,948	5/1977	Loshin	358/122
4,058,830	11/1977	Guinet et al.	358/86
4,068,264	1/1978	Pires	358/122
4,091,417	5/1978	Nieson	357/117
4,112,464	9/1978	Guif et al.	358/122
4,115,662	9/1978	Guinet et al.	179/15 BV
4,115,807	9/1978	Pires	358/122
4,160,120	7/1979	Barnes et al.	178/22
4,161,751	7/1979	Ost	358/114
4,163,254	7/1979	Block et al.	358/122
4,163,255	7/1979	Pires	358/122
4,172,213	10/1979	Barnes et al.	178/22
4,215,366	7/1980	Davidson	358/124
4,225,884	9/1980	Block et al.	358/122
4,250,524	2/1981	Tomizawa	358/122
4,253,114	2/1981	Tang et al.	358/114
4,292,650	9/1981	Hendrickson	358/123
4,302,771	11/1981	Gargini	358/86
4,304,990	12/1981	Atalla	235/379
4,316,055	2/1982	Feistal	178/22.06
4,322,745	3/1982	Saeki et al.	358/123
4,323,921	4/1982	Guillou	358/114
4,323,922	4/1982	den Toonder et al.	358/117
4,331,973	5/1982	Eskin et al.	358/84
4,331,974	5/1982	Cogswell et al.	358/86
4,336,553	6/1982	den Toonder et al.	358/120
4,338,628	7/1982	Payne et al.	358/120
4,354,201	10/1982	Sechet et al.	358/122
4,388,643	6/1983	Aminetzah	358/122
4,458,109	7/1984	Mueller-Schloer	178/22.16
4,461,032	7/1984	Skerlos	455/4
4,467,139	8/1984	Mollier	178/22.08
4,471,164	9/1984	Henry	178/22.11
4,484,027	11/1984	Lee et al.	358/122
4,531,011	7/1985	Bluestein et al.	178/22.08
4,531,020	7/1985	Wechselberger et al.	178/22.08
4,533,948	8/1985	McNamara et al.	358/122
4,533,949	8/1985	Fujimura et al.	358/122
4,535,355	8/1985	Arn et al.	358/122

Primary Examiner—Stephen C. Buczinski
Assistant Examiner—Linda J. Wallace
Attorney, Agent, or Firm—Edward W. Callan

[57] **ABSTRACT**

A system and method for scrambling and selectively descrambling television signals that are transmitted to subscribers' descramblers in a subscription television system. A working key signal is generated by processing an "initialization vector" signal in accordance with the DES algorithm upon the algorithm being keyed by either a common category key signal or some other key signal. A unique encryption keystream is generated by processing the initialization vector signal in accordance with the DES algorithm upon the algorithm being keyed by the working key signal. A television signal is scrambled in accordance with the unique encryption keystream to provide a scrambled television signal. A plurality of unique encrypted category key signals individually addressed to different selected subscribers' descramblers are generated by processing the initial common category key signal in accordance with the DES algorithm upon the algorithm being keyed by a plurality of different "unit key" signals unique to different selected descramblers. The scrambled television signal, the initialization vector signal, and the plurality of encrypted category key signals are broadcast to the descramblers. A corresponding tier of DES algorithms are employed at the descrambler to reproduce the encryption keystream; and the TV signal is descrambled in accordance therewith. Each descrambler has its unique unit key signal stored in a secure memory for use in reproducing the common category key signal when the descrambler is addressed by its unique encrypted category key signal.

