(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4023818号
(P4023818)
(45)発行日　平成19年12月19日(2007.12.19)　(24)登録日　平成19年10月12日(2007.10.12)

(51)Int.Cl.		F I		
G11B 20/10	(2006.01)	G11B	20/10	H
H04L 9/14	(2006.01)	H04L	9/00	641
H04L 9/32	(2006.01)	H04L	9/00	673D

請求項の数 21　(全 12 頁)

(21)出願番号	特願平8-503468
(86)(22)出願日	平成7年6月27日(1995.6.27)
(65)公表番号	特表平10-502479
(43)公表日	平成10年3月3日(1998.3.3)
(86)国際出願番号	PCT/US1995/008324
(87)国際公開番号	WO1996/000963
(87)国際公開日	平成8年1月11日(1996.1.11)
審査請求日	平成11年5月18日(1999.5.18)
審判番号	不服2003-21808(P2003-21808/J1)
審判請求日	平成15年11月10日(2003.11.10)
(31)優先権主張番号	08/267,635
(32)優先日	平成6年6月29日(1994.6.29)
(33)優先権主張国	米国(US)

(73)特許権者　503411967
マクロヴィジョン　コーポレイション
アメリカ合衆国　カリフォルニア州　９５０５０　サンタクララ　デ・ラ・クルーズ・ブールバード　２８３０
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　ライアン，ジョン　オー
アメリカ合衆国，カリフォルニア州　９５０１４，クパティーノ，クリークサイド・コート　２２０１５番

最終頁に続く

(54)【発明の名称】種々の記録媒体用のコピー防止の方法及び装置

(57)【特許請求の範囲】

【請求項１】

コピーが防止されるべき光ディスクに認証用署名を記録用ヘッドの半径方向の位置変調により付加する段階と、

プログラムデータを第１の暗号化器に通す段階と、

上記第１の暗号化器からの暗号化されたプログラムデータ又は暗号化されていないプログラムデータを選択的に第２の暗号化器に通す段階であり、上記認証用署名が光ディスクに付加されるときには上記第１の暗号化器からの暗号化されたプログラムデータを第２の暗号化器に通す段階と、

上記第２の暗号化器からの上記データを光ディスクに記録する段階と、

光ディスク再生装置内で上記認証用署名を検出する段階と、

上記光ディスクからの復号データを第１の暗号解読器に通す段階と、

上記第１の暗号解読器からの上記第１の暗号解読されたデータを第２の暗号解読器に通す段階と、

認証用署名が検出されたとき、上記第２の暗号解読器の出力を選択し、認証用署名が検出されないとき、上記第１の暗号解読器の出力を選択する段階と、

を有するプログラム配付光ディスクにコピー防止を設ける方法。

【請求項２】

上記第１の暗号化器及び上記第２の暗号解読器は互いに逆の関係である暗号化関数及び復号化関数を実行する請求項１記載の方法。

【請求項３】
上記第２の暗号化器及び上記第１の暗号解読器は、非対称又は公開鍵暗号化システムの相補的な部分である請求項１記載の方法。
【請求項４】
上記第１の暗号化器はデータブロックの少なくとも１ビットを反転又は交換する装置であり、
上記第２の暗号解読器は相補的な論理演算を行う請求項２記載の方法。
【請求項５】
データストリームを入力する段階と、
第１の鍵信号を発生させる段階と、
上記第１の鍵信号を対称暗号化器に結合する段階と、
上記データストリームを上記対称暗号化器に結合する段階と、
上記データストリームを暗号化する段階と、
上記対称暗号化器を選択器に接続する段階と、
上記データストリームを上記選択器に結合する段階と、
第２の鍵信号を発生させる段階と、
上記第２の鍵信号を非対称暗号化器に結合する段階と、
上記データストリーム又は対称的に暗号化されたデータのどちらが上記非対称暗号化器に接続されるのかを選択する段階と、
上記選択されたデータを非対称的に暗号化する段階と、
非対称的に暗号化されたデータを原盤作成装置のデータ処理部に結合する段階と、
認証用署名信号を発生させる段階と、
対称的に暗号化されたデータが上記非対称暗号化器に接続されるコピー防止モードが選択されたとき、上記認証用署名信号をディスク原盤作成装置へ結合する段階と、
コピー防止モードが選択されたとき、上記認証用署名信号を原盤作成装置の半径方向アクチュエータへ供給する段階と、
を有する、光ディスクの原盤作成処理にコピー防止を設ける方法。
【請求項６】
上記光ディスクは光コンパクトディスクである請求項５記載の方法。
【請求項７】
上記光ディスクは、ＣＤ－ＲＯＭディスクである請求項５記載の方法。
【請求項８】
上記第１の鍵信号はランダムな鍵である請求項５記載の方法。
【請求項９】
上記第２の鍵信号は秘密鍵である請求項５記載の方法。
【請求項１０】
上記データストリームは暗号化されていない請求項５記載の方法。
【請求項１１】
再生装置において予め暗号化されたデータを含む予め記録された光ディスクの再生処理にコピー防止を設ける方法であって、
上記予め記録された光ディスクからの予め暗号化されたデータを与える段階と、
第１の鍵信号を発生させる段階と、
上記第１の鍵信号を非対称暗号解読器に結合する段階と、
第１の暗号解読されたデータストリームを生成するため、上記予め記録された光ディスクからのデータを非対称的に暗号解読する段階と、
鍵データベースから第２の鍵信号を検出する段階と、
第２の鍵信号を発生させる段階と、
上記第２の鍵信号を対称暗号解読器に結合する段階と、
上記第１の暗号解読されたデータストリームを上記対称暗号解読器に結合する段階と、
第２の暗号解読されたデータストリームを生成するため、上記第１の暗号解読されたデー

