(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3789469号
(P3789469)
(45)発行日　平成18年6月21日(2006.6.21)　(24)登録日　平成18年4月7日(2006.4.7)

(51)Int.Cl.			F I		
H04L	9/20	(2006.01)	H04L	9/00	653
G09C	1/00	(2006.01)	G09C	1/00	
H04H	1/00	(2006.01)	H04H	1/00	F
H04N	7/167	(2006.01)	H04N	7/167	

請求項の数 45　(全 21 頁)

(21)出願番号　特願平6-513480
(86)(22)出願日　平成5年12月1日(1993.12.1)
(65)公表番号　特表平8-504308
(43)公表日　平成8年5月7日(1996.5.7)
(86)国際出願番号　PCT/US1993/011654
(87)国際公開番号　WO1994/013081
(87)国際公開日　平成6年6月9日(1994.6.9)
審査請求日　平成12年11月28日(2000.11.28)
審判番号　不服2004-14547(P2004-14547/J1)
審判請求日　平成16年7月12日(2004.7.12)
(31)優先権主張番号　984,461
(32)優先日　平成4年12月2日(1992.12.2)
(33)優先権主張国　米国(US)

(73)特許権者
サイエンテイフイク－アトランタ・インコーポレーテツド
アメリカ合衆国ジヨージア州３００９２ノークロス・ワンテクノロジーパークウエイ－サウス（番地なし）
(74)代理人
弁理士　山本　秀策
(72)発明者　ウオシリユウスキ，アンソニー・ジエイ
アメリカ合衆国ジヨージア州３０２０２アルフアレツタ・レンリツジロード１０６８０

最終頁に続く

(54)【発明の名称】データを一意的に端局暗号化するための方法及び装置

(57)【特許請求の範囲】
【請求項１】
複数Ｎの送信装置の各々から少なくとも一つの受信装置へデータのセットを伝送するための方法であって、
各送信装置は、その送信装置に一意的な同報通信キーと、すべての送信装置に対して同一のシステムキーへのアクセスとを有し、該システムキーが複数Ｓのビットを含み、該同報通信キーの各々が一意的な複数Ｂのビットを含み、ＢがＳよりも小さく、該方法は、
（ａ）該複数Ｎの送信装置の各々が、該システムキーおよびその送信装置に一意的な該同報通信キーを所定の方法で畳み込み、その送信装置に対して一意的なデータ暗号化キーを生成するステップであって、該一意的な暗号化キーは第３数Ｅのビットを含み、ＥはＢよりも少なくとも大きいステップと、
（ｂ）該複数Ｎの送信装置の各々が、その送信装置において生成された該一意的なデータ暗号化キーでデータのセットを暗号化するステップと、
（ｃ）該複数Ｎの送信装置の各々が、暗号化された該データのセットを該受信装置に伝送するステップと、
を含み、
該受信装置は、該システムキーおよび該同報通信キーの各々をメモリ内に記憶し、各送信装置のそれぞれにおいて該データセットを暗号化するために使用された一意的なデータ暗号化キーを、該暗号化データセットの任意の一つを解読する目的のために再生し、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリ容量が

、（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、
方法。
【請求項２】
前記受信装置は、以下のステップ、
（ｄ）前記送信装置の選択された一つから伝送された該暗号化データセットを受信するステップと、
（ｅ）前記システムキーおよび該選択された送信装置に一意的な前記同報通信キーを、該受信装置における前記メモリから検索するステップと、
（ｆ）該検索されたシステムキーおよび検索された同報通信キーを前記所定の方法で畳み込み、該受信されたデータのセットを暗号化するためにステップ（ｂ）において用いられた前記一意的なデータ暗号化キーを再現するステップと、
（ｇ）該受信されたデータのセットを該再現された暗号キーで解読するステップと、
を実行する、請求項１に記載の方法。
【請求項３】
前記受信装置は、選択されたグループの送信装置のみからデータを受信し、該受信装置は、前記システムキーおよび送信装置の該選択されたグループの前記同報通信キーのみを、前記メモリ内に記憶する、請求項１に記載の方法。
【請求項４】
ＥがＳ以上である、請求項１に記載の方法。
【請求項５】
各送信装置に設けられた前記システムキーは、周期的に変更され、前期受信装置において前記メモリに記憶される、請求項１に記載の方法。
【請求項６】
各送信装置に設けられた前記一意的な同報通信キーは、周期的に変更され、前記受信装置において前記メモリに記憶される、請求項１に記載の方法。
【請求項７】
前記送信装置は、加入テレビジョンシステムにおけるプログラマー装置を含み、各プログラマー装置は、局所的に生成されたプログラムキーで該プログラムデータを暗号化し、かつ、該プログラムデータを伝送し、ステップ（ｂ）において前記複数Ｎの送信装置によって暗号化された前記データのセットが、該プログラムキーを含む、請求項１に記載の方法。
【請求項８】
前記受信装置が、ケーブルヘッドエンド設備および加入テレビジョンシステム加入者位置の一方である、請求項７に記載の方法。
【請求項９】
複数Ｎの送信装置および少なくとも一つの受信装置を含むデータ伝送システムであって、各送信装置は、すべての送信装置に共通のシステムキーへのアクセスを有し、各送信装置は、その送信装置に一意的な同報通信キーを有し、該システムキーが第１数Ｓのビットを含み、該同報通報キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さい、データ伝送システムにおいて、送信装置からデータのセットを伝送するための方法であって、
（ａ）該送信装置が、該システムキーおよびその装置に一意的な該同報通信キーを畳み込み、その送信装置に対して一意的なデータ暗号化キーを生成するステップであって、該一意的なデータ暗号化キーが第３数Ｅのビットを含み、ＥがＢよりも少なくとも大きい、ステップと、
（ｂ）該送信装置が、その送信装置において生成された該一意的なデータ暗号化キーでデータのセットを暗号化するステップと、
（ｃ）該送信装置が、暗号化された該データのセットを該受信装置に伝送するステップと、
を含み、
該受信装置は、該システムキーおよび該同報通信キーの各々をメモリ内に記憶し、各送信

装置のそれぞれにおいて該データセットを暗号化するために使用された一意的なデータ暗号化キーを、該暗号化データセットを解読する目的のために再生し、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリ容量が、（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、
方法。
【請求項１０】
前記受信装置が、選択されたグループの送信装置のみからデータを受信し、該受信装置は、前記システムキーおよび送信装置の該選択されたグループの前記同報通信キーのみを、前記メモリ内に記憶する、請求項９に記載の方法。
【請求項１１】
ＥがＳ以上である、請求項９に記載の方法。
【請求項１２】
前記送信装置に設けられ、前記受信装置においてメモリに記憶されたシステムキーが周期的に変更される、請求項９に記載の方法。
【請求項１３】
前記送信装置に設けられ、前記受信装置においてメモリに記憶された一意的な同報通信キーが周期的に変更される、請求項９に記載の方法。
【請求項１４】
前記送信装置は、加入テレビジョンシステムにおけるプログラマー装置を含み、該プログラマー装置は、局所的に生成されたプログラムキーでプログラムデータを暗号化し、かつ、該プログラムデータを伝送し、ステップ（ｂ）における該送信装置によって暗号化された前記データセットが、該局所的に生成されたプログラムキーを含む、請求項９に記載の方法。
【請求項１５】
前記受信装置が、ケーブルヘッドエンド設備および加入テレビジョンシステム加入者位置の一方である請求項９に記載の方法。
【請求項１６】
複数Ｎの送信装置および少なくとも一つの受信装置を含むデータ伝送システムであって、各送信装置がその送信装置に一意的な同報通信キーを有し、各送信装置は、すべての送信装置に対して同一のシステムキーへのアクセスを有し、該システムキーが第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さく、各送信装置は、該システムキーおよびその送信装置に一意的な該同報通信キーを所定の方法において畳み込んで一意的なデータ暗号化キーを生成し、各送信装置において生成された該一意的なデータ暗号化キーが、次にその送信装置によって使用されて、該受信装置への伝送のためにデータのセットを暗号化し、さらに、該受信装置は、メモリ内に該システムキーおよび該同報通信キーの各々を記憶する、データ伝送システムにおいて、該送信装置の選択された一つから伝送された暗号化データセットを該受信装置において受信する方法であって、
（ａ）該受信装置が、該送信装置の選択された一つから伝送された該暗号化データセットを受信するステップと、
（ｂ）該受信装置が、該システムキーおよび該選択された送信装置に一意的な該同報通信キーを該メモリから検索するステップと、
（ｃ）該受信装置が、該所定の方法において、該検索されたシステムキーおよび検索された同報通信キーを畳み込み、該選択された送信装置において生成された該一意的なデータ暗号化キーを再現するステップと、
（ｄ）該受信装置が、該再現された暗号化キーで該暗号化データセットを解読するステップであって、これにより、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリ容量は、（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、ステップと、
を含む

