(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-522245
(P2004-522245A)
(43)公表日　平成16年7月22日(2004.7.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11B 20/10	G11B 20/10	H	5D029
G11B 7/007	G11B 7/007		5D044
G11B 7/24	G11B 7/24	538P	5D090
G11B 20/12	G11B 20/12		

審査請求 未請求　予備審査請求 有　（全 66 頁）

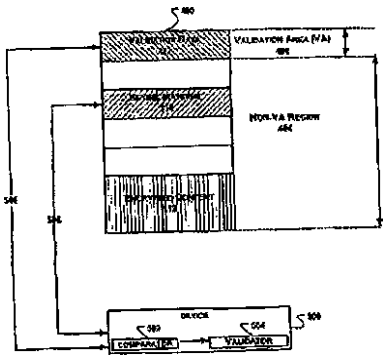
(21)出願番号　特願2002-578501(P2002-578501)
(86)(22)出願日　平成14年3月22日(2002.3.22)
(85)翻訳文提出日　平成15年9月30日(2003.9.30)
(86)国際出願番号　PCT/US2002/008971
(87)国際公開番号　WO2002/080171
(87)国際公開日　平成14年10月10日(2002.10.10)
(31)優先権主張番号　09/822,542
(32)優先日　平成13年3月30日(2001.3.30)
(33)優先権主張国　米国(US)

(71)出願人　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５２　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　100064621
弁理士　山川　政樹
(72)発明者　トロウ，ブレンデン
アメリカ合衆国・９７２２９・オレゴン州・ポートランド・ノースウエスト　スプリーム　コート・１０８５９
(72)発明者　リプリー，マイク
アメリカ合衆国・９７１２４・オレゴン州・ヒルズボロ・ノースイースト　５６ティエイチ　コート・１２２２

最終頁に続く

(54)【発明の名称】メディアに保管されたコンテンツの無許可コピーの再生を防ぐ、読取専用メディアのバリデーション・エリアを使用することによるキーイング・マテリアルの検証

(57)【要約】
本発明の一態様は、メディアのバリデーション・エリア（ＶＡ）（４０６）領域を使用してキーイング・マテリアルを検証することによって、ＤＶＤなどのメディアの無許可コピーをコンプライアント・デバイス（５００）によって再生できなくする方法である。コンプライアント・デバイスは、キーイング・マテリアルを検証する（１１４）デバイスである。本発明の一実施形態では、コンプライアント・デバイスが、メディアのＶＡ領域内の値を使用することによって、キーイング・マテリアルを検証する。代替実施形態では、コンプライアント・デバイスが、メディアの非ＶＡ領域（４０４）に書き込まれたキーイング・マテリアルと、メディアのＶＡ領域に書き込まれたバリデーション・データ（４０２）の間の対応を検査することによって、キーイング・マテリアルを検証する。代替実施形態では、キーイング・マテリアルがバリデーション・データと対応しない場合に、コンプライアント・デバイスが、メディアのコンテンツを再生できなくする。



【特許請求の範囲】
【請求項１】
暗号化されたコンテンツを有するメディアのバリデーション・エリア（ＶＡ）領域からバリデーション・データを読み取ること、
バリデーション・データからキーイング・マテリアルを導出することによって、暗号化されたコンテンツの解読に使用されるキーイング・マテリアルを判定すること、
暗号化されたコンテンツを解読するのにキーイング・マテリアルを使用することと
を含む方法。
【請求項２】
バリデーション・データがキーイング・マテリアルを含む場合に、バリデーション・データ自体を使用することによって、キーイング・マテリアルがバリデーション・データから導出される請求項１に記載の方法。
【請求項３】
バリデーション・データが、メディアの非ＶＡ領域に書き込まれたキーイング・マテリアルのコピーである場合に、バリデーション自体を使用することによって、キーイング・マテリアルがバリデーション・データから導出される請求項１に記載の方法。
【請求項４】
メディアが、コンテンツを保護するのにＣＰＰＭ（コンテンツ・プロテクション・フォー・プリレコーデッド・メディア）フォーマットを使用し、
キーイング・マテリアルが、メディアの非ＶＡ領域に書き込まれたアルバム・アイデンティファイヤを含み、
バリデーション・データが、アルバム・アイデンティファイヤのコピーを含む
請求項３に記載の方法。
【請求項５】
ＶＡ領域内のバリデーション・データを非ＶＡ領域内のキーイング・マテリアルに変換することによって、キーイング・マテリアルが、バリデーション・データから導出される請求項１に記載の方法。
【請求項６】
キーイング・マテリアルへのバリデーション・データの変換が、バリデーション・データをキーイング・マテリアルに変換する関数を使用することを含み、逆関数が、キーイング・マテリアルからバリデーション・データを作成するのに使用された請求項５に記載の方法。
【請求項７】
メディアが、コンテンツを保護するのにＣＳＳ（コンテンツ・スクランブル・システム）フォーマットを使用し、
キーイング・マテリアルが、メディアの非ＶＡ領域に書き込まれたセキュア・ディスク・キー・データを含み、
バリデーション・データが、セキュア・ディスク・キー・データに対する暗号関数を含む
請求項６に記載の方法。
【請求項８】
暗号化されたコンテンツの解読が、暗号化されたコンテンツを解読する暗号鍵を形成するのにキーイング・マテリアルを使用することを含む請求項６に記載の方法。
【請求項９】
メディアがディジタル多用途ディスク（ＤＶＤ）を含み、ＶＡがＤＶＤのバースト・カッティング・エリアを含む請求項６に記載の方法。
【請求項１０】
メディアのバリデーション・エリア（ＶＡ）領域内にバリデーション・データが存在するかどうかを判定することによって、暗号化されたコンテンツを有するメディアがバリデーテッド・メディアであるかどうかを判定すること、
メディアがバリデーテッド・メディアである場合に、バリデーション・エリアからキーイ

ング・マテリアルを導出することによって、暗号化されたコンテンツを解読するのに使用されるキーイング・マテリアルを判定すること、
キーイング・マテリアルを検証することと
を含む方法。
【請求項１１】
ＶＡ領域内にバリデーション・データが存在するかどうかの前記判定が、トリガがセットされているかどうかの判定を含む請求項１０に記載の方法。
【請求項１２】
トリガがセットされているかどうかの前記判定が、キーイング・マテリアルの最上位ビットに１がセットされているかどうかを判定することである請求項１１に記載の方法。
【請求項１３】
バリデーション・データがキーイング・マテリアルを含む場合に、バリデーション・データ自体を使用することによって、キーイング・マテリアルがバリデーション・データから導出される請求項１０に記載の方法。
【請求項１４】
バリデーション・データが、メディアの非ＶＡ領域に書き込まれたキーイング・マテリアルのコピーである場合に、バリデーション自体を使用することによって、キーイング・マテリアルがバリデーション・データから導出される請求項１０に記載の方法。
【請求項１５】
ＶＡ領域内のバリデーション・データを非ＶＡ領域内のキーイング・マテリアルに変換することによって、キーイング・マテリアルがバリデーション・データから導出される請求項１０に記載の方法。
【請求項１６】
メディアがディジタル多用途ディスク（ＤＶＤ）を含み、ＶＡがＤＶＤのバースト・カッティング・エリアを含む請求項１０に記載の方法。
【請求項１７】
バリデーション・データがメディアのバリデーション・エリア（ＶＡ）領域に存在するかどうかを判定することによって、暗号化されたコンテンツを有するメディアがバリデーテッド・メディアであるかどうかを判定することであって、メディアが、さらに、メディアの非ＶＡ領域に書き込まれたキーイング・マテリアルを有する、判定すること、
メディアが、バリデーテッド・メディアである場合に、バリデーション・データとキーイング・マテリアルとが対応するかどうかを判定すること、
バリデーション・データとキーイング・マテリアルとが対応する場合に、暗号化されたコンテンツを解読するのに非ＶＡ領域内のキーイング・マテリアルを使用することと
を含む方法。
【請求項１８】
メディアがバリデーテッド・メディアであるかどうかの前記判定が、トリガがセットされているかどうかを判定することを含む請求項１７に記載の方法。
【請求項１９】
トリガがセットされているかどうかの前記判定が、キーイング・マテリアルの最上位ビットに１がセットされているかどうかを判定することである請求項１８に記載の方法。
【請求項２０】
メディアが、ＤＶＤ－ＲＯＭ（ディジタル・ビデオ・ディスク読取専用メモリ）を含む請求項１７に記載の方法。
【請求項２１】
バリデーション・データとキーイング・マテリアルとが対応するかどうかの前記判定が、バリデーション・データとキーイング・マテリアルとが一致するかどうかを判定することを含む請求項１７に記載の方法。
【請求項２２】
メディアが、コンテンツを保護するのにＣＰＰＭ（コンテンツ・プロテクション・フォー

・プリレコーデッド・メディア）フォーマットを使用し、
キーイング・マテリアルがメディアの非ＶＡ領域に書き込まれたアルバム・アイデンティファイヤを含み、
バリデーション・データがアルバム・アイデンティファイヤのコピーを含む
請求項２１に記載の方法。
【請求項２３】
バリデーション・データとキーイング・マテリアルとが対応するかどうかの前記判定が、キーイング・マテリアルに対する暗号関数がバリデーション・データと一致するかどうかを判定することを含む請求項１７に記載の方法。
【請求項２４】
メディアが、コンテンツを保護するのにＣＳＳ（コンテンツ・スクランブル・システム）フォーマットを使用し、
キーイング・マテリアルが、メディアの非ＶＡ領域に書き込まれたセキュア・ディスク・キー・データを含み、
バリデーション・データが、セキュア・ディスク・キー・データに対する暗号関数を含む
請求項２３に記載の方法。
【請求項２５】
メディアが、ＤＶＤ（ディジタル多用途ディスク）を含み、ＶＡがＤＶＤのバースト・カッティング・エリアを含む請求項１７に記載の方法。
【請求項２６】
バリデーション・データがメディアのバリデーション・エリア（ＶＡ）領域に存在するかどうかを判定することによって、暗号化されたコンテンツを有するメディアがバリデーテッド・メディアであるかどうかを判定すること、
メディアがバリデーテッド・メディアである場合に、
バリデーション・データからキーイング・マテリアルを導出することによって、暗号化されたコンテンツの解読に使用されるキーイング・マテリアルを判定し、その後にキーイング・マテリアルを検証すること、
バリデーション・データとキーイング・マテリアルとが対応するかどうかを判定し、バリデーション・データがキーイング・マテリアルに対応する場合に、キーイング・マテリアルを検証することと
の１つを実行することと
を含む方法。
【請求項２７】
バリデーション・データがキーイング・マテリアルを含む場合に、バリデーション・データ自体を使用することによって、キーイング・マテリアルがバリデーション・データから導出される請求項２６に記載の方法。
【請求項２８】
バリデーション・データが、メディアの非ＶＡ領域に書き込まれたキーイング・マテリアルのコピーである場合に、バリデーション自体を使用することによって、キーイング・マテリアルが、バリデーション・データから導出される請求項２６に記載の方法。
【請求項２９】
ＶＡ領域内のバリデーション・データを非ＶＡ領域内のキーイング・データに変換することによって、キーイング・マテリアルがバリデーション・データから導出される請求項２６に記載の方法。
【請求項３０】
メディアが、ＤＶＤ－ＲＯＭ（ディジタル・ビデオ・ディスク読取専用メモリ）を含む請求項２６に記載の方法。
【請求項３１】
ＶＡが、ＤＶＤのバースト・カッティング・エリアを含む請求項２６に記載の方法。
【請求項３２】