26 Claims, 8 Drawing Figures



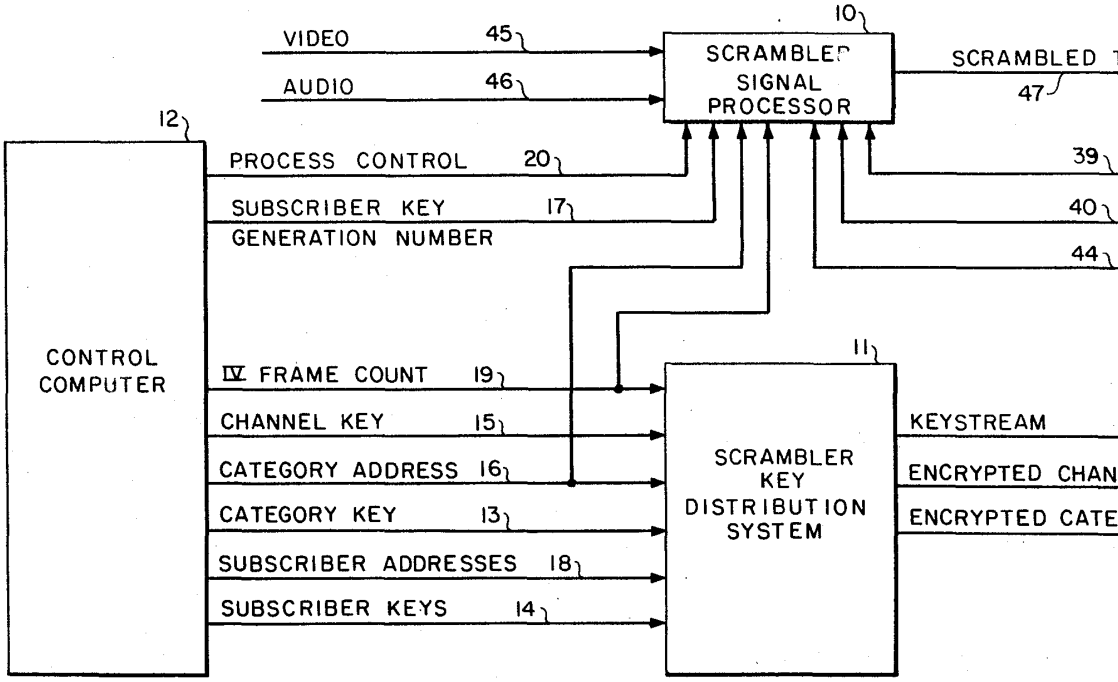

VIDEO
45
AUDIO
46
10
SCRAMBLER SIGNAL PROCESSOR
SCRAMBLED T
47
12
CONTROL COMPUTER
PROCESS CONTROL
20
SUBSCRIBER KEY GENERATION NUMBER
17
39
40
44
TV FRAME COUNT
19
CHANNEL KEY
15
CATEGORY ADDRESS
16
CATEGORY KEY
13
SUBSCRIBER ADDRESSES
18
SUBSCRIBER KEYS
14
11
SCRAMBLER KEY DISTRIBUTION SYSTEM
KEYSTREAM
ENCRYPTED CHAN
ENCRYPTED CATE