方法。
【請求項１７】
前記受信装置が、選択されたグループの送信装置のみからデータを受信し、前記受信装置は、前記システムキーおよび送信装置の該選択されたグループの前記同報通信キーのみを、前記メモリ内に記憶する、請求項１６に記載の方法。
【請求項１８】
各送信装置において生成された前記一意的なデータ暗号化キーが第３数Ｅのビットを含み、ＥはＳ以上である、請求項１６に記載の方法。
【請求項１９】
前記送信装置に設けられ、前記受信装置において前記メモリに記憶された前記システムキーが周期的に変更される、請求項１６に記載の方法。
【請求項２０】
各送信装置に設けられ、前記受信装置において前記メモリに記憶された前記一意的な同報通信キーが周期的に変更される、請求項１６に記載の方法。
【請求項２１】
少なくとも一つの受信装置への伝送のために送信装置において複数Ｎのデータセットを伝送するための方法であって、該方法が、
（ａ）該送信装置が、各データセットに対して、そのデータセットに一意的な同報通信キーと各データセットに対して同一であるシステムキーとを設けるステップであって、該システムキーが第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢはＳよりも小さい、ステップと、
（ｂ）該送信装置が、各データセットに対して、該システムキーおよびそのデータセットに一意的な該同報通信キーを所定の方法で畳み込み、そのデータセットに一意的なデータ暗号化キーを生成するステップであって、該一意的なデータ暗号化キーが第３数Ｅのビットを含み、ＥはＢよりも少なくとも大きい、ステップと、
（ｃ）該送信装置が、そのデータセットに対して生成された該一意的なデータ暗号化キーで各データセットを暗号化するステップと、
（ｄ）該送信装置が、暗号化データセットを該受信装置に伝送するステップと、を含み、該受信装置は、該システムキーおよび該同報通信キーの各々をメモリ内に記憶し、送信装置において該データセットの各々を暗号化するために使用された一意的なデータ暗号化キーを、該暗号化データセットを解読する目的のために再生し、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリ容量が、（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、
方法。
【請求項２２】
前記受信装置が、データセットの選択されたグループのみを受信し、該受信装置は、前記システムキーおよび送信装置の該選択されたグループの同報通信キーのみを、メモリ内に記憶する、請求項２１に記載の方法。
【請求項２３】
ＥがＳ以上である、請求項２１に記載の方法。
【請求項２４】
前記システムキーが周期的に変更される、請求項２１に記載の方法。
【請求項２５】
各データセットに対して設けられ、前記受信装置において記憶された前記一意的な同報通信キーが周期的に変更される、請求項２１に記載の方法。
【請求項２６】
（ａ）各データセットに対して、そのデータセットに一意的である同報通信キーと、各データセットに対して同一であるシステムキーとを設け、該システムキーが第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さいことと、（ｂ）各データセットに対して、該システムキーおよびそのデータセットに一意的な該

同報通信キーを所定の方法で畳み込み、そのデータセットに一意的なデータ暗号化キーを生成することと、（ｃ）各データセットを、そのデータセットに対して生成された該一意的なデータ暗号化キーで暗号化することとにより、該送信装置が、複数Ｎのデータセットの各々を暗号化するデータ伝送システムであって、該送信装置は、該暗号化データセットの各々を少なくとも一つの受信装置に伝送し、さらに、該送信装置は、該システムキーおよび該同報通信キーの各々を、メモリ内に記憶する、データ伝送システムにおいて、該暗号化データセットを該受信装置において受信するための方法であって、
（ａ）該受信装置が、該選択された暗号化データセットを受信するステップと、
（ｂ）該受信装置が、該システムキーおよび該選択されたデータセットに一意的な同報通信キーを該メモリから検索するステップと、
（ｃ）該受信装置が、該所定の方法において該検索されたシステムキーおよび検索された同報通信キーを畳み込み、該送信装置において生成された該一意的なデータ暗号化キーを再現するステップと、
（ｄ）該受信装置が、該再現された暗号化キーで該暗号化データセットを解読するステップであって、これにより、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリ容量が（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、ステップと、
を含む方法。
【請求項２７】
前記受信装置が、データセットの選択されたグループのみを受信し、該受信装置が、前記システムキーおよび該選択されたグループの同報通信キーのみを、前記メモリ内に記憶する、請求項２６に記載の方法。
【請求項２８】
各データセットに対して生成された前記一意的なデータ暗号化キーが第３数Ｅのビットを含み、ＥがＳ以上である、請求項２６に記載の方法。
【請求項２９】
前記システムキーが周期的に変更される、請求項２６に記載の方法。
【請求項３０】
各データセットに対して設けられ、前記受信装置において記憶された前記一意的な同報通信キーが周期的に変更される、請求項２６に記載の方法。
【請求項３１】
複数Ｎのプログラマー装置が各々少なくとも一つの受信装置にプログラムデータを伝送し、各プログラマー装置が、局所的に生成されたプログラムキーで、そのプログラマー装置から伝送されたプログラムデータを暗号化し、該プログラムキーは、該暗号化プログラムデータとともに各プログラマーによって該受信装置に伝送され、各プログラマー装置は、各プログラマー装置に一意的な同報通信キーを有し、各プログラマー装置は、すべてのプログラマー装置に対して同一であるシステムキーへのアクセスを有し、該システムキーが第１数Ｓのビットを含み、そして、該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さく、
各プログラマー装置は、該システムキーへのアクセスを有し、各プログラマー装置は、そのプログラマー装置に一意的な該同報通信キーを有する、ペイテレビジョンシステムにおいて、プログラマー装置から該プログラムキーを伝送するための方法であって、
（ａ）該プログラマー装置が、該システムキーおよびそのプログラマー装置に対する同報通信キーを所定の方法で畳み込み、そのプログラマー装置に対して一意的な暗号化キーを生成するステップであって、該一意的な暗号化キーが第３数Ｅのビットを含み、ＥがＢよりも少なくとも大きい、ステップと、
（ｂ）該プログラマー装置が、そのプログラマー装置において生成された該一意的な暗号化キーで該プログラムキーを暗号化するステップと、
（ｃ）該プログラマー装置が、該受信装置に該暗号化プログラムキーを伝送するステップであって、該受信装置は、該システムキーおよび該同報通信キーの各々を、メモリ内に記

憶し、該プログラマー装置の各々において該プログラムキーを暗号化するのに用いられた該一意的なデータ暗号化キーを、該暗号化プログラムキーを解読する目的のために再生する、ステップと、
を含み、
該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリ容量が、（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、
方法。
【請求項３２】
前記受信装置が、プログラマー装置の選択されたグループのみからプログラムデータおよびそれぞれのプログラムキーを受信し、該受信装置は、前記システムキーおよびプログラマー装置の該選択されたグループの該同報通信キーのみを、該メモリ内に記憶する、請求項３１に記載の方法。
【請求項３３】
ＥがＳ以上である、請求項３１に記載の方法。
【請求項３４】
前記プログラマー装置において設けられ、前記受信装置における前記メモリに記憶された前記システムキーが周期的に変更される、請求項３１に記載の方法。
【請求項３５】
前記プログラマー装置において設けられ、前記受信装置における前記メモリに記憶された前記一意的な同報通信キーが周期的に変更される、請求項３１に記載の方法。
【請求項３６】
複数Ｎのプログラマー装置が各々少なくとも一つの受信装置にプログラムデータを伝送し、各プログラマー装置が、局所的に生成されたプログラムキーで、そのプログラマー装置から伝送されたプログラムデータを暗号化し、各プログラマー装置は、そのプログラマー装置に一意的な同報通信キーを有し、各プログラマー装置は、すべてのプログラマー装置に対して同一であるシステムキーへのアクセスを有し、該システムキーが第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さく、そして、（ａ）該プログラマー装置において、該システムキーおよびそのプログラマー装置に一意的な該同報通信キーを設けることと、（ｂ）該システムキーおよびそのプログラマー装置に対する該同報通信キーを所定の方法で畳み込み、そのプログラマー装置に対して一意的な暗号化キーを生成することと、（ｃ）そのプログラマー装置において生成された該一意的な暗号化キーで該プログラムキーを暗号化することとにより、各プログラマー装置は、そのプログラマー装置で局所的に生成された該プログラムキーを暗号化し、各プログラマー装置は、それぞれの暗号化プログラムキーおよび暗号化プログラムデータを該受信装置に伝送し、さらに、該受信装置は、該システムキーおよび該同報通信キーの各々を、メモリ内に記憶する、ペイテレビジョンシステムにおいて、該プログラマー装置の選択された一つから伝送された該プログラムキーおよびプログラムデータを、該受信装置において受信する方法であって、
（ａ）該受信装置が、該選択されたプログラマー装置から伝送された該暗号化プログラムデータおよび該暗号化プログラムキーを受信するステップと、
（ｂ）該受信装置が、該システムキーおよび該選択されたプログラマー装置に一意的な同報通信キーを該メモリから検索するステップと、
（ｃ）該受信装置が、該所定の方法において該検索されたシステムキーおよび検索された同報通信キーを畳み込み、該選択されたプログラマー装置において生成された該一意的な暗号化キーを再現するステップと、
（ｄ）該受信装置が、該再現された暗号化キーで該暗号化プログラムキーを解読するステップと、
（ｅ）該受信装置が、該解読プログラムキーで該暗号化プログラムデータを解読するステップと、を含み、これにより、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリの記憶容量が（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、