命令のシーケンスを表すデータを保管した機械可読メディアであって、命令のシーケンスが、プロセッサによって実行される時に、プロセッサに、
バリデーション・データがメディアのバリデーション・エリア（ＶＡ）領域に存在するかどうかを判定することによって、暗号化されたコンテンツを有するメディアがバリデーテッド・メディアであるかどうかを判定すること、
メディアがバリデーテッド・メディアである場合に、
バリデーション・データからキーイング・マテリアルを導出することによって、暗号化されたコンテンツの解読に使用されるキーイング・マテリアルを判定し、その後にキーイング・マテリアルを検証すること、
バリデーション・データとキーイング・マテリアルとが対応するかどうかを判定し、バリデーション・データがキーイング・マテリアルに対応する場合に、キーイング・マテリアルを検証することと
の１つを実行することと
を実行させる機械可読メディア。
【請求項３３】
暗号化されたコンテンツが、ＣＰＰＭ（コンテンツ・プロテクション・フォー・プリレコーデッド・メディア）フォーマットを使用して保護され、キーイング・マテリアルが、アルバム・アイデンティファイヤを含み、バリデーション・データが、アルバム・アイデンティファイヤのコピーを含む請求項３２に記載の機械可読メディア。
【請求項３４】
コンテンツが、ＣＳＳ（コンテンツ・スクランブル・システム）によって保護され、
キーイング・マテリアルがセキュア・ディスク・キー・データを含み、
バリデーション・データがセキュア・ディスク・キー・データに対する関数を含む
請求項３２に記載の機械可読メディア。
【請求項３５】
少なくとも１つのプロセッサと、
命令をその上にエンコードされた機械可読メディアと
を含み、前記命令が、プロセッサによって実行される時に、プロセッサに、
バリデーション・データがメディアのバリデーション・エリア（ＶＡ）領域に存在するかどうかを判定することによって、暗号化されたコンテンツを有するメディアがバリデーテッド・メディアであるかどうかを判定し、
メディアがバリデーテッド・メディアである場合に、
バリデーション・データからキーイング・マテリアルを導出することによって、暗号化されたコンテンツの解読に使用されるキーイング・マテリアルを判定し、その後にキーイング・マテリアルを検証すること、
バリデーション・データとキーイング・マテリアルとが対応するかどうかを判定し、バリデーション・データがキーイング・マテリアルに対応する場合に、キーイング・マテリアルを検証することと
の１つを実行するように指示する装置。
【請求項３６】
暗号化されたコンテンツが、ＣＰＰＭ（コンテンツ・プロテクション・フォー・プリレコーデッド・メディア）フォーマットを使用して保護され、キーイング・マテリアルが、アルバム・アイデンティファイヤを含み、バリデーション・データがアルバム・アイデンティファイヤのコピーを含む請求項３５に記載の装置。
【請求項３７】
コンテンツが、ＣＳＳ（コンテンツ・スクランブル・システム）によって保護され、
キーイング・マテリアルが、セキュア・ディスク・キー・データを含み、
バリデーション・データが、セキュア・ディスク・キー・データに対する関数を含む
請求項３５に記載の装置。
【請求項３８】

バリデーション・データがメディアのバリデーション・エリア（ＶＡ）領域に存在するかどうかを判定することによって、暗号化されたコンテンツを有するメディアがバリデーテッド・メディアであるかどうかを判定する手段と、
メディアがバリデーテッド・メディアである場合に、
バリデーション・データからキーイング・マテリアルを導出することによって、暗号化されたコンテンツの解読に使用されるキーイング・マテリアルを判定し、その後にキーイング・マテリアルを検証すること、
バリデーション・データとキーイング・マテリアルとが対応するかどうかを判定し、バリデーション・データがキーイング・マテリアルに対応する場合に、キーイング・マテリアルを検証することと
の１つを実行する手段と
を含む装置。
【請求項３９】
暗号化されたコンテンツが、ＣＰＰＭ（コンテンツ・プロテクション・フォー・プリレコーデッド・メディア）フォーマットを使用して保護され、キーイング・マテリアルが、アルバム・アイデンティファイヤを含み、バリデーション・データが、アルバム・アイデンティファイヤのコピーを含む請求項３８に記載の装置。
【請求項４０】
コンテンツが、ＣＳＳ（コンテンツ・スクランブル・システム）によって保護され、
キーイング・マテリアルがセキュア・ディスク・キー・データを含み、
バリデーション・データがセキュア・ディスク・キー・データに対する関数を含む
請求項３８に記載の装置。
【請求項４１】
暗号化されたコンテンツと、
キーイング・マテリアルと、
メディアのバリデーション・エリア（ＶＡ）領域に書き込まれたバリデーション・データであって、キーイング・マテリアルの真正性を検証するのに使用される、バリデーション・データと
を含む装置。
【請求項４２】
暗号化されたコンテンツが、コンテンツ・プロテクション・フォー・プリレコーデッド・メディア（ＣＰＰＭ）フォーマットを使用し、バリデーション・データが、コンテンツの解読の暗号鍵を形成するのに使用されるアルバム・アイデンティファイヤを含む請求項４１に記載の装置。
【請求項４３】
キーイング・マテリアルが、メディアの非ＶＡ領域に書き込まれる請求項４１に記載の装置。
【請求項４４】
装置が、ＤＶＤ－ＲＯＭ（ディジタル・ビデオ・ディスク読取専用メモリ）を含む請求項４１に記載の装置。
【請求項４５】
ＶＡが、バースト・カッティング・エリアを含む請求項４１に記載の方法。
【請求項４６】
バリデーション・データがメディアのバリデーション・エリア（ＶＡ）領域に存在するかどうかを判定する第１モジュールであって、メディアが、メディアの暗号化されたコンテンツを解読するキー・マテリアルを有し、バリデーション・データが、キーイング・マテリアルの真正性を検証するのに使用される、第１モジュールと、
第２モジュールであって、バリデーション・データがＶＡ領域に存在する場合に、
暗号化されたコンテンツを解読するのに、メディアのＶＡ領域から導出されたキーイング・マテリアルを使用すること、

バリデーション・データとキーイング・マテリアルとの間の対応を見つけ、対応が見つかる場合に、暗号化されたコンテンツを解読するのにキーイング・マテリアルを使用することと
の１つを実行することによって、メディアを処理する第２モジュールと
を含む装置。
【請求項４７】
第１モジュールが、トリガがセットされているかどうかを判定することによって、バリデーション・データがメディアのＶＡ領域に存在するかどうかを判定する請求項４６に記載の装置。
【請求項４８】
キーイング・マテリアルの最上位ビットに１がセットされている場合に、トリガがセットされている請求項４７に記載の装置。
【請求項４９】
キーイング・マテリアルがバリデーション・データと一致する場合に、バリデーション・データがキーイング・マテリアルに対応する請求項４６に記載の装置。
【請求項５０】
暗号化されたコンテンツと、
キーイング・マテリアルと、
メディアのＶＡ領域に書き込まれたバリデーション・データと
を有するメディアと、
暗号化されたコンテンツを解読するのに、メディアのＶＡ領域から導出されたキーイング・マテリアルを使用すること、
バリデーション・データがキーイング・マテリアルに対応するかどうかを判定すること、
バリデーション・データがキーイング・マテリアルに対応する場合に、暗号化されたコンテンツを解読するのにキーイング・マテリアルを使用することと
の１つを実行することによって、暗号化されたコンテンツを再生するためにメディアに結合されたデバイスと
を含むシステム。
【請求項５１】
コンテンツが、ＣＰＰＭ（コンテンツ・プロテクション・フォー・プリレコーデッド・メディア）によって保護され、キーイング・マテリアルが、コンテンツの解読の暗号鍵を形成するのに使用されるアルバム・アイデンティファイヤを有する請求項５０に記載のシステム。
【請求項５２】
コンテンツが、ＣＳＳ（コンテンツ・スクランブル・システム）によって保護され、
キーイング・マテリアルが、セキュア・ディスク・キー・データを含み、
バリデーション・データが、セキュア・ディスク・キー・データに対する関数を含む
請求項５０に記載のシステム。
【請求項５３】
暗号化されたコンテンツと、
キーイング・マテリアルと
を含むメディアと、
メディアがバリデーテッド・メディアであり、キーイング・マテリアルの真正性が検証される場合に暗号化されたコンテンツを解読するためにメディアに結合されたデバイスと
を含むシステム。
【請求項５４】
キーイング・マテリアルの真正性が、
メディアのＶＡ領域から導出されたキーイング・マテリアルを使用すること、
バリデーション・データがキーイング・マテリアルに対応することを判定することと
の１つによって検証される請求項５３に記載のシステム。