タストリームを対称的に暗号解読する段階と、
認証用信号を含むトラッキングサーボ信号を提供する段階と、
上記認証用信号の存在を検出する段階と、
上記認証用信号の検出に基づいてコピー防止信号を生成する段階と、
コピー防止信号が存在しないとき、上記第１の暗号解読されたデータストリームを選択する段階と、
上記コピー防止信号が存在するとき、上記第２の暗号解読されたデータストリームを選択する段階と、
選択されたデータを上記再生装置のデータ処理部に出力する段階と、
を有し、上記認証用信号が検出されたときのみ上記光ディスクから読み出されるデータが２回解読される方法。

【請求項１２】
上記予め記録された光ディスクは、ＣＤ－ＲＯＭディスクである請求項１１記載の方法。

【請求項１３】
上記予め記録された光ディスクはコンパクトオーディオディスクである請求項１１記載の方法。

【請求項１４】
光ディスク上に原盤レコーディングを行うコピー防止記録装置であって、
ディジタルデータストリームを受信する入力端子と、
対称暗号化器と、
上記対称暗号化器に結合される第１の鍵信号を供給する第１のランダム鍵発生器と、
上記ディジタルデータストリーム又は上記対称暗号化器の出力のどちらかを非対称暗号化器に供給するオペレータ制御形スイッチと、
上記非対称暗号化器に結合される第２の鍵信号を供給する第２の鍵発生器と、
を有し、
上記非対称暗号化器は原盤レコーディング装置のデータ処理部に接続され、
上記オペレータ制御形スイッチがオフ位置にあるとき、上記ディジタルデータストリームは上記非対称暗号化器によって非対称的に暗号化され、
原盤レコーディングがコピー防止処理を施されるべきであることを示す認証用署名信号を発生させる認証用署名発生器が更に設けられ、
上記認証用署名信号は、上記オペレータ制御形スイッチがオン位置にあるとき、上記原盤レコーディング装置の半径方向アクチュエータシステムに供給される、コピー防止記録装置。

【請求項１５】
上記光ディスクは、ＣＤ－ＲＯＭディスクである請求項１４記載のコピー防止記録装置。

【請求項１６】
上記光ディスクはコンパクトオーディオディスクである請求項１４記載のコピー防止記録装置。

【請求項１７】
上記認証用署名信号は、原盤に認証用署名を付与するため原盤作成中に、上記半径方向アクチュエータシステムの半径方向の位置を変調する請求項１４記載のコピー防止記録装置。

【請求項１８】
上記半径方向アクチュエータシステムの変調は、通常の速度と、上記通常の速度よりも僅かに大きい速度との間でランダムに変化するレートで、原盤作成されているディスクの中心から移動することにより構成される請求項１７記載のコピー防止記録装置。

【請求項１９】
光ディスク上にコピーが防止された題材を原盤レコーディングする装置であって、
ディジタルデータストリームを対称暗号化器に供給する手段と、
第１の鍵信号を発生させる手段と、