方法。
【請求項３７】
各々がデータのセットを少なくとも一つの受信装置に伝送する複数Ｎの送信装置を含むデータ伝送システムであって、すべての送信装置に共通のシステムキーおよび各々の送信装置に一意的な同報通信キーが存在し、該システムキーが第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳより小さく、該送信装置の各々は、
該システムキーおよびそのプログラマー装置に対する該同報通信キーを所定の方法で畳み込み、その送信装置に対して一意的な暗号化キーを生成する手段と、
該一意的なデータ暗号化キーでデータのセットを暗号化するための暗号器と、
該暗号化されたデータのセットを受信装置に伝送する手段と、
を含む暗号化装置を有し、該受信装置が、
該システムキーおよび該同報通信キーの各々を記憶するためのメモリであって、該メモリの記憶容量が（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、メモリと、
該送信装置の選択された一つから伝送された暗号化データセットを受信するための手段と、
該メモリに結合され、該メモリから該システムキーおよび該選択された送信装置に一意的な該同報通信キーを検索し、該検索されたシステムキーおよび該検索された同報通信キーを該所定の方法で畳み込んで、該選択された送信装置において生成された一意的なデータ暗号化キーを再現する手段と、
該受信されたデータのセットを該再現された暗号化キーで解読する解読器と、を含む、解読装置を有する、
データ伝送システム。
【請求項３８】
前記一意的なデータ暗号化キーが第３数Ｅのビットを含み、ＥがＳ以上である、請求項３７に記載のシステム。
【請求項３９】
各送信装置に設けられ、前記受信装置における前記メモリに記憶された前記システムキーを周期的に変更するための手段をさらに含む、請求項３７に記載のシステム。
【請求項４０】
各送信装置に設けられ、前記受信装置における前記メモリに記憶された前記一意的な同報通信キーを周期的に変更するための手段をさらに含む、請求項３７に記載のシステム。
【請求項４１】
複数Ｎの送信装置および少なくとも一つの受信装置を含むデータ伝送システムにおいて使用される暗号化装置であって、すべての送信装置に共通のシステムキーと各送信装置に一意的な同報通信キーとが存在し、該システムキーが、第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さく、該送信装置の一つにおいて使用される暗号化装置が、
該システムキーおよびそのプログラマー装置に対する同報通信キーを所定の方法で畳み込み、その送信装置に対して一意的な暗号化キーを生成する手段と、
該一意的なデータ暗号化キーでデータのセットを暗号化するための暗号器と、
該暗号化されたデータのセットを受信装置に伝送する手段と、
を含み、
該受信装置におけるメモリ内に該システムキーおよび該同報通信キーの各々が記憶されて、該プログラマー装置の各々において該プログラムキーを暗号化するのに用いられた該一意的なデータ暗号化キーが、該プログラマー装置の任意の一つから伝送された該暗号化プログラムキーを解読する目的のために該受信装置において再生され、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要なメモリの記憶容量が（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、
暗号化装置。
【請求項４２】

複数Ｎの送信装置および少なくとも一つの受信装置を含むデータ伝送システムにおいて使用される解読装置であって、各送信装置は、その送信装置に一意的な同報通信キーとすべての送信装置に対して同一のシステムキーとを設けられ、該システムキーが第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さく、各送信装置において、該システムキーおよびその送信装置に一意的な該同報通信キーが所定の方法で畳み込まれて一意的なデータ暗号化キーを生成し、各送信装置において生成された該一意的なデータ暗号化キーは、該受信装置へ伝送されるデータのセットを暗号化するために、その送信装置において使用され、該受信装置において使用される該解読装置が、該システムキーおよび該同報通信キーの各々を記憶するためのメモリであって、該システムキーおよび該同報通信キーを記憶するために必要な該メモリの記憶容量は、（（ＮｘＢ）＋Ｓ）ビットより大きくないメモリと、
該送信装置の選択された一つから暗号化データセットを受信するための手段と、
該システムキーおよび該選択された送信装置の該同報通信キーを該メモリから検索するための手段と、
該検索されたシステムキーおよび該検索された同報通信キーを該所定の方法で畳み込み、該選択された送信装置において生成された該一意的なデータ暗号化キーを再現し、該受信されたデータセットを暗号化するための手段と、
該再現された暗号化キーで該受信データセットを解読するための解読器と、
を含む解読装置。

【請求項４３】
少なくとも一つの受信装置への伝送のために送信装置において複数Ｎのデータセットを一意的に暗号化するための装置であって、各データセットに対して、そのデータセットに一意的な同報通信キーおよび各データセットに対して同一のシステムキーを該送信装置において設け、該システムキーが第１数Ｓのビットを含み、そして該同報通信キーの各々が第２数Ｂのビットを含み、ＢがＳよりも小さい装置において、該装置が、
該システムキーおよび該選択されたデータセットの該同報通信キーを所定の方法で畳み込み、そのデータセットに対して一意的なデータ暗号化キーを生成するための手段と、
そのデータセットに対して生成された該一意的なデータ暗号化キーで該データセットを暗号化するための暗号器と、
該受信装置に該暗号化データセットを伝送するための手段と、
を含み、
該受信装置におけるメモリ内に該システムキーおよび該同報通信キーの各々が記憶されて、各々の送信装置のそれぞれにおいて該データのセットを暗号化するのに用いられた該一意的なデータ暗号化キーが、該送信装置の任意の一つから伝送された該暗号化データのセットを解読する目的のために、該受信装置において再生され、該受信装置において該システムキーおよび該同報通信キーを記憶するために必要な該メモリの記憶容量が（（Ｎ×Ｂ）＋Ｓ）ビットより大きくない、装置。

【請求項４４】
該一意的なデータ暗号化キーが第３数Ｅのビットを含み、ＥがＳ以上である、請求項４３に記載の装置。

【請求項４５】
送信装置および少なくとも一つの受信装置を含むデータ伝送システムにおいて使用される解読装置であって、複数Ｎのデータセットの各々は、（ａ）各データセットに対して、そのデータセットに一意的な同報通信キーと各データセットに対して同一のシステムキーとを設けられ、該システムキーが第１数Ｓのビットを含み、該同報通信キーの各々が第２数Ｂのビットを含み、ＢはＳよりも小さいことと、（ｂ）各データセットに対して、該システムキーおよびそのデータセットに一意的な該同報通信キーを所定の方法で畳み込み、そのデータセットに対し一意的なデータ暗号化キーを生成することと、（ｃ）そのセットに対して生成された該一意的なデータ暗号化キーで各データセットを暗号化することとにより、該送信装置において一意的に暗号化され、該一意的に暗号化されたデータセットの各

々は受信装置に伝送され、該受信装置において使用される該解読装置が、
該システムキーおよび該同報通信キーの各々を記憶するためのメモリであって、該システムキーおよび該同報通信キーを記憶するために必要な該メモリの記憶容量は、（（ＮｘＢ）＋Ｓ）ビットより大きくないメモリと、
該送信装置から送信された該暗号化データセットのうちの選択された１つを受信するための手段と、
該システムキーおよび該選択されたデータセットに一意的な該同報通信キーを該メモリから検索するための手段と、
該検索されたシステムキーおよび該検索された同報通信キーを該所定の方法で畳み込み、該受信され選択されたデータセットを暗号化する送信装置において生成された該一意的なデータ暗号化キーを再現する手段と、
該再現された暗号化キーで該受信されたデータセットを解読するための解読器と、
を含む解読装置。

【発明の詳細な説明】

発明の分野

本発明は、一般に、データ暗号化に関し、そしてさらに詳細には、受信地点への伝送と続く解読のために複数の伝送地点において一意的にデータを暗号化するための方法及び装置に関する。本発明の方法及び装置により、受信地点における暗号化キー記憶要求条件が緩和される。

発明の背景

デジタル伝送技術を使用する通信システムが増大する時、非認可アクセスからデジタル情報を保護するための技術が、ますます重要になっている。例えば、加入テレビジョン産業は、デジタル及びアナログ伝送の両者を使用するすべてのデジタル伝送システム又はハイブリッドシステムに向けて移動し始めている。デジタルテレビジョン信号の非認可アクセスの防止は、加入テレビジョン産業において主要な関心である。

暗号法は、非認可アクセスを防止する非常に確実な手段を設ける。暗号法の技術は、非常に公知である。「ストリームサイファー暗号作成法」は、非認可アクセスを防止するために、デジタルデータを暗号化するために特に良く適する。第１図は、ストリームサイファー暗号作成法を使用する例示のシステム１０を示す。システム１０は、クリアデータストリームを暗号化するためのデータ暗号器１２、暗号化データストリームを続いて解読するためのデータ解読器１８、及び暗号器１２から解読器１８に暗号化データストリームを伝送するための伝送媒体１１を具備する。暗号器１２、１８は、一般に、技術において「ストリームサイファー」と呼ばれる。

図示された如く、データ暗号器１２は、擬似ランダムビット発生器１４とデータコンバイナー１６を具備する。その入力において、擬似ランダムビット発生器１４は、一意的な暗号化キーＫを受信する。暗号化キーＫを「シード」値として使用して、擬似ランダムビット発生器１４は、一般に「キーストリーム」と呼ばれる擬似ランダム２進シーケンスを発生する。それから、キーストリームは、別の入力においてクリアデータストリームを受信するコンバイナーの一つの入力に送られる。コンバイナー１６は、ビット毎のモジュロ２加算を使用して、ビット単位ベースにおいてキーストリームとクリアデータストリームを組み合わせる又は混合する。即ち、コンバイナー１６は、排他的ＯＲ（ＸＯＲ）ゲートを具備する。このようにしてクリアデータストリームをキーストリームと組み合わせると、クリアデータストリームを有効に暗号化する。図示された如く、暗号化データストリームは、その後、適切な伝送媒体１１を介して伝送される。