【請求項５５】
キーイング・マテリアルがバリデーション・データと一致する場合に、バリデーション・データがキーイング・マテリアルに対応する請求項５４に記載のシステム。
【請求項５６】
キーイング・マテリアルの関数がバリデーション・データと一致する場合に、バリデーション・データがキーイング・マテリアルに対応する請求項５４に記載のシステム。
【請求項５７】
メディアが、ディジタル・ビデオ・ディスク読取専用メモリ（ＤＶＤ－ＲＯＭ）を含む請求項５３に記載のシステム。
【請求項５８】
ＶＡがバースト・カッティング・エリアを含む請求項５３に記載の方法。
【請求項５９】
バリデーション・データがＶＡ領域に存在するかどうかの前記判定がトリガがセットされているかどうかを判定することを含む請求項５３に記載のシステム。
【請求項６０】
トリガがセットされているかどうかの前記判定が、キーイング・マテリアルの最上位ビットに１がセットされているかどうかを判定することである請求項５９に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
著作権表示
この特許文書の開示の一部に、著作権保護の対象になる材料が含まれる。著作権所有者は、特許商標局の特許のファイルまたは記録に現れる特許文書または特許開示の何人による複製にも異議はないが、それ以外では全権を留保する。
【０００２】
本発明は、静的および動的な情報の保管および検索に関する。具体的には、本発明は、保管された情報の無許可のコピーからの保護の方法、装置、およびシステムに関する。
【背景技術】
【０００３】
情報またはコンテンツは、様々なメディアに保管することができる。保管された情報へのアクセスおよびコピーの速度および便利さが高まるにつれて、情報の無許可のコピーの脅威がそれに対応して高まってきた。様々なタイプのデータをメディアの異なる領域に保管することによって、読取専用メディアに保管されたコンテンツを無許可のアクセスから保護する様々な方式が使用されてきた。
【０００４】
そのような方式の１つが、図１Ａに示されているように、ＤＶＤ－ＲＯＭ（ディジタル多用途ディスク読取専用メディア）などのメディアで示すことができる。メディア１００に、データ・エリア１０２およびリードイン・エリア１０４（以下では非データ・エリア１０４と呼称する）が含まれる。図１Ｂにさらに示されているように、データ・エリア１０２に、暗号化されたコンテンツ１１２（または、コンテンツ・スクランブル・システム（Ｃｏｎｔｅｎｔ　Ｓｃｒａｍｂｌｅ　Ｓｙｓｔｅｍ、ＣＳＳ）によって保護されたＤＶＤ－Ｖｉｄｅｏコンテンツの場合にはスクランブルされたコンテンツ）が含まれる。
【０００５】
たとえばＣＰＰＭによって保護されるＤＶＤ－Ａｕｄｉｏコンテンツを含むＤＶＤ－ＲＯＭディスクでは、コントロール・データ・エリア（Ｃｏｎｔｒｏｌ　Ｄａｔａ　Ａｒｅａ）１１０（ＣＤＡ　１１０）に、アルバム・アイデンティファイヤ（Ａｌｂｕｍ　Ｉｄｅｎｔｉｆｉｅｒ）と称するキーイング・マテリアル（Ｋｅｙｉｎｇ　Ｍａｔｅｒｉａｌ）１１４（および／またはおそらくは、コンテンツ・スクランブル・システムによって保護されるＤＶＤ－Ｖｉｄｅｏコンテンツの場合にセキュア・ディスク・キー・データ（Ｓｅｃｕｒｅ　Ｄｉｓｋ　Ｋｅｙ　Ｄａｔａ））が保管される。アルバム・アイデンティファ

イヤは、保護されるアルバムのそれぞれにランダムに個別に割り当てられる８バイト（６４ビット）値である。メディアのデータ・エリア１０２に保管された暗号化されたコンテンツ１１２を解読するのに必要な暗号鍵は、アルバム・アイデンティファイヤの値に依存する。したがって、たとえば、アルバム・アイデンティファイヤが、記録可能メディアに不正にコピーされる場合に、不正なアルバムＩＤによって、プレイヤが、不正な暗号鍵を形成し、したがって、記録可能メディアがコンプライアントな形で再生されなくなる。

【０００６】

そのようなコンテンツ保護が有効であるためには、キーイング・マテリアル１１４（たとえば、ＤＶＤ－ＲＯＭの場合に、コントロール・データ・エリア１１０、セクタ＃２またはＣＤＡ１１０、セクタ＃２に保管されるアルバム・アイデンティファイヤ）を含むセクタが書き込まれないようにし、キーイング・マテリアル１１４をコピーできなくするように、記録可能メディアを設計することが理想的である。しかし、図１Ａおよび１Ｂに示されたＤＶＤ－ＲＯＭレイアウトに似たセクタ／レイアウトを有するＤＶＤ－Ｒ（ディジタル・ビデオ・ディスク－記録可能）およびＤＶＤ－ＲＷ（ディジタル・ビデオ・ディスク－書換可能）などの記録可能メディアのいくつかの形は、データ・エリア１０２にキーイング・マテリアル１１４を記録できるようにし、キーイング・マテリアル１１４を含むセクタのアドレスを割り当てられるようにし、プレイヤがそれを合法的なキーイング・マテリアル１１４と区別できなくなるように、書き込み可能なセクタ・アドレスを有する場合がある。もちろん、他のメディア（非コンプライアントＤＶＤ－ＲおよびＤＶＤ－ＲＷ）によって、直接に書き込み可能なキーイング・マテリアル１１４を含むセクタをも利用可能である。

【発明を実施するための最良の形態】

【０００７】

本発明を、制限ではなく例として添付図面に示すが、これらの図面では、類似する符号によって、類似する要素を参照する。

【０００８】

本発明の一態様では、メディアのバリデーション・エリア（ＶＡ）領域を使用してキーイング・マテリアルの真正性を検証して、読取専用メディアに事前記録されたコンテンツの無許可のコピーの再生を防ぐ、ＤＶＤ－ＲＯＭなどの読取専用メディアに保管されたキーイング・マテリアルを検証する方法を開示する。

【０００９】

キーイング・マテリアルならびにキーイング・マテリアルの真正性を検証するのに使用されるバリデーション・データは読取専用メディアに保管される。一実施形態で、バリデーテッド・メディア（すなわち、これから説明する、キーイング・マテリアルを検証するバリデーション・エリアを含み、それを使用するメディア）は、メディアのバリデーション・エリアに直接に書き込むことができるキーイング・マテリアルを含む。この実施形態では、バリデーション・データはキーイング・マテリアル自体を含む。

【００１０】

１つの代替実施形態では、バリデーテッド・メディアは、メディアの非バリデーション・エリア（非ＶＡ領域）に書き込まれるキーイング・マテリアルを含み、そのキーイング・マテリアルに関係するバリデーション・データが作成され、メディアのバリデーション・エリア（ＶＡ領域）に書き込まれる。

【００１１】

この代替実施形態の１つの変形形態では、キーイング・マテリアルがメディアの非ＶＡ領域に書き込まれ、バリデーション・データがメディアのＶＡ領域に書き込まれるキーイング・マテリアルのコピーを含む。もう１つの変形形態では、キーイング・マテリアルがメディアの非ＶＡに書き込まれ、バリデーション・データがメディアのＶＡ領域に書き込まれるキーイング・マテリアルの関数を含む。

【００１２】

本発明の複数の実施形態で、バリデーテッド・メディアを再生するデバイスをコンプライ

アント・デバイスと称する（以下では、「コンプライアント・デバイス」または単に「デバイス」と称し、非コンプライアントであるデバイスを「非コンプライアント・デバイス」と称する）。

【００１３】

一実施形態で、バリデーテッド・メディアに、メディアのＶＡ領域に直接に書き込まれるキーイング・マテリアルが含まれ、バリデーション・データに、キーイング・マテリアルが含まれ、コンプライアント・デバイスが、メディアのＶＡ領域内にあるキーイング・マテリアルのゆえに、キーイング・マテリアルとバリデーション・データの間の対応関係を見つけることなく、キーイング・マテリアルを検証する。より新しいメディアに、ＶＡ領域に直接に書き込まれるキーイング・マテリアルを含めることができ、このメディアは、再生可能性に関してコンプライアント・デバイスに頼る。

【００１４】

代替実施形態のバリデーテッド・メディアは、メディアの非ＶＡ領域にキーイング・マテリアルを含み、かつメディアのＶＡ領域にキーイング・マテリアルに関連するバリデーション・データを含み、コンプライアント・デバイスは、対応を見つけることなく、あるいは、その代わりに、検証の前提条件として、キーイング・マテリアルとバリデーション・データの間の対応を見つけることによって、キーイング・マテリアルを検証することができる。（メディアのＶＡ領域のバリデーション・データを調べない）非コンプライアント・デバイスとの互換性を保つために、より新しいメディアは、メディアの非ＶＡ領域（非コンプライアント・デバイスがキーイング・マテリアル１１４がここにあると期待し、コンプライアント・デバイスは検証のためにキーイング・マテリアル１１４を探す）に書き込まれるキーイング・マテリアル１１４を含み、メディアのＶＡ領域（コンプライアント・デバイスは、非ＶＡ領域にあるキーイング・マテリアル１１４を検証するデータがここで見つかると期待する）にバリデーション・データを書き込む。

【００１５】

要するに、コンプライアント・デバイスは、バリデーション・データがキーイング・マテリアル自体を含み、キーイング・マテリアルがメディアのＶＡ領域に書き込まれた対応を検査せずにバリデーテッド・メディアのキーイング・マテリアルの真正性を検証することができる。バリデーション・データがメディアのＶＡ領域に書き込まれ、キーイング・マテリアルがメディアの非ＶＡ領域に書き込まれる場合に、コンプライアント・デバイスが、対応を検査せずにバリデーテッド・メディアのキーイング・マテリアルの真正性を検証できることも企図されている。

【００１６】

対応が検査されない場合に、コンプライアント・デバイスは、メディアの非ＶＡ領域に書き込まれるキーイング・マテリアル１１４に対応するか否かに無関係に、ＶＡ領域に含まれるバリデーション・データが正しいことを確立するために、ＶＡ領域のプロパティに頼る。ＶＡ領域のバリデーション・データは、バリデーション・データにキーイング・マテリアル１１４自体が含まれる（すなわち、コンプライアント・デバイスに頼るより新しいメディア）場合、バリデーション・データにキーイング・マテリアル１１４のコピーが含まれる場合、あるいは、たとえばバリデーション・データをキーイング・マテリアル１１４に変換する関数が存在する場合に、保護方式で直接に使用することができる。最悪でも、ＶＡ内のバリデーション・データが不正である場合に、結果のキーイング・マテリアル１１４が、不正な暗号鍵を形成し、これによって、コンテンツが、コンプライアントな形では再生されなくなる。

【００１７】

その代わりに、コンプライアント・デバイスは、バリデーション・データがメディアのＶＡ領域に書き込まれ、キーイング・マテリアル１１４がメディアの非ＶＡ領域に書き込まれる場合に、キーイング・マテリアル１１４とバリデーション・データの間の対応を見つけることによって、バリデーテッド・メディア内のキーイング・マテリアル１１４の真正性を検証することができる。