上記第１の鍵信号を使用して上記ディジタルデータストリームを対称的に暗号化する手段と、
データを非対称暗号化器に供給する手段と、
上記ディジタルデータストリームと対称的に暗号化されたデータの間で選択を行う手段と、
第２の鍵信号を発生させる手段と、
上記第２の鍵信号を用いて上記選択されたデータを非対称的に暗号化する手段と、
非対称的に暗号化されたデータを原盤レコーディング装置のデータ処理部に供給する手段と、
上記ディジタルデータストリームはコピーが防止されるべきことを示す認証用署名信号を発生させる手段と、
コピー防止モードと、コピーが防止されないモードとの間で選択を行う手段と、
上記認証用署名信号に応答して、上記光ディスク上で記録用ヘッドの半径方向の位置を変調する手段と、
を有する装置。
【請求項２０】
上記第１の鍵はランダムな鍵である請求項１９記載の装置。
【請求項２１】
上記第２の鍵は秘密鍵である請求項１９記載の装置。
【発明の詳細な説明】
背景
光コンパクトディスク（ＣＤ）は、一般的にディジタルデータの記憶用の優れた媒体であると認められている。その高い記憶密度、低い製造コスト及び取扱いの誤りに対する相対的な抵抗力は、他の媒体とは比較にならない。ハイファイオーディオの担体としてのＣＤの成功は、ＣＤ－ＲＯＭ、ＣＤ－Ｖｉｄｅｏ、ＣＤ－Ｉ等の多種の規格に準拠して、種々の目的のためディジタル化されたオーディオ、ビデオ及び英数字情報を記憶するより幅広い役割に技術が適合させられたマルチメディアの分野においても繰り返される可能性が高い。
従来、ＣＤ－ＲＯＭのソウトウェアの著作権者は、ビデオカセット及びオーディオカセットの媒体を危険に晒す過激な著作権侵害行為（無許可の複製）に対処する必要はなかった。その理由は、ＣＤの原盤製作及び複製には大きい資本投下が伴うことに略完全に起因するからであり、著作権侵害行為に対する実質的な財政上の障壁になる。しかし、予め記録されたＣＤから完全なデータのコピーを作成可能なプロのユーザ用のコンパクトディスク記録装置は約２０００ドルで入手可能であり、これから僅か数年の後には、消費者に手頃な価格の再生記録装置が広く入手可能になるであろう。これにより、利益を得るため自分の製品を＋５０ドルで販売することを要求するソフトウェア製作者と、まもなく１０ドル乃至２０ドルの範囲に収まるよう計画された無記入のディスクの値段で完全なコピーを作成する能力が得られる消費者との間には、厳しい衝突が生じる。この問題は、ビデオ事業を悩ます著作権侵害行為よりももっと厳しくなる可能性が高い。その理由は、映画を２回以上観ることを望む人は少ないのに対し、多数のマルチメディア製品は繰り返し使用されることが意図されているので、レンタルではなく所有の方が標準的になるからである。
本発明により解決される基本的な問題は、消費者が合法的に製作されたＣＤを再生することだけによりソフトウェア製作者の製品を楽しめることを保証することである。
著作権侵害行為に対する一つの解決策は、ディジタル・オーディオ・テープ（ＤＡＴ）の媒体のため開発されたシリアルコピーマネージメントシステム（ＳＣＭＳ）に類似した製作者間の一般協定によって指定された特殊なコピー防止回路をＣＤ記録装置に組み込むことである。この機構を用いて、ＣＤ記録装置は、ディジタルデータ内で特殊なコピー防止命令を探し、その命令の検出後、記録を中止する。しかし、このようなシステムは非常に限られた保護しか与えない。ＳＣＭＳシステムがＤＡＴ媒体に対し最初に提案されたときでさえ、このシステムはプロ、或いは、アマチュアの著作権侵害行為に対する保護を殆ど

与えないことが完全に認められた。プロ、或いは、アマチュアの著作権侵害者は、データフォーマットを知ることにより、コピー防止命令を除去するための低価格の“ブラックボックス”（電子回路）を構築可能であり、実際に構築して、記録装置によって無制限の複製をすることが可能である。

本出願人は、データストリームに挿入されたコピー防止命令に依存する全てのコピー防止システムが上記命令を探索するＣＤ記録装置内の回路と同じオーダーの複雑さ及びコストからなるブラックボックスによって破られることを確信している。従って、かかるシステムの有効性は限られている。ブラックボックスは、ＣＤ再生装置とＣＤ記録装置との間のラインに接続され、データストリーム内の特殊なコピー防止命令を探し、その命令を単に除去するか、或いは、変更する。従って、上記種類のコピー防止システムが採用されたならば、低価格のブラックボックスが急激に広まることを予期する必要がある。

コピー防止のための上記解決策の別の問題点は、全ＣＤ記録装置の製造者がその製品内に要求された検出回路を組み込まなければならないことである。製造者の中には、恐らく、自分の市場占有率の増大を期待して、その要求に応じないものが含まれる。たとえ僅かな割合であっても、市場にその要求に応じない装置が存在するならば、上記タイプのコピー防止機構の有効性は危うくなる。

上記の理由から、ソフトウェアの著作権所有者に高い保護のレベルを供与し、ブラックボックスに対する抵抗力があり、かつ、少数のハードウェア製造者が規格への準拠を拒否することにより危険に晒されることのないコンパクトディスク媒体用のコピー防止システムが求められる。

発明の概要

本発明によれば、条件付き再生システムは、種々の媒体、例えば、コンパクトディスク媒体上に予め記録された題材に著作権保護を与える。以下に説明される本発明は多数の異なる媒体に適用可能であり、かつ、当業者は本発明の教示を他の媒体に容易に適応することができるので、以下の説明は、コンパクトディスク媒体の応用だけに関して行う。

本発明は上記システムの欠点を解決する。条件付き再生システムによれば、ＣＤ記録装置が保護されたＣＤからデータを複写することは防止されない。その代わりに、上記システムの方法は、個々のＣＤが合法的なオリジナルであるか、又は、不正なコピーであるかをＣＤ再生装置によって判定することができる。合法的であるならば、再生装置はＣＤを正常に再生する。合法的でないならば、再生装置は停止し、適当な著作権警告メッセージを表示する。

原盤ディスクの製造中に、ＣＤ再生装置の通常の光学的ピックアップでは読むことができないが、他の手段により容易に検出可能な方法で、認証用署名がディスク上に刻まれる。この認証用署名には、原盤ディスクから作られた全ての製造ディスクに忠実に転写されるような性質がある。しかし、ＣＤ記録装置を用いて、製造ディスクの不正なコピーが作成されたならば、そのコピーはディスクのプログラムデータの忠実な複製を含むが、認証用署名はコピーに転写されない。かかるコピー保護規格に従う全てのＣＤ再生装置は、認証用署名を探すサブシステムを含む。署名が検出されなかったならば、ＣＤ再生装置はディスクの再生を行わない。