FIG. 1

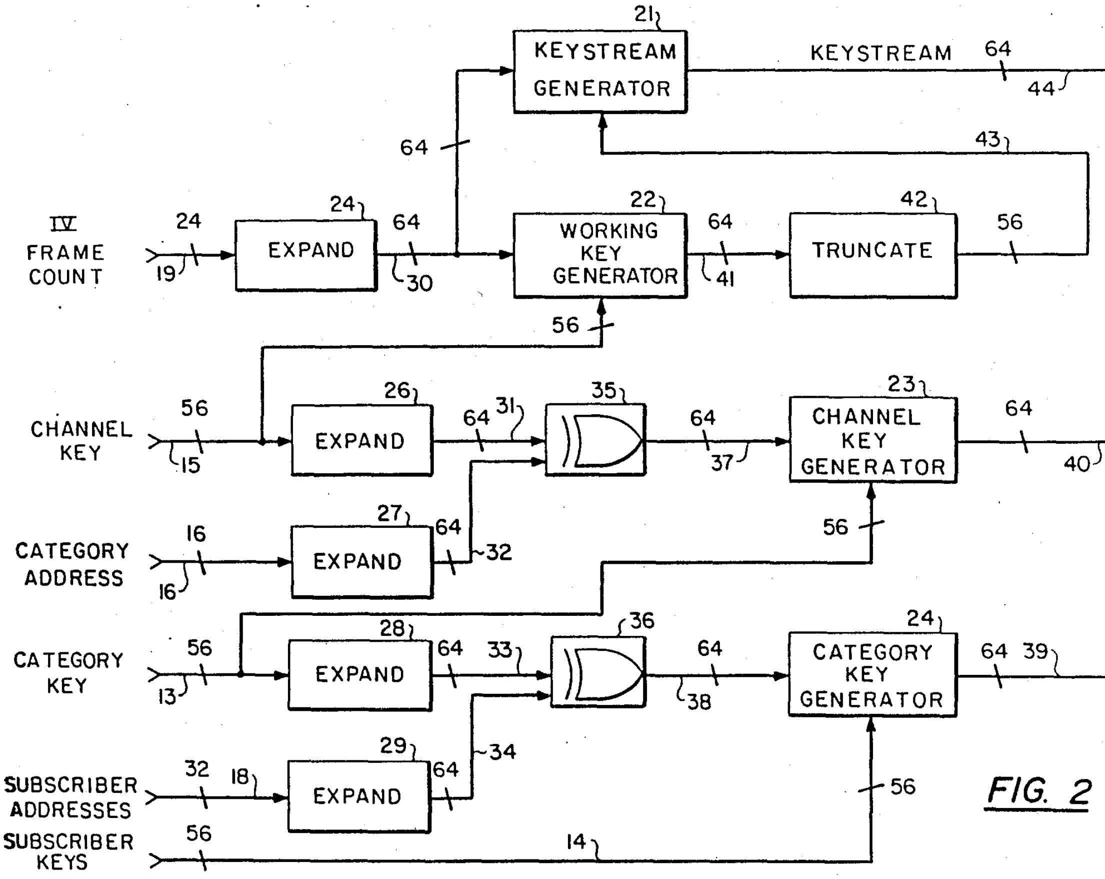
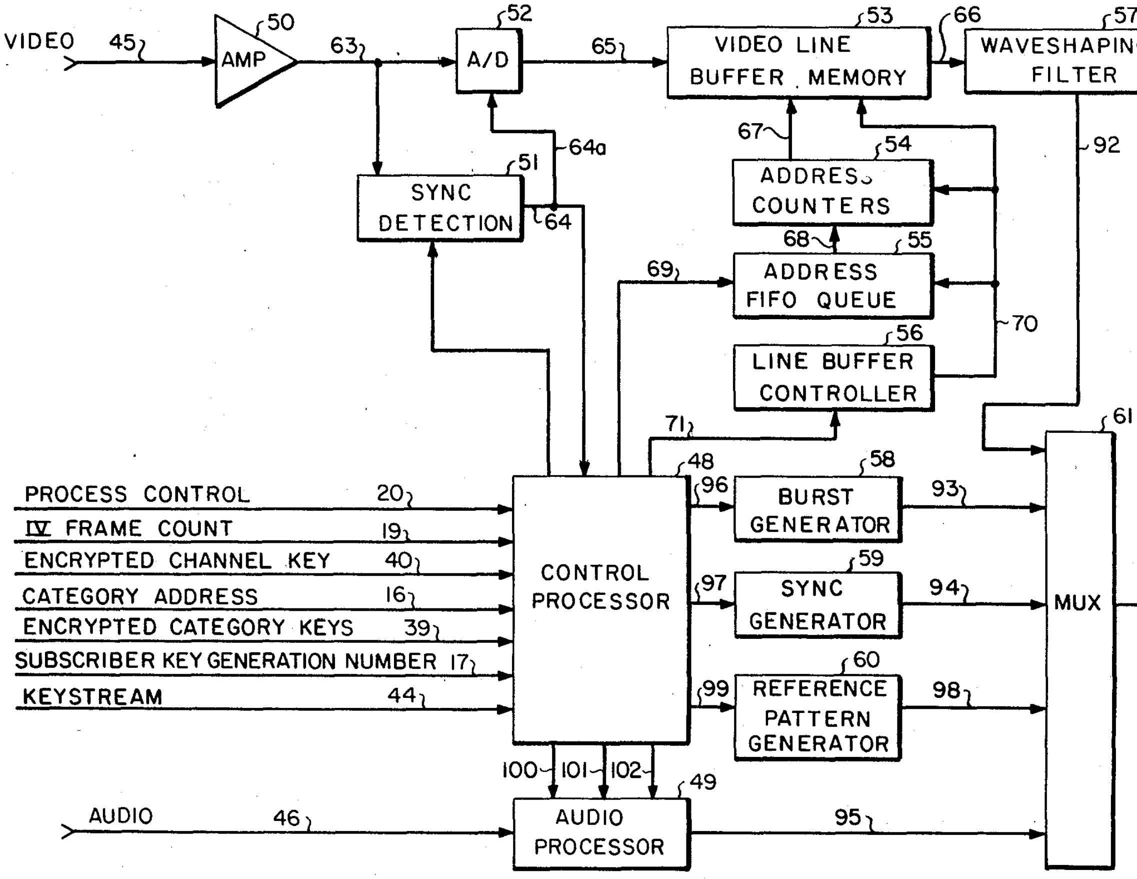