【００１８】
対応が検査され、検証される場合に、コンプライアント・デバイスは、メディアの非ＶＡ領域のキーイング・マテリアル１１４のタンパリングがなかったことを確信することができる。というのは、このキーイング・マテリアルは、ＶＡ内のバリデーション・データに正しく対応するからである。後者の場合に、キーイング・マテリアル１１４とバリデーション・データが対応しない場合には、コンプライアント・デバイスは、メディアがタンパリングされたと仮定することができ、デバイスは、キーイング・マテリアル１１４を検証せず、メディアが再生されなくなる。
【００１９】
本発明に、下で説明する様々なオペレーションが含まれる。本発明のオペレーションは、ハードウェア・コンポーネントによって実行するか、機械実行可能命令に組み込むことができ、この機械実行可能命令は、汎用プロセッサ、特殊用途プロセッサ、または命令を用いてプログラムされた論理回路にこのオペレーションを実行させる。別法では、オペレーションをハードウェアとソフトウェアの組み合わせによって実行することができる。
【００２０】
本発明は、コンピュータ・プログラム製品として提供することができ、このコンピュータ・プログラム製品には、本発明による処理を実行するようにコンピュータ（または他の電子デバイス）をプログラムするのに使用することができる命令を保管された機械可読メディアを含めることができる。機械可読メディアには、フロッピ・ディスケット、光ディスク、ＣＤ－ＲＯＭ（コンパクト・ディスク読取専用メモリ）、光磁気ディスク、ＲＯＭ（読取専用メモリ）、ＲＡＭ（ランダム・アクセス・メモリ）、ＥＰＲＯＭ（消去可能プログラマブル読取専用メモリ）、ＥＥＰＲＯＭ（電気的消去可能プログラマブル読取専用メモリ）、磁気カード、光カード、フラッシュ・メモリ、または、電子命令を保管するのに適する他のタイプのメディア／機械可読メディアを含めることができるが、これに制限はされない。さらに、本発明を、コンピュータ・プログラム製品としてダウンロードすることもでき、この場合に、プログラムを、搬送波または通信リンク（たとえば、モデムまたはネットワーク接続）を介する他の伝搬メディアで実施されるデータ信号によって、リモート・コンピュータ（たとえばサーバ）から要求元コンピュータ（たとえばクライアント）に転送することができる。したがって、本明細書で、搬送波は、機械可読メディアを含むとみなされなければならない。
【００２１】
用語
本明細書全体を通じて使用される時に、下記の用語は、それぞれの意味と一致しなければならない。
【００２２】
ＶＡ（バリデーション・エリア）
ＶＡは、メディアの部分であって、通常の消費者記録機器／メディアを使用して模倣することを困難にする物理的特性を有する部分である。ＶＡは、書込に特殊な製造用機器を必要とし、そのコンテンツをコピーしにくくされている。さらに、ＶＡは、メディアの他のエリアを読み取るのに使用されるプロセスと物理的に異なるプロセスを使用して読み取られるので、デバイスは、ＶＡに書き込まれたコンテンツを、通常の記録可能メディアに通常のレコーダで書き込まれたコンテンツと区別することができる。ＶＡの１例が、ＤＶＤ－ＲＯＭのバースト・カッティング・エリア（Ｂｕｒｓｔ　Ｃｕｔｔｉｎｇ　Ａｒｅａ）である。
【００２３】
用語「ＶＡ」または「ＶＡ領域」が、本明細書に記載の全般的なプロパティを有するエリアと解釈されなければならないこと、用語「ＶＡ」または「ＶＡ領域」が、本明細書に記載のＶＡのプロパティを有する他のエリアをＶＡの同等物と解釈することを排除してはならないことを、当業者は理解するに違いない。
【００２４】

バリデーテッド・メディア
バリデーテッド・メディアは、ＶＡを使用して、キーイング・マテリアル１１４を検証するメディアである。バリデーテッド・メディアは、メディアのＶＡ領域にバリデーション・データを含む。本発明の実施形態では、下でさらに説明するように、バリデーテッド・メディアのキーイング・マテリアル１１４を検証できない場合に、そのメディアは違法または無許可である。
【００２５】
非バリデーテッド・メディアは、単に、ＶＡ領域にバリデーション・データを含まないが、そのメディアが違法メディアまたは無許可メディアであることを暗示しないメディアである。本発明の実施形態では、非バリデーテッド・メディアは、コンプライアント・メディアと合法的なより古いメディアの間の互換性を保つために、コンプライアント・デバイス（ならびに非コンプライアント・デバイス）によって再生される。これらの実施形態によって、消費者が、より古いメディアを再生でき、違法ディスクを再生できない、より新しいデバイスを購入することが奨励される。もちろん、コンプライアント・デバイスが、非バリデーテッド・メディアを再生できなくすることも企図されている。
【００２６】
キーイング・マテリアル
キーイング・マテリアル１１４には、保護されたコンテンツへのアクセスするための値が含まれる。ＣＳＳ（後で説明する）によって保護されるコンテンツでは、キーイング・マテリアル１１４に、セキュア・ディスク・キー・データ（Ｓｅｃｕｒｅ　Ｄｉｓｃ　Ｋｅｙ　Ｄａｔａ）を含めることができ、ＣＰＰＭ（後で説明する）によって保護されるコンテンツでは、キーイング・マテリアル１１４に、アルバム・アイデンティファイヤを含めることができる。通常、この値は、暗号化されたコンテンツ１１２を解読する鍵として使用されるか、暗号鍵を形成するのに使用される。この値は、すべてのメディアについて一意とすることができるが、通常は、メディアのある組について一意である。
【００２７】
バリデーション
キーイング・マテリアル１１４は、暗号化されたコンテンツ１１２を解読するのに使用される（または、コンテンツを解読するのに必要な暗号鍵を形成する）時に検証され、これによって、読取専用コンテンツの再生が可能になる。
【００２８】
バリデーションの前に対応が検査される場合に、対応が見つかったならば、メディアの非ＶＡ領域からのキーイング・マテリアル１１４が使用される。
【００２９】
バリデーションについて対応が検査されない場合には、暗号化されたコンテンツの解読に使用されるキーイング・マテリアル１１４はバリデーション・データから導出される。バリデーション・データにキーイング・マテリアル１１４が含まれる（すなわち、これらが同一である）場合、または、バリデーション・データが、非ＶＡ領域のキーイング・マテリアル１１４のコピーである場合には、キーイング・マテリアル１１４は、バリデーション・データ自体を使用することによって、バリデーション・データから導出される。
【００３０】
他の場合に、キーイング・マテリアル１１４は、バリデーション・データを元のキーイング・マテリアルに変換することによって、バリデーション・データから導出することができる。たとえば、いくつかの実施形態（後で説明する、ＣＳＳに似たコンテンツ保護方式など）で、バリデーション・データは、キーイング・マテリアル１１４の関数であり、元のキーイング・マテリアル１１４を使用してコンテンツを解読するために、同一の暗号関数をバリデーション・データに対して使用して、元のキーイング・マテリアル１１４を形成する。
【００３１】
デバイス

デバイスは、読取専用メディア上のコンテンツを再生する任意の機構である。ＤＶＤの場合に、そのような機構に、ＤＶＤ再生デバイスが含まれ、これは、たとえばＤＶＤプレイヤまたはＤＶＤドライブとすることができる。

【００３２】

コンプライアント・デバイス

コンプライアント・デバイスはバリデーテッド・メディアを再生するデバイスである。

【００３３】

概論

一般に、図２の流れ図（ブロック２００で開始される）に示されているように、バリデーテッド・メディアを再生するコンプライアント・デバイスは、２つの形の１つでキーイング・マテリアル１１４を検証する。コンプライアント・デバイスは、ブロック２０２に示されているように、ＶＡ内のバリデーション・データを使用することによってキーイング・マテリアル１１４を検証することができ、ここで、バリデーション・データには、ＶＡ領域内のキーイング・マテリアル１１４、非ＶＡ領域内のキーイング・マテリアル１１４のコピー、または非ＶＡ領域に書き込まれたキーイング・マテリアル１１４の関数（この場合に、バリデーション・データは、上で説明したように、コンテンツの解読に使用される前の、関数への第１の対象である）を含めることができる。バリデーション・データに不正な暗号鍵を作る他の値が含まれるか、値が全く含まれないという希な場合またはありそうにない場合には、コンプライアント・デバイスは、それでもキーイング・マテリアルを「検証」し、ＶＡ領域内の値を使用するが、ＶＡ領域内の値が不正／無効であると、コンテンツは再生されなくなる。

【００３４】

別法では、コンプライアント・デバイスは、ブロック２０４で、メディアの非ＶＡ領域に書き込まれたキーイング・マテリアル１１４を、メディアのＶＡ領域に書き込まれたバリデーション・データと比較する。ブロック２０６で、キーイング・マテリアル１１４とバリデーション・データが対応するかどうかを判定する。これらが対応しない場合には、デバイスは、ブロック２０８で、キーイング・マテリアル１１４を検証せず、これによって、キーイング・マテリアル１１４が、暗号化されたコンテンツ１１２の解読に使用されなくなり、これによって、コンテンツを再生できなくなる。キーイング・マテリアル１１４とバリデーション・データ４０２が対応する場合には、ブロック２１０で、デバイスが、キーイング・マテリアル１１４を検証し、これを暗号化されたコンテンツ１１２の解読に使用できるようにする。この方法は、ブロック２１２で終わる。

【００３５】

本発明の実施形態を示したので、以下で、メディアの再生に関して存在する可能性がある異なるシナリオの概要を示す。

【００３６】

１．バリデーテッド・メディアがコンプライアント・デバイスで再生される：コンプライアント・デバイスは、メディアのＶＡ領域を認識し、したがって、ＶＡ内のバリデーション・データを探す。キーイング・マテリアル１１４を、コンプライアント・デバイスだけに頼るより新しいメディアでは、図２のブロック２０２に示されているように自動的に検証することができ、あるいは、特定の実施形態では、メディアのＶＡプロパティを信頼する。他の実施形態では、図２のブロック２０６に示されているように、キーイング・マテリアル１１４の検証の前に、ＶＡ内のバリデーションと非ＶＡのキーイング・マテリアル１１４の間の対応を見つけることを選択することができる。

【００３７】

２．バリデーテッド・メディアが非コンプライアント・デバイスで再生される：非コンプライアント（すなわち、より古い）デバイスは、メディアのＶＡ領域を認識しないか、ＶＡ内のバリデーション・データを探すように設計されていない場合がある。そのようなデバイスは、メディアの非ＶＡ領域のキーイング・マテリアル１１４を使用して、以前の解読方法に従って、コンテンツを解読する。