解読器１８は、暗号化データストリームからクリアデータストリームを回復するために動作する。図示された如く、解読器１９は、擬似ランダムビット発生器１４’とデコンバイナー１６’を具備する。技術における当業者は知っている如く、解読器１８は、暗号器１２においてデータを暗号化するために使用された同一暗号化キーＫを設けられなければならず、そして擬似ランダムビット発生器１４’は、擬似ランダムビット発生器１４と同一でなければならず、その結果、同一暗号化キーＫにより、擬似ランダムビット発生器１４

’は、暗号器１２において発生されたキーストリームを再現することができる。再現されたキーストリームと暗号化されたデータストリームは、その後、デコンバイナー１６’のそれぞれの入力に設けられる。デコンバイナー１６’は、暗号器１２におけるコンバイナー１６に関して相互又は相補的方式で動作しなければならず、その結果、暗号化プロセスは、有効に逆転される。技術における当業者は知っている如く、コンバイナー１６がビット毎のモジュロ２加算（即ち、ＸＯＲ化）を行う時、デコンバイナー１６’は、ＸＯＲ関数が対称的であるために、コンバイナー１６に同一である。こうして、暗号化データストリームと再現キーストリームのＸＯＲを取ると、暗号化プロセスを有効に逆転させる。クリアデータストリームは、その後、デコンバイナー１６’から出力される。

前述の議論から認められる如く、システム１０は、暗号器１２と解読器１８の両者が、各々、一意的な暗号化キーＫを設けられないならば、機能しない。このため、機密保持は、暗号化キーを秘密にしておくことに左右される。そのようなシステムは、一般に、「私用キー」暗号化システムと呼ばれる。「私用キー」暗号化システムにおいて機密保持を高める一つの方法は、暗号化キーを周期的に変更することである。機密保持はまた、擬似ランダムビット発生器によって発生されたキーストリームの「ランダム性」に依存する。システム開発者は、クリアデータストリームを暗号化データストリームと比較することによって実現可能に演繹されない擬似ランダムビット発生アルゴリズムを選択しなければならない。一般に、より大きなランダム性は、短いキーよりもむしろ、大きな暗号化キー（即ち、より多数のビット）を使用するアルゴリズムで達成される。

多くの応用において、暗号器は、遠隔受信地点への伝送のためのデータストリームを暗号化するために伝送地点において使用される。受信地点は、もちろん、暗号化データからクリアデータを回復するために、解読器を使用しなければならない。受信地点は伝送地点から遠隔であるために、確実な手段が、受信地点に適切な暗号化キーを設けるために使用されなければならない。例えば、暗号化キー自体は、暗号化され、その後、受信地点に伝送される。いったんキーが受信地点において受信されるならば、それは、受信地点において確実なメモリ装置に記憶されなければならない。代替的に、キーは、確実なメモリに事前記憶される。

通信システムは、しばしば、各々が一つ以上の受信地点にデータのセットを伝送する複数の異なる伝送地点を具備する。例えば、加入テレビジョンシステムにおいて、複数の「プログラマー」は、各々、加入テレビジョンサービス（即ち、プログラム）を遠隔加入者に設ける。各プログラマーは、一般に、それぞれの伝送地点においてデータを暗号化するために、それ自身の一意的な暗号化キーを使用することを望む。システムが非常に多数の伝送地点を含む時、各伝送地点に一意的な暗号化キーを設けることは、禁止される。上記の如く、システムの暗号強度を増大させるために、大きな暗号化キーを使用することが望ましい。一意的な暗号化キーの各々は、受信地点における解読器が伝送地点のいずれかから受信されたデータを解読することができるように受信地点において確実なメモリに記憶されなければならないために、問題が発生する。技術における当業者は知っている如く、確実なメモリは高価であり、そして確実なメモリ装置は、一般に、限定記憶容量を有する。このため、非常に多数の伝送地点が各々、データを一意的に暗号化することができるが、暗号化キーを記憶するために受信地点において必要なメモリの量を縮小する、システム及び方法の必要性がある。本発明は、この必要性を満足する。

発明の要約

本発明の一つの実施態様により、データのセットが、少なくとも一つの受信地点への伝送と続く解読のために、複数Ｎの伝送地点の各々において一意的に暗号化される。Ｎ伝送地点の各々は、その伝送地点に一意的な同報通信キーと、すべての伝送地点に対して同一のシステムキーを設けられる。システムキーは、複数Ｓのビットを具備し、Ｎ個の同報通信キーの各々は、一意的な複数Ｂのビットを具備し、この場合、ＢはＳよりも小さい。各伝送地点において、システムキーとその伝送地点に一意的な同報通信キーは、その伝送地点のために一意的なデータ暗号化キーを発生するために所定の方法で畳み込まれる。各伝送地点において発生された一意的な暗号化キーは、第３数Ｅのビットを具備し、Ｅは、Ｂよ

りも少なくとも大きい。好ましくは、Ｅは、Ｓ以上である。各伝送地点において、データのセットは、その後、その地点において発生された一意的なデータ暗号化キーで暗号化される。各伝送地点において一意的に暗号化されたデータのセットは、その後、受信地点に伝送される。受信地点におけるメモリにおいて、システムキーと同報通信キーの各々が記憶され、暗号化データセットの選択された一つを受信地点において解読可能にする。受信地点においてシステムキーと同報通信キーを記憶するために必要なメモリ容量は、（（Ｎｘ Ｂ）＋Ｓビットより大きくない。

受信地点において、伝送地点の選択された一つから伝送された暗号化データセットが、受信される。本発明により、システムキーと選択伝送地点に一意的な同報通信キーは、受信地点におけるメモリから検索される。畳み込み手段が、選択伝送地点において行われたと同一の所定の方法において、検索されたシステムキーと検索された同報通信キーを畳み込むために受信地点において設けられ、受信データセットを暗号化するために選択伝送地点において使用された一意的なデータ暗号化キーを再現する。受信された暗号化データセットは、その後、再現された暗号化キーで解読される。

受信地点は、伝送地点の選択グループのみからデータを受信するために認可される。そのような場合に、システムキーと選択グループの同報通信キーのみが、受信地点においてメモリに記憶される。暗号強度は、各伝送地点に設けられ、受信地点においてメモリに記憶されたシステムキー及び／又は一意的な同報通信キーを周期的に変更することにより高められる。

加入テレビジョンシステムの文脈において適用された時、伝送地点は、プログラムデータを伝送し局所的に発生されたプログラムキーでプログラムデータを暗号化する、加入テレビジョンシステムにおけるプログラマー地点を具備する。本発明のこの出願において、プログラマー地点において局所的に発生されたプログラムキーは、本発明の方法及び装置により暗号化される。加入テレビジョンシステムにおける受信地点は、ケーブル加入者又は直接同報通信衛星加入者の如く、ケーブルヘッドエンド設備又は加入者位置のいずれかである。

本発明の代替態様において、単一伝送地点における複数Ｎのデータセットは、各々、受信地点への伝送のためにその地点において一意的に暗号化される。この実施態様において、Ｎ個のデータセットの各々は、そのデータセットに一意的な同報通信キーと、各データセットに対して同一のシステムキーとを備える。次の段階が、その後、各データセットに対して行われる。（１）データセットに対して一意的なデータ暗号化キーを発生するために、システムキーとそのデータセットに一意的な同報通信キーを所定の方法で畳み込む段階と、（２）データセットに対して発生された一意的なデータ暗号化キーでデータセットを暗号化する段階と、（３）受信地点へ一意的に暗号化されたデータセットを伝送する段階である。前実施態様における如く、受信地点におけるメモリにおいて、システムキーと該同報通信キーの各々が記憶される。これらのキーは、暗号化データセットの選択された一つを受信地点において解読可能にするために受信地点において必要とされる。再び、受信地点においてシステムキーと同報通信キーを記憶するために必要なメモリ容量は、（（Ｎｘ Ｂ）＋Ｓ）ビットより大きくない。

本発明のいっそうの詳細及び特徴は、以後明らかになるであろう。

【図面の簡単な説明】

前述の要約並びに好ましい実施態様の次の詳細な説明は、添付の図面に関連して精読した時、より良く理解される。発明を例示する目的のために、図面において、現在好ましい実施態様が示されるが、発明は、開示された特定の方法及び装置に限定されないことが理解される。図面において、

第１図は、暗号法技術を使用する先行技術のデータ伝送システムのブロック図である。

第２図は、本発明の暗号化及び解読方法及び装置の好ましい実施態様により動作するデータ伝送システムのブロック図を示す。

第３図と第４図は、加入テレビジョンシステムへの本発明の適用を示す。

第５図は、本発明の代替態様により動作するデータ伝送地点のブロック図である。

発明の詳細な説明

好ましい実施態様において、本発明は、複数Ｎの伝送地点に、各々、少なくとも一つの受信地点への伝送のためのデータのセットを一意的に暗号化させる。しかし、最も重要なことには、本発明の方法及び装置では、各伝送地点における一意的な暗号化は、暗号化キーを記憶するために受信地点において相当な量の記憶容量を必要とすることなく達成される。本発明は、複数の伝送地点の各々においてデータの独立な暗号化を必要とする通信システムにおいて使用されるが、本発明は、加入テレビジョンシステムの文脈において特定の応用を有する。本発明が使用される例示の加入テレビジョンシステムは、“Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｔｒａｎｓｍｉｔｔｉｎｇ ａ Ｐｌｕｒａｌｉｔｙ ｏｆ Ｄｉｇｉｔａｌ Ｓｅｒｖｉｃｅｓ”（Ａｔｔｏｒｎｅｙ Ｄｏｃｋｅｔ ＳＡ－００１９Ａ）と題する１９９２年１０月３０日に提出された同時係属米国出願第０７／９６８、８４６号において記載される。