コンパクトディスクの応用の場合に、認証用署名は、好ましくは、原盤ディスクを作成する書き込みヘッドを、ヘッドの通常位置の周辺で数十ナノメートルのピーク・ツウ・ピークだけ半径方向に位置変調させることにより原盤ディスク上に刻まれる。この認証用署名は、以下に説明するように、ＣＤ再生装置の既存の半径方向トラッキングサーボシステムを利用することにより、最小限の複雑さの増加しか伴わないＣＤ再生装置に読み込まれる。

全てのＣＤ再生装置において、光学式読み取りヘッドは、再生装置の機能の通常部分として、巧妙な誤差検出システムによってトラック上に維持される。例えば、ヘッドがトラックの一方又は他方の側面の方に僅かに移動したとき、或いは、トラックが中心から逸れた軸に起因してヘッドの下側から動いたとき、誤差が検出、増幅され、トラックのヘッドを再度中心に置くため半径方向アクチュエータに供給される。光学式読み取りヘッドは、認

証用署名を定義する故意に誘起された位置変調を追尾する必要があるので、上記誤差電圧は、これに対応した信号成分を、楕円形の誤差等に対応した他の信号と共に含む。従って、この誤差電圧の適当な処理により、認証用署名が検出される。
位置変調信号は、整数個のサイクルがディスクの各回転中に加えられ、又は、１個の完全なサイクルがディスクの整数回の回転中に加えられるような単純な周波数のシヌソイドでもよい。いずれの場合でも、種々の他のトラッキング誤差信号からの認証用署名の取得は簡単化される。関係したタイプの異常な走査は、トラッキングを平均周波数の周辺でシヌソイド状のパスに曲げる通常のトラッキング信号のゆらぎを説明するモリモトによる米国特許第５，２４７，５０７号（参考のため引用）に記載されている。
明らかに、上記コピー防止システムは、認証用署名が記録装置に転送されないので、ＣＤ再生装置の信号出力と、ＣＤ記録装置の信号入力との間に接続されたブラックボックスによって危険に晒されることがない。
少数の製造者が認証用システムを自分のＣＤ再生装置に導入しないことを選んだとしても、海賊版ディスクの製造者は、自分の製品が市場の要求を満たさない限られたＣＤ再生装置セット上でしか再生できないというラベルを付けなければならないので、システムが危険に晒されることはない。海賊版ディスクの製造者は、実際上、自分の製品の不正を公表し、起訴を招くことになる。
以下、上記の条件付き再生システムの３通りの形式を説明する。３種類の全ての条件付き再生システムに共通の要素は、認証用署名が記録された“プログラム”信号の一部ではなく、無許可のコピー上には伝達されないような態様で合法的に製造されたＣＤ又は他の媒体に刻まれた上記の特殊な認証用署名を使用することである。
第１の条件付き再生システムは、当該特定の規格、例えば、ＣＤ－ＲＯＭに従う全てのＣＤ再生装置が、再生されるべき各個のＣＤ上で認証用署名を探すべきことを要求する。ＣＤ再生装置の制御システムは、認証用署名が見つからなかったならば、ＣＤの再生を停止するよう設計される。上記の如く、ＣＤの無許可のコピーは認証用署名を含まないので、かかるコピーは、実際上、役に立たない。従って、無許可のコピーがプログラム情報の完全な複製を含んでいても、有効なコピー防止が達成される。
上記の第１のシステムの欠点は、上記の特殊なＣＤ再生装置で再生されることを意図された全ての合法的なＣＤに認証用署名を付加しなければならない点である。従って、上記システムは、システムコントローラが全てのＣＤのコピー防止を指令できる閉じたシステムだけに対し適当である。しかし、商品化の観点からは、プログラム毎のコピー防止を提供、請求し得ることが望ましい。以下に説明する第２及び第３の条件付き再生システムはこの能力を有する。
第２の条件付き再生システムにおいて、コピーが防止されるべきＣＤは、全てのＣＤ再生装置に認証用署名を探索し、認証用署名の無いＣＤを再生しないよう通知する特殊な命令を含む。上記命令は、例えば、ＣＤの初期化区分、即ち、通常、プログラム以外の情報のため確保された部分に記録される。上記命令は、準拠した全てのＣＤ再生装置の特殊なサブシステムにより実行される。かくして、コピーが防止されたＣＤのオリジナルだけが再生され、無許可のコピーは拒絶される。この命令はコピー防止を必要としないプログラムのＣＤから削除され、かかるプログラムに対しオリジナルＣＤとそのコピーの両方は、正常に再生される。このようにして、コピー防止は、上記の“認証用署名の探索と、検出された場合に限り再生”命令の使用又は不使用により、１プログラム毎に与えられる。
しかし、上記第２の条件付き再生システムは、コピー防止の特徴を１プログラム毎に提供するが、このコピー防止は、原則として、ＣＤ再生装置とＣＤ記録装置との間の信号ラインに接続された特殊なブラックボックスにより危険に晒される可能性がある。上記ブラックボックスは、ＣＤ再生装置からのデータストリーム内で上記の“認証用署名の探索と、検出された場合に限り再生”命令を探索し、結果として得られた無許可のコピーがＣＤ再生装置における認証処理を起動させないように上記命令を削除又は変更する。
プログラマブル条件付き再生システム（ＰＣＰＳ）と称する第３の条件付き再生システムは、上記システムの問題点を解決し、１プログラム毎に活性化され、かつ、ブラックボッ