【００３８】
３．非バリデーテッド・メディアがコンプライアント・デバイスで再生される：コンプライアント・デバイスは、バリデーション・データを含むＢＣＡを探すが、見つけない。デバイスは、この場合には、非ＶＡ領域のキーイング・マテリアル１１４を使用して、以前の解読方法に従って、コンテンツを解読する（上で説明したように、デバイスは、その代わりに、メディアのコンテンツの再生を防ぐことができる）。
【００３９】
４．非バリデーテッド・メディアが非コンプライアント・デバイスで再生される：非コンプライアント・デバイスは、非ＶＡ領域のキーイング・マテリアル１１４を使用して、以前の解読方法に従って、コンテンツを解読する。
【００４０】
シナリオ２および４では、非コンプライアント・デバイスが、メディアの無許可コピーの再生を防止しない。シナリオ２および３では、バリデーテッド・メディアまたはコンプライアント・デバイスを用いて無許可コピーの防止を実施することができないが、新しいデバイスと古いメディアの間のインターオペラビリティ（シナリオ３）ならびに古いデバイスと新しいメディアの間のインターオペラビリティ（シナリオ２）が維持される。古いデバイスと古いメディアに関する互換性を保つために、図２の方法を、ブロック３００から開始される図３のように修正することができる。
【００４１】
ブロック３０２で、読み取られるメディアがバリデーテッド・メディアであるかどうかに関する判定を行う（この判定は、さらに詳細に説明する）。メディアがバリデーテッド・メディアでない場合には、ブロック３１４で、コンプライアント・デバイスは、バリデーション・データを探すのではなく、単にメディアの非ＢＣＡ領域のキーイング・マテリアル１１４を使用して、以前の解読方法に従ってコンテンツを解読する。この判定では、コンプライアント・デバイスと非ＢＣＡバリデーテッド・メディアの間のインターオペラビリティが保たれ、読み取られるメディアがバリデーテッド・メディアでない場合に、コンプライアント・デバイスが必ずしも非バリデーテッド・メディアの再生を防止しない。
【００４２】
ブロック３０６および３０８では、メディアがバリデーテッド・メディアであると判定されている。コンプライアント・デバイスは、ブロック３０６に示されているように、ＶＡ（いくつかの場合を上で説明した）内のバリデーション・データを使用することによって、キーイング・マテリアル１１４を検証することができる。ＶＡは、コンテンツのコピーを困難にする特殊なプロパティを有するので、コンプライアント・デバイスは、ＶＡ内のデータがタンパリングされていないことをある程度確信する。
【００４３】
コンプライアント・デバイスは、その代わりに、ブロック３０８に示されているように、メディアの非ＶＡ領域のキーイング・マテリアル１１４をメディアのＶＡのバリデーション・データと比較することによって、キーイング・マテリアル１１４を検証することができる。メディアの非ＶＡ領域へのキーイング・マテリアル１１４の保管を継続することは、バリデーテッド・メディアと非コンプライアント・デバイスの間のインターオペラビリティを保つ手段であり、バリデーテッド・メディアが、所与のメディアの非ＶＡ内のキーイング・マテリアル１１４を期待する非コンプライアント・デバイスによって読み取られる場合に、非コンプライアント・デバイスがエラーにならなくなる。したがって、非コンプライアント・デバイスは、メディアの非ＶＡ内のキーイング・マテリアル１１４を探し、その値を使用してコンテンツを解読する。しかし、非コンプライアント・デバイスは、メディアがバリデーテッド・メディアであっても、キーイング・マテリアル１１４の真正性を検証する機構を有しない。
【００４４】
その一方で、コンプライアント・デバイスは、バリデーテッド・メディアに書き込まれたキーイング・マテリアル１１４の真正性を検証することができる。ブロック３１０で、キ

ーイング・マテリアル１１４がバリデーション・データに対応するかどうかに関する判定を行う。対応がない（対応を後で説明する）場合に、ブロック３０４で、コンプライアント・デバイスは、キーイング・マテリアル１１４を検証せず、これによって、コンテンツが再生されなくなる。ブロック３１２で、対応がある場合に、コンプライアント・デバイスがキーイング・マテリアル１１４を検証する。この方法は、ブロック３１６で終了する。

【００４５】

本発明の実施形態によれば、ＢＣＡバリデーテッド・メディアによって、ハッカーが、たとえばＤＶＤ－ＲＯＭに保管されたキーイング・マテリアル１１４（および／またはそれに関連するバリデーション・データ）をＤＶＤ－Ｒにコピーできなくなり、これによって、ＤＶＤ－ＲへのＤＶＤ－ＲＯＭの無許可コピーが再生不能になる。非バリデーテッドＤＶＤなどの非バリデーテッド・メディアでは、ハッカーが、たとえば下記によって、これを行うことができる。

【００４６】

・キーイング・マテリアル１１４を、ＤＶＤ－Ｒのデータ・エリア１０２に書き込む（具体的には、ＤＶＤ－Ｒのユーザ・データ・エリア）が、ＤＶＤ－ＲＯＭのＣＤＡ１１０内のアドレスを割り当てて、デバイスが、それを元のＤＶＤ－ＲＯＭにある合法的なキーイング・マテリアル１１４と区別できなくする。

【００４７】

・ＤＶＤ－ＲＯＭから非コンプライアントＤＶＤ－ＲディスクのＣＤＡ１１０に、有効なキーイング・マテリアル１１４を直接に書き込む。

【００４８】

したがって、図４に示されているように、バリデーテッド・メディア４００に、バリデーション・エリア４０６（ＶＡ）領域と非ＶＡ領域４０４が含まれ、ＶＡ領域にはバリデーション・データ４０２が含まれ、非ＶＡ領域４０４には暗号化されたコンテンツ１１２が含まれる。いくつかの実施形態で、非ＶＡ領域４０４に、さらに、キーイング・マテリアル１１４が含まれる。

【００４９】

例示的実施形態

バリデーション・エリア４０６を含むメディアの例に、ＤＶＤ－ＲＯＭ（ＤＶＤ－読取専用メモリ）が含まれる。本明細書で、ＤＶＤメディアに関して複数の実施形態を説明する。具体的に言うと、本発明に関する概念を下記の例示的実施形態に関して説明する。

【００５０】

・ＣＰＰＭによって保護されるＤＶＤコンテンツ

【００５１】

・ＣＳＳによって保護されるＤＶＤコンテンツ

【００５２】

・ＣＰＰＭ／ＣＳＳによって保護されるＤＶＤコンテンツ

【００５３】

これらの特定の実施形態を説明するが、本発明が、これらの特定の実施形態に制限されることを意図されていないこと、本発明の全般的な概念を、本明細書に記載されていない様々な実施形態に適用可能であることを、当業者は理解するに違いない。

【００５４】

これらの実施形態の現在の状態を、この節（「例示的実施形態」）で説明する。これらの例示的実施形態に関連する本発明の全般的な概念を、後続の節で説明する。適当な場合に、あるいは本発明の理解に役立つ場合に、本発明の全般的な概念を、これらの例示的実施形態に関して示す。

【００５５】

ＣＰＰＭによって保護されるＤＶＤコンテンツ

コンテンツ・プロテクション・フォー・プリレコーデッド・メディア（Ｃｏｎｔｅｎｔ

Ｐｒｏｔｅｃｔｉｏｎ Ｆｏｒ Ｐｒｅｒｅｃｏｒｄｅｄ Ｍｅｄｉａ、ＣＰＰＭ）仕様では、事前記録された（読取専用）メディア・タイプで配布されるコンテンツを保護する、堅牢で更新可能な方法が定義されている。１つの例示的実施形態で、ＣＰＰＭ技術を使用して、読取専用ＤＶＤ（ＤＶＤ－ＲＯＭ）ディスクで配布されるＤＶＤ－Ａｕｄｉｏコンテンツを保護する仕様を定義する。

【００５６】

一般に、各ＣＰＰＭコンプライアントＤＶＤ－Ａｕｄｉｏ再生デバイス（ハードウェアＤＶＤプレイヤ、またはＤＶＤドライブを備えるコンピュータと共に使用されるソフトウェア・プレイヤ）に、K_{d_0}、K_{d_1}、．．．、K_{d_15}と表される１６個のデバイス鍵の組が与えられる。これらの鍵は、４Ｃ Ｅｎｔｉｔｙ、ＬＬＣ社によって供給され、メディア鍵（Ｋｍ）を計算するためにＭＫＢ（メディア鍵ブロック）を処理する際に使用される。鍵セットは、デバイスごとに一意とするか、複数のデバイスによって共通して使用されるものとすることができる。

【００５７】

ＣＰＰＭ保護されたＤＶＤ－Ａｕｄｉｏコンテンツを有するディスクの各面に、下記が含まれる。

【００５８】

・リードイン・エリア１０４（具体的には、非ユーザ・データ・エリア）に事前記録されたアルバム・アイデンティファイヤ（ID_{album}）と称するキーイング・マテリアル１１４。

【００５９】

・データ・エリア１０２に特定のファイルとして事前記録されたメディア鍵ブロック（ＭＫＢ）。

【００６０】

・データ・エリア１０２に特定のファイルとして事前記録された暗号化されたコンテンツ１１２。

【００６１】

本発明において、アルバム・アイデンティファイヤを、下でさらに説明するが、ＭＫＢおよび暗号化されたコンテンツ１１２という概念は、上で説明したもの以外の本発明の実施形態に直接に関係しないので、これ以上は説明しない。アルバム・アイデンティファイヤが、ＣＰＰＭによって保護されたコンテンツの無許可コピーを防ぐのに、メディア鍵ブロックと共にどのように使用されるかの詳細な説明については、４Ｃ Ｅｎｔｉｔｙ、ＬＬＣ社が公表した文書、「ＣＯＮＴＥＮＴ ＰＲＯＴＥＣＴＩＯＮ ＦＯＲ ＰＲＥＲＥＣＯＲＤＥＤ ＭＥＤＩＡ ＳＰＥＣＩＦＩＣＡＴＩＯＮ, ＤＶＤ ＢＯＯＫ」、Ｒｅｖｉｓｉｏｎ ０．９３、２００１年1月３１日を参照されたい。

【００６２】

ＣＰＰＭ保護されたＤＶＤ－Ａｕｄｉｏコンテンツの各面に、６４ビットのアルバム・アイデンティファイヤ（ID_{album}）が含まれ、このアルバム・アイデンティファイヤは、ディスク製造業者によって、非データ・エリア１０４に配置される。具体的に言うと、アルバム・アイデンティファイヤは、コントロール・データ・エリア１１０セクタ＃２のバイト８０から８７に配置される。アルバム・アイデンティファイヤの上位８ビット（バイト８０に保管される）は、現在、０の値を有するように定義されている。上位互換性のために、これらの８ビットの非ゼロ値はエラーとみなされない。残りの５６ビットについて、コンテンツ・プロバイダが、ＣＰＰＭを使用して保護されるＤＶＤ－ａｕｄｉｏアルバムのそれぞれに、秘密の予測不能な（たとえばランダムな）値を個別に割り当てる。コンテンツ・プロバイダのオプションとして、所与のアルバムのすべてのプレスに、同一のID_{album}値を含めることができ、あるいは、異なるプレスに異なる値を割り当てることができる。