21
KEYSTREAM GENERATOR
KEYSTREAM
64
44
64
43
IV
FRAME COUNT
24
19
24
EXPAND
64
30
22
WORKING KEY GENERATOR
64
41
42
TRUNCATE
56
56
CHANNEL KEY
56
15
26
EXPAND
64
31
35
64
37
23
CHANNEL KEY GENERATOR
64
40
CATEGORY ADDRESS
16
16
27
EXPAND
64
32
56
CATEGORY KEY
56
13
28
EXPAND
64
33
36
64
38
24
CATEGORY KEY GENERATOR
64
39
SUBSCRIBER ADDRESSES
32
18
29
EXPAND
64
34
56
SUBSCRIBER KEYS
56
14

FIG. 2


VIDEO
45
AMP
50
63
A/D
52
65
VIDEO LINE BUFFER MEMORY
53
66
WAVESHAPIN
FILTER
57
92
67
64a
SYNC DETECTION
51
64
ADDRESS COUNTERS
54
68
ADDRESS FIFO QUEUE
55
69
70
LINE BUFFER CONTROLLER
56
71
61
PROCESS CONTROL
20
TV FRAME COUNT
19
ENCRYPTED CHANNEL KEY
40
CATEGORY ADDRESS
16
ENCRYPTED CATEGORY KEYS
39
SUBSCRIBER KEY GENERATION NUMBER
17
KEYSTREAM
44
CONTROL PROCESSOR
48
96
BURST GENERATOR
58
93
97
SYNC GENERATOR
59
94
MUX
99
REFERENCE PATTERN GENERATOR
60
98
100
101
102
49
AUDIO
46
AUDIO PROCESSOR
95