クスの攻撃に対し非常に抵抗力のあるコピー防止機構を提供する。
以下、上記の目標を達成するため、対称暗号化技術と非対称暗号化技術の組合せを使用するプログラマブル条件付き再生システムの一実施例を説明する。
【図面の簡単な説明】
図１は本発明の幾つかの要素を組み込む原盤作成処理ハードウェアのブロック図であり、図２は本発明の更なる要素を組み込むコンパクトディスク再生装置のブロック図である。
発明の詳細な説明
本発明は、コンパクトディスク媒体のような種々のプログラム配給媒体のコピーを防止する方法及び装置に関する。本発明は、あらゆるディスク媒体に適用可能であり、当業者は本発明の原理を磁気テープのような他の媒体に拡張することができる。本発明は、ソフトウェアの著作権所有者に高い保護レベルを与え、ブラックボックスに対する抵抗力があり、多少のハードウェア製造者がその規格に従うことを拒否することによって危険に晒されることはない。
上記の如く、著作権所有者に１プログラム毎のコピー防止を与え、対価として１プログラム当たりの料金、又は、１ディスク当たりの料金を受けることが望ましい。これは、ブラックボックスを用いて破るには、非常に困難、法外に高価、かつ、時間的な浪費の多い態様で、コピー防止処理され、又は、コピー防止処理されていないディスクをＣＤ再生装置によって取り扱えるように、対称及び非対称（公開鍵として知られている）のデータ暗号化の組合せを使用するプログラマブル条件付き再生システムにより達成される。
従来の暗号化方法の概説は、本発明をより完全に理解するため有用である。対称暗号化と称する最も一般的なデータ暗号化形式は、上記データの暗号化と暗号解読に同じ鍵を使用する。上記鍵を推測する試行錯誤の企てに対する保護のため、上記鍵は、好ましくは、時間的に変えられる非常に大きいランダムに発生させられた数である。例えば、上記鍵は、349,247,839,636,290,351,673のような数である。システムの保全を保証するため、この数（鍵）は通常秘密にされたままである。この鍵を秘密にしておく必要があることは、対称暗号化システムの重大な欠点である。一般的に使用されるＤＥＳアルゴリズムは、対称暗号化システムの一例であり、ＤＥＳアルゴリズムにおいて６４ビットのブロックに配置されたディジタル語は５６ビットの鍵を用いて暗号化される。５６個の２値のビットは、約１７個の１０進数と等価である。
非対称暗号化システムは、Ｐ及びＱのように称される２個の異なる鍵を使用する。一方の鍵Ｐは暗号化のため使用され、もう一方の鍵Ｑは暗号解読のため使用される。非対称システムの重要な利点は、暗号解読のため使用される鍵Ｑに関する知識は、メッセージを暗号化するために十分ではない点である。従来、非対称暗号化用の最も安全なアルゴリズムの一つは、ＲＳＡデータセキュリティ社により設計され、ライベスト（Rivest）他による米国特許第４，４０５，８２９号の技術を使用するアルゴリズム（ＲＳＡ）である。このシステムの安全性は、Ｑに関する知識からＰを演算することが計算的に困難であるという教示から生じる。この計算は、５００個以上の数字を含む非常に大きい数の因数分解に係わる。鍵Ｐ及びＱの数字が増加すると共に、因数分解処理に要する時間が増加する。実際上、鍵のサイズは、予測される計算能力の増加を適当に考慮して、製品の寿命の間に因数分解の可能性が許容可能なレベルに低下させるよう選択される。
ＰＣＰＳの第１の実施例は、図１に示されるようなディスク原盤作成装置の一部分と、図２に示されるようなＣＤ再生装置の別の部分とを包含する。
ＰＣＰＳディスク原盤作成装置は、通常のソースから“クリア”（暗号化されていない）ディジタルデータストリームを受けるコピー防止記録装置１０と、入力端子２１とを含み、入力端子２１は、対称暗号化器２２と、オペレータ制御形の２極のシングルスロー制御スイッチ２４の一方の極Ｓ１ａとに入力される。スイッチ２４を適当に設定することにより、オペレータは、ライン２１上に入力されたプログラムから製作されるＣＤにコピー防止処理を行うかどうかを制御する。対称暗号化器２２は、更に、鍵のソース３３からの第１の鍵信号であるライン２３上の鍵Ｋを受ける。
対称暗号化器２２の出力は、ライン２１上のクリアディジタルデータストリームの暗号化