同様の番号が同様の要素を示す図面を参照すると、第２図において、複数Ｎの伝送地点２２、２４、２８と少なくとも一つの受信地点３０を具備するシステム２０の機能ブロック図が示される。本発明により、各伝送地点２２、２４、２８に共通のシステムキー４０が設けられる。各伝送地点２２、２４、２８は、その伝送地点に一意的なそれぞれの同報通信キー４２、４４、４８をさらに備える。システムキー”ＳＫ”は、第１数のビットＳを具備し、そして各同報通信キー”ＢＫ”は、第２数のビットＢを具備する。本発明の重要な見地により、Ｂは、Ｓよりも小さい。例えば、システムキーは、５６ビット（Ｓ＝５６）を具備するが、各同報通信キーは、わずかに８ビット（Ｂ＝８）を有していてよい。

任意の手段が、各伝送地点にシステムキー４０とその地点に一意的な同報通信キーを設けるために使用される。例えば、システムキーと同報通信キーの両者は、国内制御センターの如く、遠隔位置からそれぞれの各伝送地点へ伝送され、あるいはキーの一方又は両方が、伝送地点において事前記録される。代替的に、少なくとも同報通信キーは、それぞれの伝送地点において局所的に発生される。請求の範囲において、用語「設ける」は、そのような可能性のすべてを覆うために使用された。

各伝送地点２２、２４、２８には、データのセット、例えば、データ３２、３４と３８をそれぞれ暗号化するための装置を設けてある。第２図において示された如く、各伝送地点２２、２４、２８における暗号化装置は、その地点のための一意的なデータ暗号化キーを発生するために、所定の方法でシステムキーとその地点に一意的な同報通信キーを畳み込むための手段５０を具備する。技術における当業者が認める如く、その地点において一意的な暗号化キーを発生するために、各伝送地点においてシステムキーと同報通信キーを畳み込むために無数の方法がある。例えば、システムキーの選択ビットは、同報通信キーの選択ビットと排他的論理和を取られる。代替的に、ずっと複雑な畳み込みが、例えば、システムキーと同報通信キーを複雑な一方向関数に通過させることにより行われる。請求の範囲において使用された如く、用語「畳み込み(convolving)」は、そのような可能性のすべてを覆うことを意図される。

本発明により、それぞれの畳み込み手段５０によって各伝送地点２２、２４、２８において発生された一意的なデータ暗号化キーは、各々、第３数Ｅのビットを具備する。好ましくは、Ｅは、Ｓ以上である。背景において述べた如く、より大きな暗号化キーにより、より大きな「ランダム性」が、クリアデータストリームの暗号化中達成され、これにより、システムの暗号強度を増大させる。技術における当業者は認める如く、各伝送地点において一意的な同報通信キーでシステムキーを畳み込むと、一意的な同報通信キーのみよりも大きな一意的な暗号化キーを各伝送地点に設ける。後述される如く、本発明により、システムキーと同報通信キーのみが、解読目的のために受信地点において設けられる必要がある。結果的に、受信地点においてシステムキーと同報通信キーの各々を記憶するために必要なメモル容量は、（（ＮｘＢ）＋Ｓ）ビットより大きくない。

好ましくは、各地点２２、２４、２８における畳み込み手段５０は、同一である。即ち、それらは、各々、同一の所定の方法でそれぞれの同報通信キーとシステムキーを畳み込む。各伝送地点２２、２４、２８において、その地点において畳み込み手段５０によって発

生された一意的なデータ暗号化キーは、それぞれの暗号器５４に送られる。各伝送地点２２、２４、２８において使用された手段５０と同様に、それぞれの伝送地点において使用された暗号器５４は、好ましくは、同様に機能する。各暗号器５４は、それぞれの伝送地点２２、２４、２８において畳み込み手段５０によって発生された一意的なデータ暗号化キーによりそれぞれのデータセット（例えば、データ３２、３４又は３８）を暗号化する。技術における当業者は知っている如く、キーベース暗号器を実現するために多数の方法があり、そして各伝送地点２２、２４、２８における暗号器５４は、いずれかの実現に限定されない。例えば、各暗号器５４は、第１図の暗号器１２の如く、ストリームサイファーである。そのような場合に、各暗号器５４における擬似ランダムビット発生器は、好ましくは、同一である。代替的に、暗号器５４は、非常に公知のデジタル暗号化標準（ＤＥＳ）アルゴリズムを実現する。技術における当業者には、暗号器５４がどのような暗号化関数を実現したとしても、各暗号器５４は一方向関数を規定することが認められるであろう。

さらに第２図を参照すると、各暗号器５４の出力は、コンバイナー／送信器５６に結合される。コンバイナー／送信器５６は、各暗号器５４から出力された暗号化データセットを組み合わせ、組み合わされたデータを受信地点３０の如く受信地点に伝送するために動作する。コンバイナー／送信器５６は、所与の応用のために適する任意の方法で暗号化データセットを組み合わせる。例えば、コンバイナー５６は、周波数分割多重化を行う。代替的に、コンバイナー５６は、時分割多重化機構を使用して、暗号化データセットを組み合わせる。技術における当業者が認める如く、コンバイナー／送信器５６の機能は、本発明の特定の応用に依存する。幾つかの応用において、コンバイナー／送信器５６は、各伝送地点２２、２４、２８から遠隔に位置する。そのような場合に、伝送地点の各々は、まず、それぞれの暗号化データセットをその遠隔地点に伝送しなければならない。暗号化データセットは、その後、遠隔地点において組み合わされ、その遠隔地点から受信地点に再伝送されなければならない。例えば、加入テレビジョンシステムにおいて、暗号化データは、しばしば、各伝送位置から衛星を介してケーブルヘッドエンド設備に個別に伝送される。ケーブルヘッドエンド設備は、その後、個別暗号化データストリームを単一ケーブルテレビジョン信号に組み合わせ一つ以上の受信地点へ伝送するために動作する。システム２０は、伝送地点のすべてが、それぞれの暗号化データを同時に伝送することを必要としないことが理解される。任意の所与の時点において、一つ以上の伝送地点はアイドル状態である。

組み合わせの後、暗号化データセットは、適切な媒体５８を介して、受信地点３０の如く受信地点に伝送される。システムキー４０と同報通信キー４２、４４、４８の各々は、受信地点においてメモリ６０に記憶される。メモリ６０にシステムキーと同報通信キーを供給するために任意の方法が使用される。例えば、システムキーと同報通信キーは、メモリ６０に事前記憶される。代替的に、システムキー及び／又は同報通信キーは、国内制御センサーの如く、遠隔位置から受信地点に伝送される。同報通信キーが各伝送地点において局所的に発生されるならば、各伝送地点は、例えば、受信地点において現場設置を行うか、又は代替的に、メモリ６０への自動挿入のために受信地点にそれぞれの同報通信キーを伝送することにより、メモリ６０にそれぞれの同報通信キーを設けるために責任を負う。上記の如く、受信地点においてシステムキーと同報通信キーの各々を記憶するために必要なメモリ容量は、（（ＮｘＢ）＋Ｓ）ビットより大きくない。後述の如く、受信地点におけるこれらのキーの記憶は、選択伝送地点から伝送された暗号化データセットを受信地点において解読可能にする。

受信地点３０における解読装置は、各伝送地点から伝送された暗号化データセットを受信し、解読のためにこれらの受信データセットの一つを選択するための受信器６２を具備する。図示された如く、セレクト線６３は、受信データセットの一つの選択を制御する。コンバイナー／送信器５６と同様に、受信器６２の詳細な動作は、本発明の特定の応用に依存する。周波数分割多重化が使用される時、受信器６２は、所与の搬送周波数において選択伝送地点から伝送された暗号化データセットを受信するための同調器として機能する。

代替的に、時分割多重化がコンバイナー／送信器５６において使用される時、受信器６２は、入りデータ信号を多重分離し、多重化データストリームから選択データセットを受信するために動作する。こうして、暗号化データセットは組み合わされるが、受信器６２は、伝送地点２２、２４、２８の選択された一つから伝送された暗号化データセットを受信するために相応して動作する。

受信地点における解読装置は、さらに、メモリ３０からシステムキー４０と選択伝送地点に一意的な同報通信キー（例えば、同報通信キー４２、４４又は４８）を検索するための手段を具備する。例えば、伝送地点２２から伝送された暗号化データセットが受信器６２において受信のために選択されるならば、システムキー”ＳＫ”と同報通信キー４２（BK_1）が、メモリ３０から検索される。例えば直接メモリアドレス指定の如く、任意の適切な検索手段が使用される。第２図において、検索手段は、ライン６３を介して使用者の選択を受け取り、ライン６８において適切な同報通信キーを出力するＮ対１マルチプレクサー６６として機能的に描かれる。