【００６３】

アルバム・アイデンティファイヤの役割は、個々のメディア識別の役割と異なる。そうで

はなく、アルバム・アイデンティファイヤは、ＣＰＰＭ暗号鍵管理に一体化されたアルバム固有の値として働き、コンプライアントＤＶＤ記録可能－書換可能メディアで書き込み可能でない位置に配置される。ＰＣ（パーソナル・コンピュータ）システムでは、アルバム・アイデンティファイヤが、ＤＶＤドライブ認証プロトコルを使用してアクセスされる。そのプロトコルの他の非ＣＰＰＭ使用との一貫性のために、アルバム・アイデンティファイヤ値を含むコントロール・データ・エリア１１０セクタ＃２内のデータの信頼性を維持しなければならない。

【００６４】

ＣＳＳによって保護されたＤＶＤコンテンツ

コンテンツ・スクランブル・システム（ＣＳＳ）は、ディスクから直接にＤＶＤ－Ｖｉｄｅｏファイルをコピーできなくすることを意図されたデータ・スクランブルおよび認証の方式である。

【００６５】

ＣＳＳスクランブル・アルゴリズムでは、ドライブ・ユニットと鍵を交換して、暗号化鍵を生成し、この暗号化鍵を使用して、ディスクからのデータをスクランブル解除するのに必要なディスク鍵およびタイトル鍵の交換を不明瞭にする。ＤＶＤプレイヤは、デコードされ表示される前にデータを解読するＣＳＳ回路を有する。コンピュータ側では、ＤＶＤデコーダのハードウェアおよびソフトウェアに、ＣＳＳ解読モジュールが含まれなければならない。すべてのＤＶＤドライブが、コンピュータ内のＣＳＳモジュールと認証鍵および解読鍵を交換するための余分なファームウェアを有する。

【００６６】

ＣＰＰＭ／ＣＳＳによって保護されたＤＶＤコンテンツ

ＣＰＰＭコンテンツとＣＳＳコンテンツの両方を含む組み合わせディスクでは、ＣＤＡ１１０は、ＣＰＰＭアルバム・アイデンティファイヤだけではなく、秘密に保たれなければならないセキュア・ディスク・キー・データをも含む。

【００６７】

メディアがＢＣＡバリデーテッド・メディアであるかどうかの判定

本明細書で使用される、キーイング・マテリアル１１４を検証するのにバリデーション・エリア４０６を使用するメディアをバリデーテッド・メディア４００と称する。メディアがバリデーテッド・メディア４００であるかどうかを判定する様々な方法がある。たとえば、本発明の一実施形態では、メディアが、ＣＰＰＭ保護されたコンテンツを有する事前記録されたＤＶＤである。ＤＶＤでは、メディアのＶＡ領域４０６をバースト・カッティング・エリアと称し、ＤＶＤでＣＰＰＭ保護方式が使用される場合に、キーイング・マテリアル１１４に、アルバム・アイデンティファイヤが含まれる。アルバム・アイデンティファイヤは、非ＢＣＡ領域、具体的にはリードイン・エリア１０４のコントロール・データ・エリア１１０に書き込まれる。前に述べたように、アルバム・アイデンティファイヤは、８バイト（６４ビット）値である。技術の現状では、最上位８ビットに０がセットされる。

【００６８】

ＣＰＰＭによって保護されるＤＶＤを使用して本発明の実施形態を実施するために、最上位８ビットを使用して、これらのビットの１つまたは複数に１をセットすることによって、メディアがバリデーテッド・メディア４００であることを示す。したがって、デバイスが、ＣＰＰＭ保護されたメディアがバリデーテッド・メディア４００であると判定する時に、そのデバイスは、アルバム・アイデンティファイヤを検査して、たとえば、その最上位ビットに１がセットされているかどうかを判定する。そうである場合には、デバイスは、メディア４００のバリデーション・エリア４０６（具体的にはＢＣＡ）内のバリデーション・データ４０２を探すようにトリガされる。そうでない場合には、メディアは、バリデーテッド・メディア４００ではなく、デバイスは、単に、メディアの非ＶＡ領域のキーイング・マテリアル１１４を使用して、以前の方法に従ってコンテンツを解読する。

【００６９】

セキュア・ディスク・キー・データがメディアの非ＶＡ領域に書き込まれるものなどの他の実施形態では、他の方法を使用して、メディアがバリデーテッド・メディア４００であるかどうかを判定することができる。一般に、ある種のトリガが使用され、これには、通常は、現在予約済みまたは未使用のデータ項目に、現在定義されている値以外の値をセットすることが含まれる。本発明の実施形態では、トリガとして使用されるデータ項目が、キーイング・マテリアル１１４と一体化され、コンプライアント・デバイスが、キーイング・マテリアル１１４を検証する時に、トリガ値がタンパリングされたかどうかも判定できるようになっている。

【００７０】

たとえば、ＣＰＰＭによって保護されたコンテンツで、コンテンツを解読する暗号鍵が、アルバム・アイデンティファイヤに依存するので、アルバム・アイデンティファイヤをタンパリングする試みによって、正しい暗号鍵を作れなくなり、これによって、コンテンツが再生できなくなる。したがって、ハッカーが、最上位ビットを１から０に反転する（上の例に関して）ことによってこの方式の裏をかくことを試みる場合に、ハッカーは、アルバム・アイデンティファイヤも変更することになる。コンプライアント・デバイスは、検証をバイパスするが、それでも、コンテンツを解読する試みの際にアルバム・アイデンティファイヤを使用し、そのアルバム・アイデンティファイヤがタンパリングされているので、コンテンツの解読の正しい鍵は作られない。

【００７１】

キーイング・マテリアル

キーイング・マテリアル１１４は、保護されたコンテンツを含むメディア１００および４００に書き込まれる、コンテンツへのアクセスがそれに基づく値または値の組である。たとえば、上で述べたように、ＣＰＰＭ（コンテンツ・プロテクション・フォー・プリレコーデッド・メディア）によって保護されるＤＶＤ－Ａｕｄｉｏメディアでは、キーイング・マテリアル１１４に、アルバム・アイデンティファイヤが含まれ、このアルバム・アイデンティファイヤは、保護される各アルバムに個別にランダムに割り当てられる８バイト（６４ビット）値であり、メディアのコンテンツを解読するのに必要な暗号鍵を形成する際に使用される。ＣＳＳ（コンテンツ・スクランブル・システム）によって保護されるＤＶＤ－Ｖｉｄｅｏでは、キーイング・マテリアル１１４に、セキュア・ディスク・キー・データが含まれる。ＣＳＳ／ＣＰＰＭ保護方式の組み合わせを使用するメディアには、アルバム・アイデンティファイヤとセキュア・ディスク・キー・データの両方が存在する。

【００７２】

コンテンツの解読に使用される（それを直接に使用することによって、またはコンテンツの解読のための暗号関数を形成することによってのいずれか）キーイング・マテリアル１１４は、上の「バリデーション」の節で説明したように、ＶＡ領域にあるバリデーション・データから導出することができ、あるいは、非ＶＡ領域から直接に使用することができる。

【００７３】

バリデーション・データ

バリデーション・データ４０２は、メディアから読み取られたキーイング・マテリアル１１４が真正である（すなわち、広範囲で入手可能な記録機器および記録可能メディアを使用して書き込まれた無許可コピーでない）ことを再生デバイスが検証できるようにするデータである。

【００７４】

バリデーション・データ４０２の性質および位置は、所与のバリデーテッド・メディア４００について使用可能にされた保護のタイプに依存する。いくつかの場合に、バリデーション・データ４０２に、キーイング・マテリアル１１４自体を含めることができ、他の場合に、バリデーション・データ４０２に、キーイング・マテリアル１１４のコピーまたはキーイング・マテリアル１１４の暗号関数を含めることができる。上で説明した例示的実施形態のそれぞれに関する例を下で示す。本明細書に記載の本発明の実施形態では、バリ

デーション・データ４０２が、メディアのＶＡ領域４０６に書き込まれる。
【００７５】
ＣＰＰＭによって保護されるＤＶＤコンテンツ
キーイング・マテリアル１１４にアルバム・アイデンティファイヤが含まれるＣＰＰＭによって保護されたバリデーテッド・メディアでは、バリデーション・データ４０２に、アルバム・アイデンティファイヤのコピーが含まれる。
【００７６】
ＣＳＳまたはＣＰＰＭ／ＣＳＳによって保護されたＤＶＤコンテンツ
コンテンツがＣＳＳによって保護される場合およびコンテンツがＣＰＰＭ／ＣＳＳの組み合わせ方式によって保護される場合のバリデーテッド・メディアでは、セキュア・ディスク・キー・データを秘密に保たなければならない。その結果、たとえばドライブからホストへの転送中にセクタをスクランブルする形に起因して、セキュア・ディスク・キー・データを含むＣＤＡ１１０セクタのすべての値（おそらくは、アルバム・アイデンティファイヤを含むセクタ＃２を含む）を秘密に保たなければならない。しかし、ＶＡ領域４０６にアルバム・アイデンティファイヤのコピーを保管することによって、セキュア・ディスク・キー・データの値が明白になるはずである（組み合わせＣＰＰ／ＣＳＳ方式が使用される場合に）。というのは、標準的なドライブ・インターフェースで、ＢＣＡ領域４０６を自由に読み取ることができるからである。
【００７７】
したがって、キーイング・マテリアル１１４にセキュア・ディスク・キー・データが含まれている、ＣＳＳによって保護されるコンテンツの場合には、バリデーション・データ４０２がセキュア・ディスク・キー・データの関数を含む。組み合わせ方式によってコンテンツが保護され、キーイング・マテリアル１１４が、アルバム・アイデンティファイヤとセキュア・ディスク・キー・データの両方を含む場合に、バリデーション・データ４０２が、アルバム・アイデンティファイヤの関数ならびにセキュア・ディスク・キー・データの関数を含む。
【００７８】
バリデーション・データ４０２を作成するのに、所与の値自体を使用するのではなく、値に対する１方向暗号関数を使用すると、ＶＡ領域４０６を読み取ることによってはその値を発見できなくなる。それと同時に、下の「対応の判定」の節で説明するように、デバイスが、ＢＣＡ領域４０６内のバリデーション・データ４０２を、ＣＤＡ１１０のキーイング・マテリアル１１４と比較できるようになる。
【００７９】
他のコンテンツ保護フォーマット
メディアの読み取りに関する新しいコンテンツ保護フォーマットおよびコンテンツ保護方式は、バリデーション・データ４０２にキーイング・マテリアル１１４が含まれるように、キーイング・マテリアル１１４をメディアのＶＡ領域に単に配置するように設計することができる。ＶＡ領域は、その領域の模倣を非常に困難にする特殊なプロパティを有するので、コンプライアント・デバイスは、ＶＡ領域内のデータがタンパリングされていないことを高い度合で信頼することができる。
【００８０】
その代わりに、新しいフォーマットを、メディアの非ＶＡ領域内のキーイング・マテリアルおよびＢＣＡ内のバリデーション・データ（おそらくはキーイング・マテリアルのコピー）を用いて設計することができる。この手法を用いると、新しいフォーマットでのコンテンツのプロバイダが、ＢＣＡにバリデーション・データを含めるか否か（すなわち、無許可コピーに対する強化された保護と、ＢＣＡを含めることの製造コストの増加との間のトレードオフ）を選択できるようになる。
【００８１】
対応の判定
図５に示されているように、対応は、メディアの非ＶＡ領域に書き込まれたキーイング・