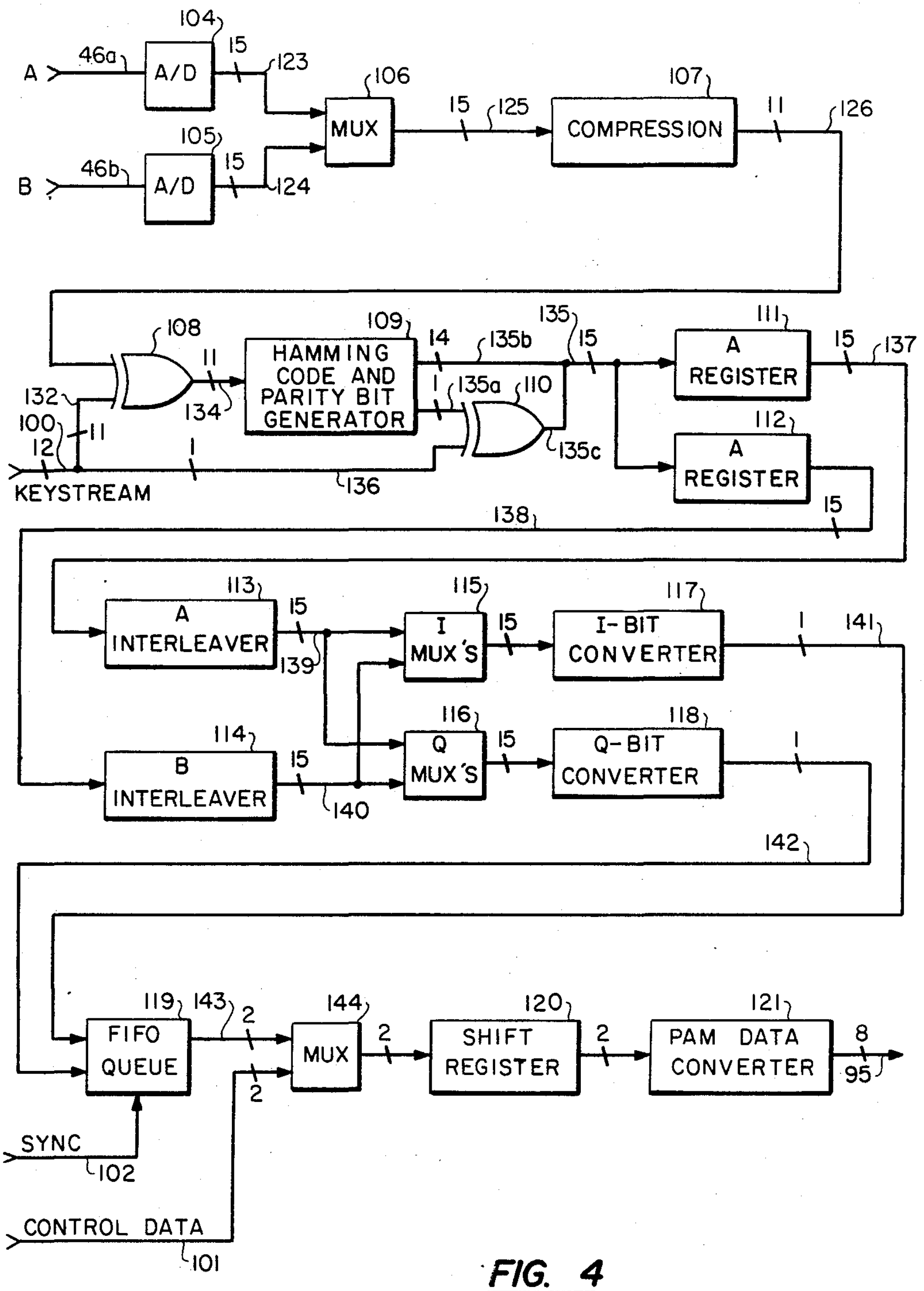

A
46a
A/D
104
15
123
B
46b
A/D
105
15
124
MUX
106
15
125
COMPRESSION
107
11
126
108
11
134
HAMMING CODE AND PARITY BIT GENERATOR
109
14
135b
135
15
A REGISTER
111
15
137
132
100
12
11
1
135a
110
135c
KEYSTREAM
136
A REGISTER
112
15
138
A INTERLEAVER
113
15
139
I MUX'S
115
15
I-BIT CONVERTER
117
1
141
B INTERLEAVER
114
15
140
Q MUX'S
116
15
Q-BIT CONVERTER
118
1
142
FIFO QUEUE
119
143
2
MUX
144
2
SHIFT REGISTER
120
2
PAM DATA CONVERTER
121
8
95
SYNC
102
CONTROL DATA
101

FIG. 4

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.