検索されたシステムキーと検索された同報通信キーは、それぞれ、ライン７０と６８を介して畳み込み手段７２に供給される。畳み込み手段７２は、受信データセットを暗号化するために、選択伝送地点において使用された一意的な暗号化キーを再現するように検索されたシステムキーと検索された同報通信キーを畳み込む。このため、認められる如く、畳み込み手段７２は、選択伝送地点における畳み込み手段５０と同一の所定の方法で機能しなければならない。上記の如く、各伝送地点における畳み込み手段５０は、好ましくは、同一である。しかし、これは必須なことではない。しかし、一つ以上の伝送地点における畳み込み手段５０が異なるならば、受信地点３０における解読装置は、いろいろな伝送地点において使用された異なる畳み込み手段の各々に対する対応する畳み込み手段を含まなければならない。技術における当業者は認める如く、各伝送地点において同一の畳み込み手段５０を使用することは、単一畳み込み手段７２が使用されることにおいて、受信地点３０における解読装置を簡易化する。

解読装置は、さらに、それぞれの入力において受信された暗号化データセットと再現された暗号化キーを受け取り、再現された暗号化キーで暗号化データセットを解読する解読器６４を具備する。解読されたデータセットは、所望に応じて、受信地点における使用のためにライン７６を介して出力される。畳み込み手段７２と同様に、解読器６４は、データセットを暗号化するために、選択された伝送地点において使用された暗号器５４と同様に機能しなければならない。即ち、解読器６４と選択伝送地点における暗号器５４は、同一暗号化機能を実現しなければならない。例えば、デジタル暗号化標準（ＤＥＳ）アルゴリズムが選択伝送地点において暗号器５４によって実現されるならば、解読器６４は、同一アルゴリズムを実現しなければならない。受信地点において解読装置を簡易化するために、いろいろな伝送地点における暗号器５４は、好ましくは、同一である。しかし、再び、解読器が、いろいろな暗号化地点において使用された異なる各暗号器に対して受信地点において使用される限り、これは、必要なことではない。

このため、動作において、所与の伝送地点は、システムキー”ＳＫ”とその地点に一意的な同報通信キー”ＢＫ”を設けられる。例えば、伝送地点２２は、システムキー”ＢＫ”とその地点２２に一意的な同報通信キー２２（BK_1）を設けられる。伝送地点２２において、システムキー４０と一意的な同報通信キー４２が、その伝送地点２２のための一意的なデータ暗号化キーを発生するために所定の方法で畳み込まれる。一意的なデータ暗号化キーは、その後、ライン５２を介して、地点２２における暗号化５４に設けられる。暗号器５４は、一意的なデータ暗号化キーでデータセット３２を暗号化する。暗号化データセットは、その後、受信地点３０に伝送される。他の各伝送地点（例えば、地点２４と２８）も、自身の暗号化データセットを設けるために同様の方法で動作する。各伝送地点からの暗号化データセットは、その後、受信地点３０への伝送のために組み合わされる。

受信地点３０において、伝送地点の一つから伝送された暗号化データセットは、受信と続く解読のために、ライン６３を介して選択される。従って、選択データセットは、受信器６２によって受信され、解読器６４に設けられる。例えば、伝送位置２８から伝送された

暗号化データセットは、受信され、解読器６４に設けられる。いったん暗号化データセットが受信されたならば、システムキー４０と伝送地点２８に一意的な同報通信キー４８（即ち、”BK_N”）が、メモリ６０から検索される。畳み込み手段７２は、伝送地点２８における畳み込み手段５０と同一の所定の方法で検索されたシステムキー４０と検索された同報通信キー４８を畳み込み、データセット３８を暗号化するために、伝送地点２８において使用された一意的なデータ暗号化キーを再現する。再現された暗号化キーは、その後、受信データセットを解読する解読器６４に設けられる。

上記が示す如く、本発明の方法及び装置により、複数の伝送地点は、各々、比較的大きな一意的な暗号化キー（即ち、畳み込み手段５０によって発生された一意的な暗号化キー）を使用して、それぞれのデータセットを一意的に暗号化することができる。しかし、最も重要なことは、特定の受信地点におけるメモリ６０の記憶容量は、一意的な暗号化キーが記憶される必要はないために最小化される。むしろ、より小さな同報通信キーが記憶される。

多数の応用において、受信地点は、選択伝送地点グループからデータを受信するためにのみ認可される。本発明により、そのような場合に、システムキーと選択グループの同報通信キーのみが、受信地点においてメモリ６０に記憶される。メモリ６０は、選択伝送地点グループの同報通信キーのみを含むために、解読装置は、これらの地点から伝送されたデータのみを解読することができる。特定伝送地点の同報通信キーがないと、解読装置は、その伝送地点においてデータを暗号化するために使用された一意的なデータ暗号化キーを再現することができない。結果的に、選択伝送地点グループの同報通信キーのみを記憶することにより、他の（即ち、非認可）地点から伝送されたデータへのアクセスは、排除される。このため、技術における当業者は認める如く、条件付きアクセス機構が、本発明の方法及び装置で容易に実現される。付加的に、いろいろな受信地点が選択伝送地点グループの同報通信キーのみを記憶するために、システム機密保持は、システムアタッカーが単一受信地点における確実なメモリの内容を決定することができるならば、完全には妥協されない。

システム機密保持を高めるために、システムキー及び／又は各伝送地点の同報通信キーは、周期的に変更される。技術における当業者が認める如く、キーは、伝送及び受信地点の双方で変更されなければならない。上記の方法は、新しいシステム及び同報通信キーを受信地点と伝送地点に供給するために使用される。

前述の如く、本発明は、加入テレビジョンシステムへの特定の応用を有する。加入テレビジョンシステムにおいて、複数の個別「プログラマー」地点は、各々、プログラムデータ（例えば、映画、新サービス及び有料視聴イベントの如くペイテレビジョンサービス）を複数のシステム加入者に設ける。第３図は、本発明の方法と装置を具現する例示の「プログラマー」地点の機能ブロック図である。

第３図に示された如く、例示のプログラマー地点１００は、その地点においてプログラムデータ１０２を暗号化するための暗号器１０４を有する。暗号器１０４は、局所的に発生された「プログラムキー」１０６でプログラムデータ１０２を暗号化する。「プログラマー」によるプログラムデータの暗号化は、そのプログラマーのデータへの非認可アクセスを防止する。”Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｔｒａｎｓｍｉｔｔｉｎｇ ａ Ｐｌｕｒａｌｉｔｙ ｏｆ Ｄｉｇｉｔａｌ Ｓｅｒｖｉｃｅｓ”（Ａｔｔｏｒｎｅｙ Ｄｏｃｋｅｔ ＳＡ－００１９Ａ）と題する１９９２年１０月３０日に提出された、同時係属米国特許出願０７／９６８，８４６号において記載された如く、暗号強度は、一定間隔においてプログラムキーを変更することにより高められる。好ましくは、プログラムキーは、毎秒数回変更される。結果的に、プログラムキーの連続ストリームが、プログラマー地点において局所的に発生される。キーベース暗号化機構と同様に、解読装置がデータを暗号化するために使用された同一のプログラムキーを供給されるならば、解読が行われる。従って、加入テレビジョンシステムにおいて、各プログラマーは、それぞれのプログラムデータを暗号化するために使用されたプログラムキーをプログラムデータを解読することを望む任意の位置に供給しなければならない。遠隔位置に必要なプログラム

キーを供給する好ましい方法は、暗号化するために使用されたプログラムキーをデータと多重化し、それから、多重化プログラムキーと暗号化プログラムデータを遠隔位置に伝送することである。そのような方法は、”Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｔｒａｎｓｍｉｔｔｉｎｇ ａ Ｐｌｕｒａｌｉｔｙ ｏｆ Ｄｉｇｉｔａｌ Ｓｅｒｖｉｃｅｓ”と題する前述の同時係属米国特許出願において非常に詳細に記載される。しかし、プログラムキーが伝送中に割り込まれるならば、システム機密保持は、妥協される。このため、プログラマー地点はまた、伝送されたプログラムキーを暗号化しなければならない。複数のプログラマー地点を具備する加入テレビジョンシステムにおいて、各プログラマー地点は、一般に、その地点から伝送されたプログラムキーを一意的に暗号化することを望む。本発明の方法及び装置は、これらのプログラムキーを暗号化するために特に適する。

本発明により、加入テレビジョンシステムにおいて適用される時、システムにおける各プログラマー地点は、そのプログラマー地点に一意的な同報通信キーとすべての地点に対して同一のシステムキーを備える。システムキーとそれぞれの同報通信キーを各プログラマー地点に設けるために任意の方法が使用される。幾つかの加入テレビジョンシステムは、国内制御センターを含み、そのようなシステムにおいて、システムキー及び／又は同報通信キーは、国内制御センターから衛星を介して各プログラマー地点に設けられる。しかし、好ましくは、各プログラマーは、局所的にそれぞれの同報通信キーを発生する。代替的に、システムキー及び／又は同報通信キーは、郵便サービスを介して交付される。請求の範囲において、用語「設ける」は、そのような可能性のすべてを覆うことを意図される。