マテリアル１１４をメディアのＶＡ領域のバリデーション・データ４０２と比較することによって、デバイス５００がキーイング・マテリアル１１４を検証できるかどうかに関連する。本発明の実施形態では、キーイング・マテリアル１１４を、より安全なＶＡ領域４０６に配置するのではなく、メディアの非ＶＡ領域４０４に配置する場合に、および所与のコンプライアント・デバイスがＶＡ領域４０６に書き込まれたバリデーション・データ４０２を自動的に検証しない方式の場合に、対応が判定される。

【００８２】

コンプライアント・デバイスと、上で説明した一実施形態のＢＣＡバリデーテッド・メディア４００を仮定すると、デバイス５００は、非ＶＡ領域４０４（たとえば、ＤＶＤのリードイン・エリア１０４のコントロール・データ・エリア１１０）からキーイング・マテリアル１１４を検索５０６し、ＶＡ領域４０６からバリデーション・データ４０２を検索する。

【００８３】

デバイス５００内のコンパレータ５０２が、キーイング・マテリアル１１４をバリデーション・データ４０２と比較する。値が対応する場合に、デバイス５００内のバリデータ５０４が、キーイング・マテリアル１１４の真正性を検証し、キーイング・マテリアル１１４をコンテンツ１１２の解読に使用できるようにする。コンパレータ５０２およびバリデータ５０４は、デバイス５００内の別々の実体として図示されているが、そのような描写が、例示のみであり、これらの機能性を単一の実体に組み合わせることができ、その代わりに、デバイス自体と別個の実体とすることができることを、当業者は理解するに違いない。

【００８４】

キーイング・マテリアル１１４とバリデーション・データ４０２の間の対応は、特定の実施形態で使用されるキーイング・マテリアル１１４およびバリデーション・データ４０２のタイプに応じて、複数の形で判定することができる。本発明の例示的実施形態でこの判定を行う例を、下で説明する。

【００８５】

ＣＰＰＭによって保護されたＤＶＤコンテンツ

ＣＰＰＭによって保護されたコンテンツに対して、キーイング・マテリアル１１４とバリデーション・データ４０２の間の対応は、非ＶＡ領域４０４（たとえばＤＶＤのコントロール・データ・エリア１１０）のアルバム・アイデンティファイヤが、ＢＣＡ領域４０６内のアルバム・アイデンティファイヤのコピーと一致する場合に存在する。コンパレータ５０２によって比較されるこの２つの値が一致する場合に、デバイス５００のバリデータ５０４が、アルバム・アイデンティファイヤを認証し、これを使用して、メディア・コンテンツ１１２を解読することができる。

【００８６】

ＣＳＳによって保護されたＤＶＤコンテンツ

ＣＳＳによって保護されたコンテンツについて、キーイング・マテリアル１１４とバリデーション・データ４０２の間の対応は、非ＶＡ領域４０４（たとえばＤＶＤのコントロール・データ・エリア１１０）のセキュア・ディスク・キー・データの関数が、ＶＡ内のバリデーション・データ４０２（すなわち、セキュア・ディスク・キー・データの関数）と一致する場合に存在する。たとえば、ＣＤＡ１１０からのセキュア・ディスク・キー・データ値の１つの１方向暗号関数をＶＡ領域４０６に書き込み、デバイス５００が非ＶＡ領域４０４からセキュア・ディスク・キー・データを読み取る時に、デバイス５００がその値に同一の１方向暗号関数を使用するようにする。

【００８７】

デバイス５００が、コンパレータ５０２によって判定される計算された値を比較し、たとえば、これをＶＡ領域４０６で見つかったバリデーション・データと比較する。値が一致する場合に、デバイス５００のバリデータ５０４が、セキュア・ディスク・キー・データ値を認証し、これを使用して、メディア・コンテンツ１１２を解読することができる。

【００８８】
ＣＰＰＭ／ＣＳＳによって保護されたＤＶＤコンテンツ
ＣＰＰＭ／ＣＳＳによって保護されたコンテンツについて、キーイング・マテリアル１１４とバリデーション・データ４０２の間の対応は、非ＶＡ領域４０４（たとえばＤＶＤのコントロール・データ・エリア１１０）のアルバム・アイデンティファイヤの関数が、ＶＡ内のバリデーション・データ４０２（すなわち、セキュア・ディスク・キー・データの関数およびアルバム・アイデンティファイヤの関数）と一致する場合に存在する。ＣＤＡ１１０セクタ＃２からのアルバム・アイデンティファイヤの１つの１方向暗号関数と、セキュア・ディスク・キー・データの１方向暗号関数がＢＣＡ領域４０６に書き込まれ、デバイスが、ＣＤＡからアルバム・アイデンティファイヤおよびセキュア・ディスク・キー・データを読み取る時に、これらの値に対して同一の１方向暗号関数を使用するようにする。
【００８９】
デバイス５００は、非ＢＣＡ領域４０４からのアルバム・アイデンティファイヤとセキュア・ディスク・キー・データに対する関数を計算し、計算された値を、ＢＣＡ領域４０６で見つかったバリデーション・データの計算された値と比較する。値が一致する場合には、デバイス５００のバリデータ５０４が、アルバム・アイデンティファイヤおよびセキュア・ディスク・キー・データを認証し、これらを使用して、メディア・コンテンツ１１２を解読することができる。
【００９０】
結論
したがって、本発明の実施形態は、ＤＶＤ－ＲＯＭメディアに事前記録されたＣＰＰＭコンテンツまたはＣＳＳコンテンツなどのコンテンツを無許可コピーから保護するためのキーイング・マテリアル１１４の検証という堅牢な手段を提供する。機能強化された保護は、本発明を使用する、新しいディスクおよび新しいデバイスによって使用可能になる。それと同時に、新しいデバイスと古いデバイスの間、および新しいメディアと古いメディアの間の完全なインターオペラビリティが維持される。
【００９１】
この明細書では、本発明を、その特定の実施形態に関して説明した。しかし、本発明の広義の趣旨および範囲から逸脱せずに、本発明に対して様々な修正および変更を行うことができることは明白である。したがって、明細書および図面は、制限的な意味ではなく、例示とみなされなければならない。
【００９２】
たとえば、複数の例示的実施形態を説明したが、本発明の概念を、他のタイプのコンテンツ、コンテンツ保護システム、およびメディア・フォーマットに適用できることを、当業者は理解するに違いない。たとえば、本明細書に記載の例示的実施形態は、現在の保護の形態のいくつか（すなわち、ＣＰＰＭ、ＣＳＳ）に関連するＤＶＤメディアに固有であるが、本明細書に記載の読取専用メディアに、ＶＡ領域および非ＶＡ領域が含まれ、必ずしもＤＶＤメディアにあるすべての領域が含まれない場合があることを、当業者は理解するに違いない。
【００９３】
さらに、本明細書に記載の本発明の実施形態では、バリデーション・エリアと称するエリアに言及したが、バリデーション・エリアが、本明細書に記載の特性を有するエリアであること、そのようなエリアが、バリデーション・エリアと呼ばれるエリア、または用語バリデーション・エリアを含むエリアに制限されないことを理解されたい。１例として、ＤＶＤ－ＲＯＭは、バースト・カッティング・エリアと称するバリデーション・エリアを含んでいる。
【００９４】
本明細書で、１方向暗号関数について述べたが、両方向暗号関数を使用することができることも企図されている。たとえば、対応が検査されず、バリデーション・データにキーイ

ング・マテリアルの関数が含まれる場合に、バリデーション・データを元のキーイング・マテリアルに変換する両方向暗号関数を使用することができる。

【図面の簡単な説明】

【００９５】

【図１Ａ】ＤＶＤ（ディジタル多用途ディスク）などのメディアの第１の図を示す図である。

【図１Ｂ】図１Ａに示されたメディアの代替の図を示す図である。

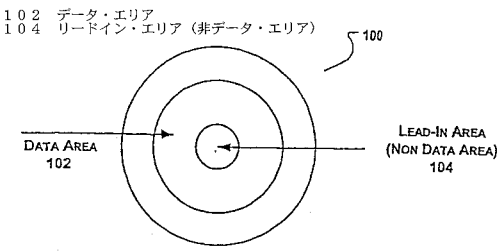
【図２】本発明の全般的な実施形態での方法を示す流れ図である。

【図３】本発明の実施形態での代替方法を示す流れ図である。

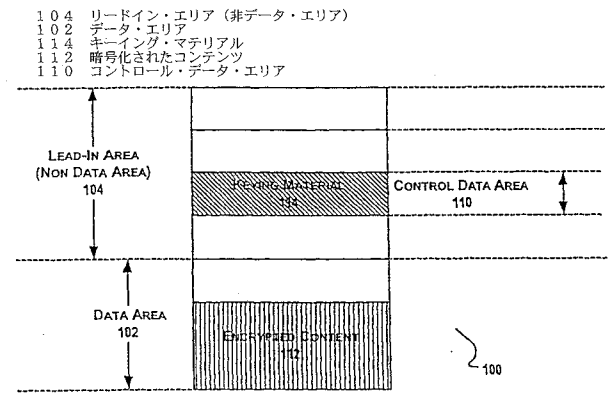
【図４】本発明の実施形態によるＢＣＡバリデーテッド・メディアのレイアウトを示す図である。