されたバージョンである。以下、暗号化器２２により使用される暗号化アルゴリズムのタイプと、鍵Ｋの性質を説明する。本発明を理解するためには、暗号化器２２が鍵Ｋにより定められたある式に従ってライン２１上のクリアデータを変形することが分かれば十分である。対称暗号化器２２の出力端子は、スイッチＳ１ａの第２の入力に接続される。スイッチＳ１ａの出力は、公開鍵システムの一部分である非対称暗号化器２５の入力に接続される。

上記プログラマブル条件付き再生システムの安全性を保証するため、公開鍵対Ｐ、Ｑの鍵Ｐの暗号化は、厳密に秘密の状態に保護される必要がある。このため、鍵Ｐは、好ましくは、鍵のソース２７の揮発性メモリに記憶される。かかる揮発性メモリは、鍵Ｐを無許可で読み出そうとする試みによって上記メモリが消去され、システムが停止させられるような態様で、保護された物理的な筐体内にある。これを実現し得る物理的な安全システムは、従来技術において周知であり、ここで詳しく説明する必要はない。

非対称暗号化器２５からのライン２８上の非対称的に暗号化されたデータは、他の従来のディスク原盤作成装置のデータ入力部に接続される。

認証用署名発生器２９は、上記の性質及び目的を有する認証用署名３１を発生する。ライン３１は、コピー防止制御スイッチ２４の第２の極であるスイッチＳ１ｂの一方の入力に接続される。スイッチＳ１ｂのもう一方の端子は、信号が供給されず、通常接地される。オペレータ制御形スイッチＳ１ｂは、コピー保護モードが選択されたときに限り、認証用署名３１をライン３２を介して半径方向アクチュエータに接続する。

ＣＤ再生装置に収容された対応するコピー防止装置４０は図２に示されている。適当に復号化され、かつ、誤り訂正されたライン４１上のＣＤからのプログラムデータは、上記公開鍵Ｐ、Ｑの中の第２の鍵Ｑにより駆動される非対称暗号解読器４２に入力される。鍵Ｑは鍵のソース４３からライン４４に供給される。ライン４５上の非対称的に暗号解読されたデータは、スイッチ５５の入力と、対称暗号解読器４６の入力とに結合される。対称暗号解読器４６は、鍵のソース４９からライン４８上に供給された同じ鍵Ｋの制御下で、図１の対称暗号化器２２と全く逆の処理を行う。

ライン５６上の対称暗号解読器４６の出力は、スイッチ５５の第２の入力に結合される。ライン５４のスイッチ５５の出力は、ＣＤ再生装置の中の残りの通常のデータ処理部に結合される。鍵Ｑ及びＫは、ＣＤ再生装置内のある都合の良い読み出し専用メモリに永久に記憶され、特殊な安全対策は必要ではない。以下に説明するように、上記の鍵についての知識は、上記コピー防止機構を破ろうとする将来の著作権侵害行為に対し少しも役に立たない。

ＣＤ再生装置の半径方向トラッキングサーボ増幅器からの誤差信号は、認証用信号検出器５２にライン５１で入力される。上記の如く、この信号は認証用署名に対応する成分を有する信号である。検出器５２は、認証用署名が入力に存在するかどうかに対応する２値の出力をライン５３上に発生するよう設計される。例えば、この出力は、認証用署名が存在する場合には論理的な１であり、存在しない場合には論理的な０である。

認証用署名の無い場合にスイッチ５５が１回だけ暗号解読されたライン４７からの入力を選択し、認証用署名が検出された場合にスイッチ５５が２重に暗号解読されたライン５６からの入力を選択するよう、論理レベルは選定される。

異なる環境下での応答を調査することにより、プログラマブル条件付き再生システムの動作が評価される。

・オリジナルのコピー防止処理されたディスク又はコピー防止処理されていないディスクが再生されたとき、認証用署名の有無に依存して、スイッチＳは、１回だけ暗号解読されたデータ又は２重に暗号解読されたデータのいずれかを正確に選択する。従って、スイッチＳの出力は適切に暗号解読されたデータである。これにより、全てのオリジナルディスクは正常に再生される。

・コピー防止処理をされていないディスクのコピーが再生されたとき、認証用署名が無いので、スイッチＳは１回だけ暗号解読されたデータを正確に選択し、かかるディスクを正常に再生することができるようになる。

・しかし、コピー防止処理を施されたディスクの不正なコピーが再生されたとき、認証用署名が無い場合に、スイッチＳは１回だけ暗号解読されたデータを誤って選択する。ライン５４上の部分的に暗号解読されたデータは、ディスクが正常に再生されることを抑止する。ＰＣＰＳの安全性により、保護されたディスクの再生可能なコピーを著作権侵害行為によって作成することが不可能でなくても非常に困難、かつ、不経済になる。