第３図において、システムキーと例示のプログラマー地点１００に一意的な同報通信キーは、それぞれ、ブロック１０８と１１０において示される。

第３図に示された如く、畳み込み手段５０は、その地点のための一意的な暗号化キーを発生するために、システムキー１０８とその地点に一意的な同報通信キー１１０を畳み込むためにプログラマー地点１００において設けられる。第３図の畳み込み手段５０は、第２図の畳み込み手段に同一である。プログラマー地点１００において畳み込み手段５０によって発生された一意的な暗号化キーは、ライン５２を介して暗号器５４に送られる。第３図の暗号器５４は、第２図の暗号器５４に同一である。暗号器５４は、畳み込み手段５０によって発生された一意的な暗号化キーでプログラマー地点１００において局所的に発生されたプログラムキー１０６を暗号化するために動作する。マルチプレクサー１１２は、一入力における暗号化プログラムキーと別の入力における暗号化プログラムデータを受け取る。マルチプレクサー１１２は、任意の非常に公知の方法においてプログラムキーとプログラムデータを多重化し、多重化データを受信地点に伝送する。上記の如く、受信地点への伝送のために暗号化プログラムキーとプログラムデータを多重化する好ましい方法は、”Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｔｒａｎｓｍｉｔｔｉｎｇ ａ Ｐｌｕｒａｌｉｔｙ ｏｆ Ｄｉｇｉｔａｌ Ｓｅｒｖｉｃｅｓ”（Ａｔｔｏｒｎｅｙ Ｄｏｃｋｅｔ Ｎｏ．ＳＡ－００１９Ａ）と題する１９９２年１０月３０日に提出された同時係属米国特許出願第０７／９６８，８４６号において見いだされる。

本発明の方法及び装置を使用する加入テレビジョンシステムにおいて、各プログラマー地点において発生された多重化プログラムキーとプログラムデータは、一般に、各地点から衛星を介していろいろな受信地点に伝送される。技術における当業者は知っている如く、加入テレビジョンシステムにおける受信地点は、ケーブルヘッドエンド設備、ケーブル加入者又は直接同報通信衛星（ＤＢＳ）加入者である。第４図は、本発明を具現する加入テレビジョンシステム受信地点の詳細を示す機能ブロック図である。図示の如く、複数のプログラマー地点の各々（例えば、第３図の地点１００）から伝送された暗号化プログラムデータとそれぞれのプログラムキーは、受信器６２において受信される。一般に、各プログラマー地点から伝送されたデータは、明確な搬送周波数において受信地点に設けられる。ライン６３において設けられた選択信号に応答して、受信器６２は、プログラマー地点の選択された一つから伝送されたプログラムデータとプログラムキーを受信するために適切な搬送周波数に「同調」する。上記の如く、所与のプログラマー地点から伝送されたプ

ログラムデータとプログラムキーは、多重化フォーマットである。結果的に、第４図に示された如く、選択プログラマー地点から受信されたデータは、デマルチプレクサー１１６に供給される。多重分離の後、受信された暗号化プログラムデータは、ライン１２０を介して解読器１２２に設けられ、そして受信された暗号化プログラムキーは、解読器６４に設けられる。

受信地点におけるメモリ６０は、システムキー１０８と、各プログラマー地点に一意的な同報通信キー（例えば、キー１１０、１１０’と１１０”）を記憶する。システムキーと同報通信キーをメモリ６０に供給するために任意の方法が使用される。例えば、システムキーと同報通信キーは、メモリ６０において事前記憶される。代替的に、システムキー及び／又は同報通信キーは、メモリ６０への自動挿入のために、国内制御センターの如く遠隔位置から受信地点に伝送される。上記の如く、同報通信キーは、好ましくは、各プログラマー地点において局所的に発生される。そのような場合に、個別プログラマーは、例えば、受信地点において現場設置を行うか、又は代替的に、メモリ６０への自動挿入のために受信地点にそれぞれの同報通信キーを伝送することにより、その地点におけるメモリ６０への挿入のために、所与の受信地点にそれぞれの同報通信キーを設ける。

さらに第４図を参照すると、システムキーと選択伝送地点に一意的な同報通信キー（例えば、同報通信キー１１０、１１０’又は１１０”）をメモリ６０から検索するための手段が設けられる。例えば、直接メモリアドレス指定の如く、任意の適切な検索手段が使用される。第４図において、検索手段は、ライン６３を介して使用者の選択を受け取り、ライン６８において適切な同報通信キーを出力する、Ｎ対１マルチプレクサー６６として機能的に描かれる。

検索されたシステムキーと検索された同報通信キーは、それぞれ、ライン７０と６８を介して畳み込み手段７２に供給される。畳み込み手段７２は、受信されたプログラムキーを暗号化するために、選択されたプログラマー地点において使用された一意的な暗号化キーを再現するように検索されたシステムキーと検索された同報通信キーを畳み込む。畳み込み手段７２は、もちろん、選択されたプログラマー地点における畳み込み手段５０と同一の所定の方法で機能しなければならない。解読器６４は、それぞれの入力において受信された暗号化プログラムキーと再現された暗号化キーを受け取り、再現された暗号化キーで暗号化プログラムキーを解読する。畳み込み手段７２と同様に、解読器６４は、選択されたプログラマー地点において使用された暗号器５４と同様に機能しなければならない。即ち、解読器６４と選択されたプログラマー地点における暗号器５４は、同一の暗号化機能を実現しなければならない。解読されたプログラムキーは、ライン７６を介して解読器１２２に出力される。解読されたプログラムキーにより、解読器１２２は、受信された暗号化プログラムデータを解読することができる。解読されたプログラムデータは、その後、所望に応じて受信地点における使用のためにライン１２４を介して出力される。

第５図は、本発明の代替態様を示し、この場合、上記の方法及び装置が、伝送地点１３０における複数Ｎのデータセット１３２、１３４、１３８を一意的に暗号化させるために、単一伝送地点１３０において使用される。この代替態様により、伝送地点１３０における各データセット１３２、１３４、１３８は、そのデータセットに一意的なそれぞれの同報通信キー１４２、１４４、１４８を設けられる。すべてのデータセット１３２、１３４、１３８に共通なシステムキー１４０がまた、設けられる。システムキー”ＳＫ”は、第１数のビットＳを具備し、そして各同報通信キー”ＢＫ”は、第２数のビットＢを具備する。本実施態様の重要な見地により、ＢはＳよりも小さい。

前述の任意の手段は、システムキー１４０と同報通信キー１４２、１４４、１４８を伝送地点１３０を設けるために使用される。請求の範囲において、用語「設ける」は、そのような可能性のすべてを覆うために使用された。各データセット１３２、１３４、１３８に対して、畳み込み手段１５０は、そのデータセットに対する一意的なデータ暗号化キーを発生するために所定の方法でシステムキー１４０とそのデータセットに一意的な同報通信キーを畳み込みために設けられる。畳み込み手段１５０は、第２図と第３図の畳み込み手段５０と同様に機能する。各データセット１３２、１３４、１３８に対して発生された一

意的なデータ暗号化キーは、第３図Ｅのビットを具備する。好ましくは、ＥはＳ以上である。背景において記載された如く、暗号化キーが大きいほど、クリアデータストリームの暗号化中、より大きな「ランダム性」が達成され、これにより、システムの暗号強度を増大させる。技術における当業者は認める如く、各データセットに対して一意的な同報通信キーとシステムキーを畳み込むことは、一意的な同報通信キーのみよりも大きい一意的な暗号化キーを各データセットに設ける。後述される如く、本実施態様により、システムキーと同報通信キーは、解読目的のために受信地点におけるメモリに記憶される。受信地点においてシステムキーと同報通信キーの各々を記憶するために必要なメモリ容量は、（（ＮｘＢ）＋Ｓ）ビットより大きくない。

好ましくは、畳み込み手段１５０は、同一である。即ち、それらは、各々、同一の所定の方法でそれぞれの同報通信キーとシステムキーを畳み込む。各畳み込む手段１５０によって発生された一意的なデータ暗号化キーは、それぞれの暗号器１５４に送られる。各暗号器１５４は、そのデータセットに対して発生された一意的なデータ暗号化キーでそれぞれのデータセット１３２、１３４、１３８を暗号化する。暗号器１５４は、第２図と第３図の暗号器５４と同一である。好ましくは、暗号器１５４は、各々、同様な方法で機能する。即ち、それらは、各々、同一の暗号化アルゴリズムによりデータを暗号化する。技術における当業者は知っている如く、キーベース暗号器を実現するために多数の方法があり、そして暗号器１５４は、いずれの実現にも限定されない。例えば、各暗号器１５４は、第１図の暗号器１２の如く、ストリームサイファーである。そのような場合に、各暗号器１５４における擬似ランダムビット発生器は同一になる。代替的に、暗号器１５４は、非常に公知なデジタル暗号化標準（ＤＥＳ）アルゴリズムを実現する。技術における当業者には、暗号器１５４がどのような暗号化関数を実現しても、各暗号器１５４は、一方向関数を規定することが認められるであろう。

さらに第５図を参照すると、各暗号器１５４の出力は、コンバイナー／送信器１５６に結合される。コンバイナー／送信器１５６は、各暗号器１５４から出力された暗号化されたデータセットを組み合わせ、第１図の受信地点３０の如く受信地点に組み合わせデータを伝送するために動作する。コンバイナー／送信器１５６は、所与の応用に対して適切な任意の方法で暗号化データセットを組み合わせる。例えば、コンバイナー１５６は、周波数分割多重化を行う。代替的に、コンバイナー１５６は、時分割多重化機構を使用して、暗号化データセットを組み合わせる。技術における当業者は認める如く、コンバイナー／送信器１５６の機能は、本発明の特定の応用に依存する。