コピー防止処理を施されたディスクの再生可能なコピーを作成するため、即ち、上記機構を打ち破るため、著作権侵害者は以下の行為の中の一つを行う必要がある。即ち、

１．全てのコピー防止処理を施されたディスク上に記録された２重に暗号化されたプログラムデータを、認証用署名が見つからない場合にＣＤ再生装置により要求される１回だけ暗号化されたフォーマットに変換する。このため、著作権侵害行為者は、ディスク原盤作成処理で使用された秘密鍵Ｐを取得する必要があるが、この秘密鍵Ｐは、上記の如く、ディスク原盤作成プラントにあり、密封され、ブービートラップを仕掛けられた装置内に厳密に保護される。著作権侵害行為者は、ＣＤ再生装置内で２重に暗号化されたオフディスクデータを容易に得ることができ、更に、ＣＤ再生装置内の鍵Ｋ及びＱと共に部分的に暗号解読され、及び、完全に暗号解読された（クリア）プログラムデータを容易に得ることができる。しかし、著作権侵害行為者が、要求された１回だけ暗号化されたプログラムデータを発生させるため必要とされる秘密鍵Ｐを推定するために十分な情報を依然として得ることができない点に非対称暗号化方法の本質がある。上記合成暗号化機構によれば、かくして、プログラムの選択的な保護が得られ、ブラックボックスの攻撃に対する抵抗力が得られる。

２．規格に準拠したＣＤ再生装置がディスクを正常に再生するように、ディスクが記録される際に実行可能な認証用署名を不正のコピーに付加する。これは実現可能ではあるが、それを行うためには、著作権侵害行為者は、位置変調されたトラックを半径方向に記録することができるようにＣＤ記録装置に重大な変更を行う必要がある。このような変更は、消費者及びソフトウェアディーラーの能力では及ばない。しかし、財政的に豊かな著作権侵害者の操作によりかかる変更を行う方法が見つけられないと主張することは現実的ではない。著作権侵害者による認証用署名の“偽造”をより困難にさせるための種々の方法があるが、それら全ての方法は、利用可能なＣＤ記録装置の（もしあれば）半径方向のサーボシステムの正確な能力に多少でも依存している。例えば、署名は、商業的に入手可能なＣＤ記録装置の半径方向のサーボが追尾できないように（単純なシヌソイドではなく）インパルス関数の形からなる。勿論、仮想的な著作権侵害者の財源が無制限であるならば、著作権侵害者はプロ用のディスク原盤作成システムに投資し、必要な変更を行うことが可能である。

しかし、実際上の問題として、消費者、ディーラー、及び、技術的に精通しているプロのレベルの著作権侵害行為を排除する上記システム及び方法の能力は、非常に価値があるに違いない。

ＲＳＡデータセキュリティ社から入手可能な公開鍵アルゴリズム（ＲＳＡ）が上記応用の対称暗号化及び暗号解読のため使用されるならば、安全性を危険に晒すことなく、非常に単純な対称暗号化及び暗号解読アルゴリズムを使用することが可能になる。特に、この“アルゴリズム”は、簡単にデータブロックの任意の１ビットを反転させ、或いは、任意の２ビットを交換することができる。従来より理解されているような正式の鍵制御形暗号化及び暗号解読システムは、単純な相補的な論理演算のため回避される。従って、原盤作成処理及びＣＤ再生装置において使用されるような鍵Ｋは不要になる。

本発明を実施する制限の更なる簡単化は、データストリーム全体ではなく、プログラムデータの小さい部分集合に関して種々の暗号化及び暗号解読処理を行うことにより実現可能になる。これは、非対称暗号解読サブシステムが動作しなければならない１秒当たりのビット数のレートを低下させ、これにより、低価格のプロセッサの使用が可能になるので有利である。

ディスクを認証する他の同等に効果的な方法は、少なくとも１個の特定のデータブロックを、原盤処理が施されたディスクの中心からの特定の半径方向の距離と結合させることで

ある。
原盤ディスクがカッティングされているとき、書き込みヘッドは、通常の速度と、通常の速度よりも少し大きい速度との間でランダムに変化するレートで中心から移動可能である。ヘッドの開始位置は、正常な開始位置からランダムな距離で変位させてもよい。特定のデータブロックのディスク中心からの距離、及び、特定のデータブロックの相互の距離は、上記のランダムな変数の関数でもよい。上記ランダムな変数の値は、プログラムとプログラムの間で変化するように設けられる。
少なくとも１個のデータブロックのディスク中心からの距離は、非対称暗号化システムの秘密鍵の下で暗号化され、暗号化されたデータは、システムデータの一部としてディスクに記録される。ＣＤ記録装置がかかるディスクのコピーを作成するとき、上記データブロックのコピー上のＣＤ中心からの距離は、オリジナルディスク上の距離とは相違する。その理由は、商業的に入手可能なＣＤ記録装置の書き込みヘッドは一定速度で半径方向に駆動されるからである。
対応する各ＣＤ再生装置には、ディスク中心からの読み取りヘッドの距離が再生装置内のディジタル語として得られるように、較正された半径方向のサーボシステムが設けられる。ＣＤが再生されたとき、暗号化された半径方向の距離データは、ＣＤ再生装置のメモリに記憶された鍵の対Ｐ、Ｑの中の公開鍵Ｑを用いて暗号解読される。上記の暗号解読されたデータは、ランダムアクセスメモリに一時的に記憶される。
ＣＤが再生され続けると共に、上記のデータブロックの実際の距離は、要求された距離の暗号解読された値と比較される。許容誤差に起因する差よりも大きいと考えられる計算された距離の差は、不正のコピーであるＣＤに起因していると想定される。次いで、ＣＤ再生装置は、再生を停止し、場合によっては著作権のメッセージを表示する。
ディスクの認証の標識として、特定のデータブロックのディスク中心からの距離及び特定のデータブロック間の距離を用いる代わりに、他の実施例は、種々のデータブロックの場所における読み取りヘッドの半径方向の速度の測定量を使用する。この解決策は、正確に知る必要のある読み取りヘッドとディスク中心との間の距離を要求しない点で有利である。その代わりとして、上記解決策は、トラッキング制御システムから容易に得られる種々の場所におけるヘッドの半径方向の速度の相対的な測定量に依存する。
上記の実施例は、コンパクトディスクフォーマット用のプログラマブル条件付き再生システムを記述しているが、その原理は磁気テープフォーマットにも適用可能である。かかる応用に対し、認証用署名３２はテープの制御トラックに付加される。
上記の如く、好ましい実施例と組み合わせて本発明の説明を行ったが、本発明の精神を逸脱することなく種々の変形が行えることが当業者により認められるであろう。本出願人により意図された範囲は、請求項の記載及びその等価物により明確にされる。

【図１】

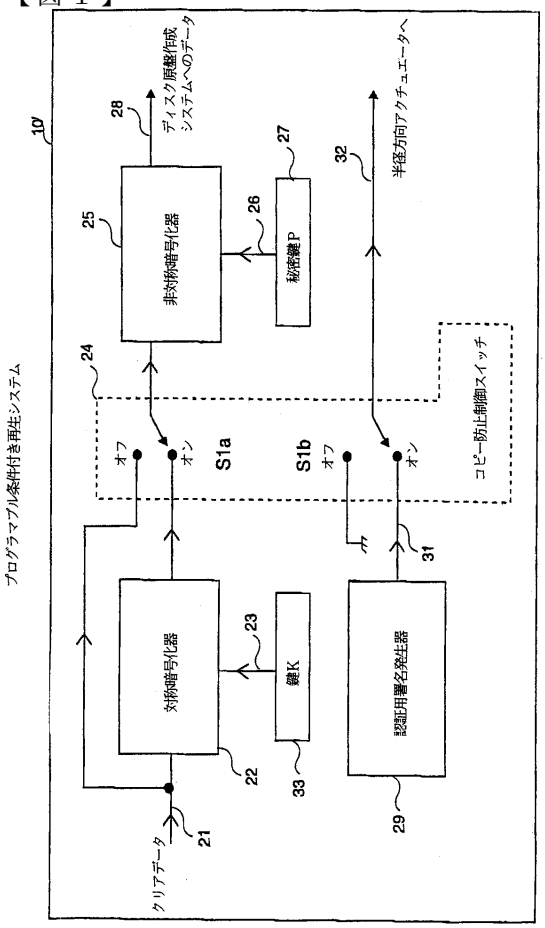

FIGURE 1
ディスク原盤作成装置
プログラマブル条件付き再生システム

【図２】

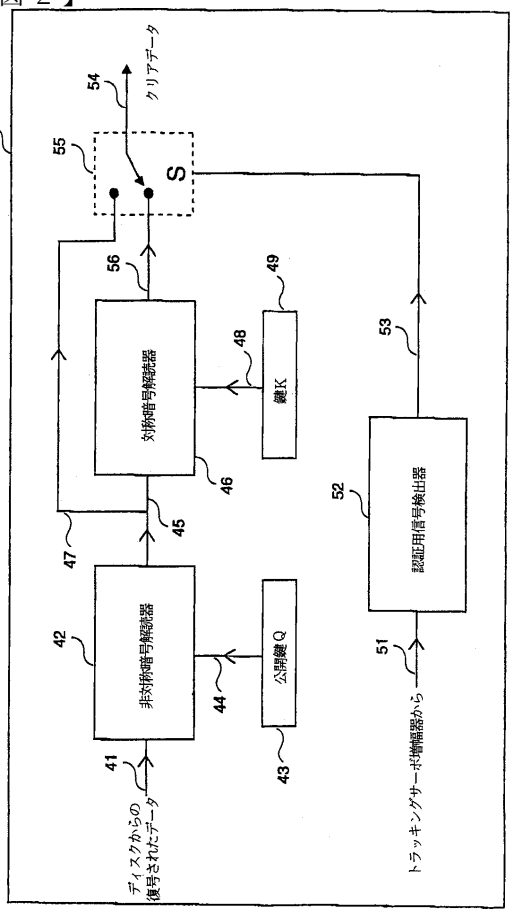

FIGURE 2
CD再生装置

フロントページの続き

合議体
審判長　山田　洋一
審判官　中野　浩昌
審判官　早川　卓哉

(56)参考文献　特開平５－２５７８１６（ＪＰ，Ａ）
特開平２－２９３９３０（ＪＰ，Ａ）
特開昭６３－１３２３３６（ＪＰ，Ａ）
特開平１－１８２９７１（ＪＰ，Ａ）
特開平６－９７９３１（ＪＰ，Ａ）
特開平６－６９９１５（ＪＰ，Ａ）
特開平３－１０２５９２（ＪＰ，Ａ）
特開平３－４０６８９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G11B20/10
H04L 9/00