記載された如く、上記の本発明の代替態様は、受信地点への伝送のために単一伝送位置において複数のデータセットを一意的に暗号化するための手段を設ける。技術における当業者は認める如く、第１図の受信地点３０は、第５図の伝送位置１３０から伝送された暗号化データセットの選択された一つを受信及び解読するために使用される。暗号化データが複数の伝送地点の各々から伝送される（第１図）か、又は複数の暗号化データセットが、各々、単一伝送地点から伝送される（第５図）かに拘わらず、第１図の受信地点３０は、同様な方法で動作する。

技術における当業者には、広い発明の概念に反することなく、上記の実施態様に変更が行われることが認められるであろう。このため、この発明は、開示された特定の実施態様に限定されず、添付の請求の範囲によって規定された発明の範囲と精神内にあるすべての修正を包含することが意図される。

【図１】

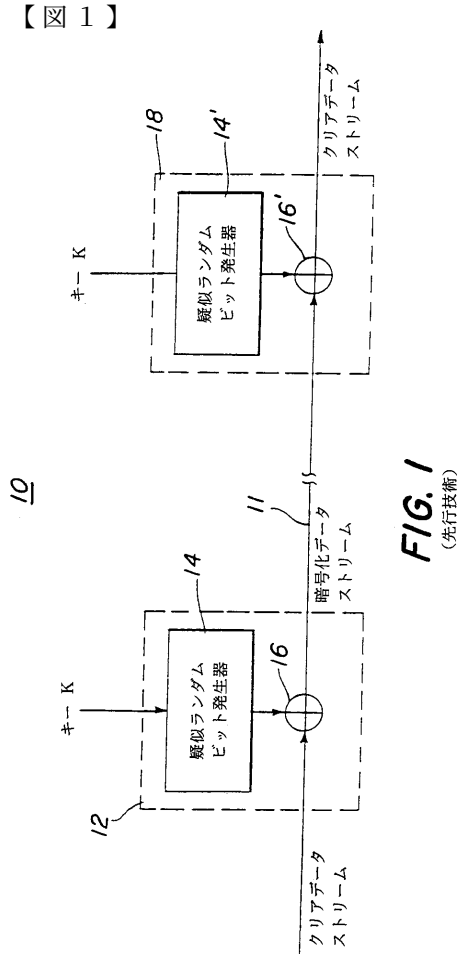

FIG. 1
(先行技術)

【図２】

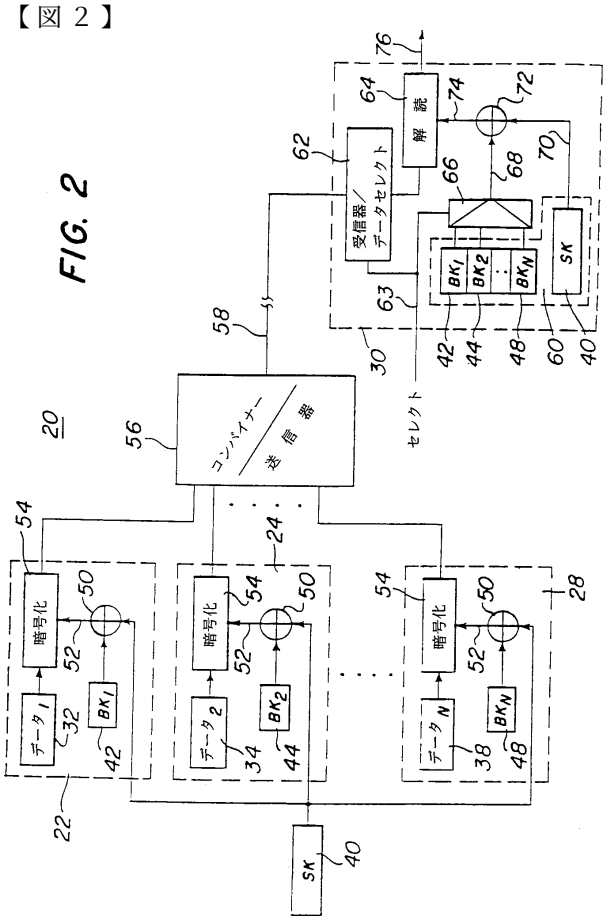

FIG. 2

【図３】

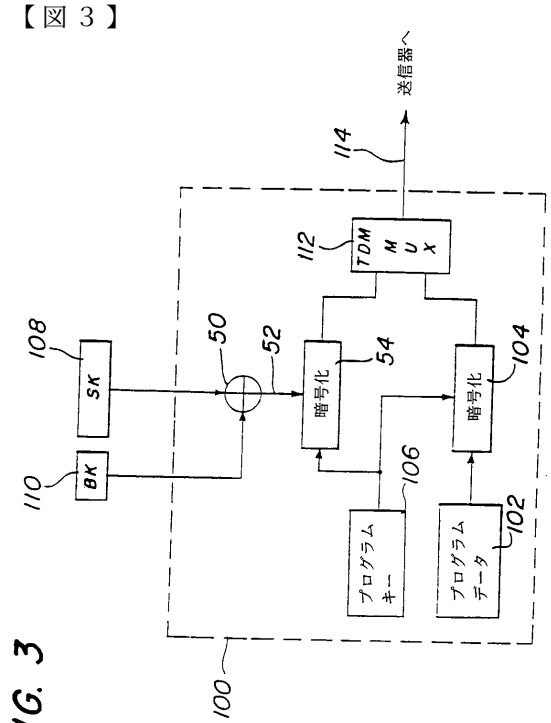

FIG. 3

【図４】

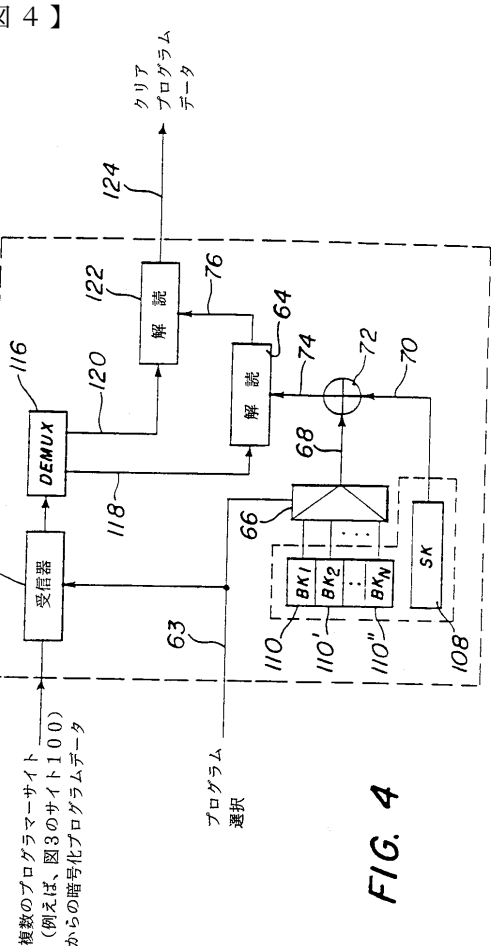

FIG. 4

【図５】

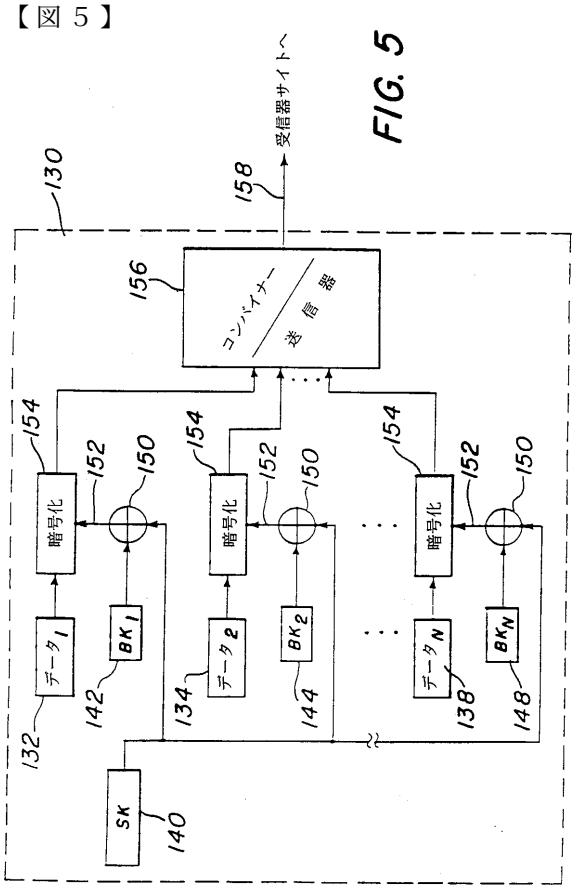
130
158
受信器サイトへ
156
コンバイナー／送信器
154
152
150
暗号化
データ1
BK1
132
142
134
データ2
BK2
144
データN
BKN
138
148
SK
140

FIG. 5

フロントページの続き

(72)発明者 ガミー，キース
カナダ・オンタリオ エル３ピー １ダブリユー１・マーカム・ホークリツジアベニユー５１

合議体
審判長 井関 守三
審判官 林 毅
審判官 長島 孝志

(56)参考文献 特開平１－２３３８５１（ＪＰ，Ａ）
特開平３－１０１５３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/00
G09C 1/00
H04H 1/00
H04N 7/167