【図５】本発明の実施形態によるシステムを示す概念図である。

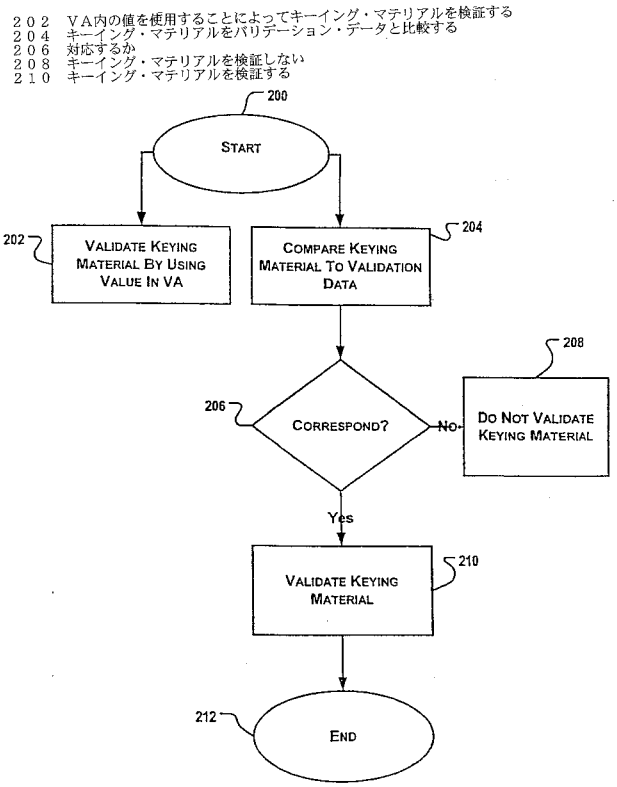
【図１Ａ】



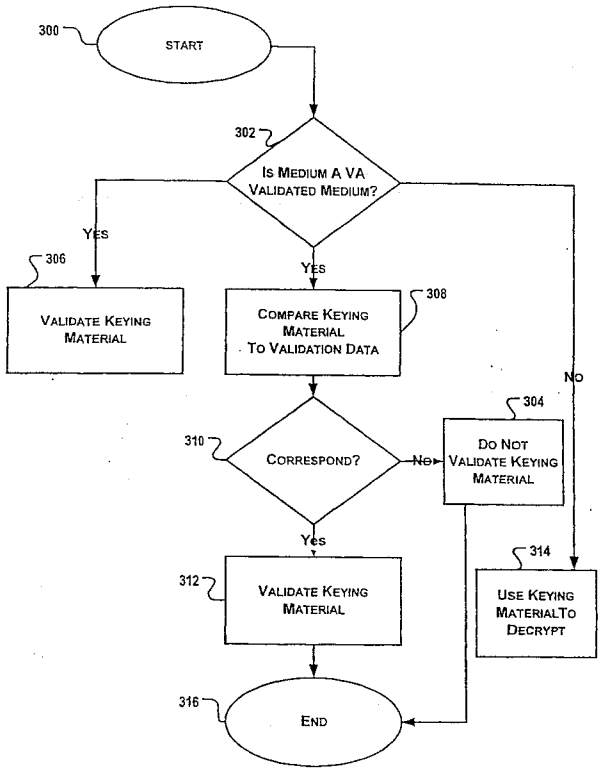
【図１Ｂ】



【図２】

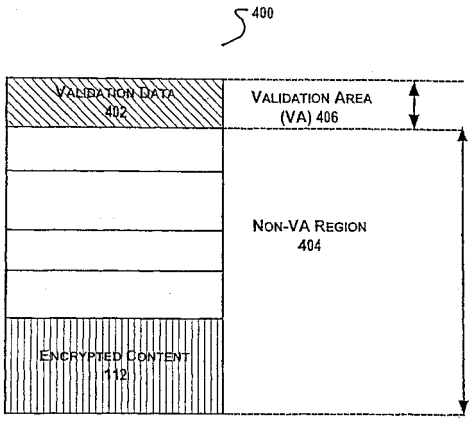


【図３】



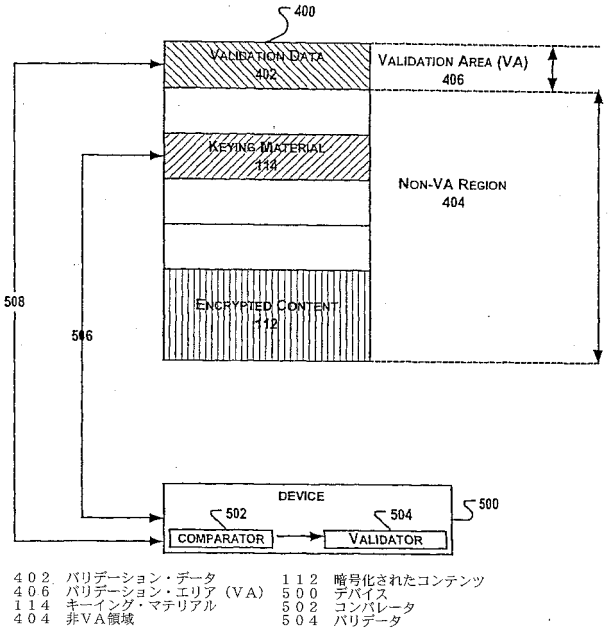
３０２　メディアはバリデーテッド・メディアか
３０６　キーイング・マテリアルを検証する
３０８　キーイング・マテリアルをバリデーション・データと比較する
３１０　対応するか
３０４　キーイング・マテリアルを検証しない
３１２　キーイング・マテリアルを検証する
３１４　キーイング・マテリアルを使用して解読する

【図４】



４０２　バリデーション・データ
４０６　バリデーション・エリア（ＶＡ）
４０４　非ＶＡ領域
１１２　暗号化されたコンテンツ

【図５】



４０２　バリデーション・データ
４０６　バリデーション・エリア（ＶＡ）
１１４　キーイング・マテリアル
４０４　非ＶＡ領域
１１２　暗号化されたコンテンツ
５００　デバイス
５０２　コンパレータ
５０４　バリデータ

【国際公開パンフレット】

(M)60215370071

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 October 2002 (10.10.2002)

PCT

(10) International Publication Number
WO 02/080171 A1

(51) International Patent Classification?: G11B 20/00

(21) International Application Number: PCT/US02/08971

(22) International Filing Date: 22 March 2002 (22.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/822,542 30 March 2001 (30.03.2001) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: TRAW, Brendan; 10859 NW Supreme Court, Portland, OR 97229 (US). RIPLEY, Mike; 1222 NE 56th Court, Hillsboro, OR 97124 (US).

(74) Agents: MALLIE, Michael, J. et al.; Blakely, Sokoloff, Taylor & Zafman, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

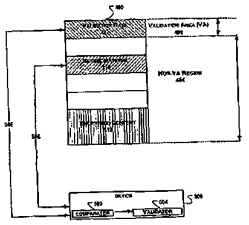
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: VALIDATING KEYING MATERIAL BY USING A VALIDATION AREA OF READ-ONLY MEDIA TO PREVENT PLAYBACK OF UNAUTHORIZED COPIES OF CONTENT STORED ON THE MEDIA



(57) Abstract: In one aspect of the invention is a method for preventing unauthorized copies of a medium, such as a DVD, from being played by a compliant device (500) by using the validation area (VA) (406) region of a medium to validate keying material. A compliant device is a device that will validate (114) keying material. In one embodiment of the invention, a compliant device validates keying material by using the value in the VA region of the medium. In alternative embodiments, a compliant device will validate keying material by checking correspondence between keying material written to a non-VA region (404) of a medium and validation data (412) written to a VA region of a medium. In the alternative embodiments, if the keying material does not correspond to the validation data, then a compliant device will prevent the contents of the medium from being played.

WO 02/080171 A1

VALIDATING KEYING MATERIAL BY USING A VALIDATION AREA OF READ-ONLY MEDIA TO PREVENT PLAYBACK OF UNAUTHORIZED COPIES OF CONTENT STORED ON THE MEDIA

COPYRIGHT NOTICE

FIELD OF THE INVENTION

[0002] This invention relates to static and dynamic information storage and retrieval. More particularly, this invention relates to methods, apparatus and systems for the protection of stored information from unauthorized copying.

BACKGROUND OF THE INVENTION

[0003] Information or content may be stored on a wide variety of media. As the speed and convenience of accessing and copying stored information have increased, the threat of unauthorized copying of the information has increased correspondingly. Various schemes have been employed to protect content stored on read-only media from unauthorized access by storing various types of data in different regions of the medium.

[0004] One such scheme can be illustrated in a medium such as a DVD-ROM (Digital Versatile Disc - Read Only Media), as illustrated in FIG. 1A. The medium 100 comprises a Data Area 102 and a Lead-In Area 104 (hereinafter referred to as a Non- Data Area 104). As further illustrated in FIG. 1B, the Data Area 102 comprises encrypted content 112 (or scrambled content in the case of DVD-Video content protected by the Content Scramble System (CSS)).

[0005] On a DVD-ROM disc that contains DVD-Audio content protected by CPPM, for example, the Control Data Area 110 (CDA 110) stores Keying Material 114 called an Album Identifier (and/or possibly Secure Disk Key Data in the case

of DVD-Video content protected by the Content Scramble System). The Album Identifier is an 8-byte (64-bit) value that is randomly and individually assigned to each album to be protected. The cryptographic key needed to decrypt Encrypted Content 112 that is stored on the Data Area 102 of the medium is dependent on the Album Identifier value. Thus, if the Album Identifier is incorrectly copied to recordable media, for example, the incorrect Album I.D. will cause a player to form an incorrect cryptographic key, thus preventing the recordable medium from being played in a compliant manner.

[0006] For such content protection to be effective, it is ideal that recordable media be designed to prevent the sector that contains the Keying Material 114 (e.g., Album Identifier that is stored in Control Data Area 110, Sector #2 or CDA 110 Sector #2 in the case of a DVD-ROM) from being written such that the Keying Material 114 cannot be copied. However, some forms of recordable media, such as DVD-R (Digital Video Disc - Recordable) and DVD-RW (Digital Video Disc - ReWriteable), which have sectors/layout similar to the DVD-ROM layout depicted in FIGS. 1A and 1B, may contain writeable sector addresses which allow one to record Keying Material 114 in the Data Area 102 and assign it the address of the sector containing the Keying Material 114, such that a player may not be able to distinguish it from legitimate Keying Material 114. Of course, it is also possible that other media (such as non-compliant DVD-Rs and DVD-RWs) may allow the sector that contains the Keying Material 114 to be directly written.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[0008] FIG. 1A depicts a first view of a medium, such as a DVD (Digital Versatile Disc).

[0009] FIG. 1B depicts an alternative view of the medium shown in FIG. 1A.

[0010] FIG. 2 is a flowchart illustrating a method in general embodiments of

the invention.

[0011] FIG. 3 is a flowchart illustrating an alternative method in embodiments of the invention.

[0012] FIG. 4 depicts a layout of a BCA validated medium in accordance with embodiments of the invention.

[0013] FIG. 5 is a conceptual diagram illustrating a system in accordance with embodiments of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0014] In one aspect of the invention, a method for validating Keying Material stored on read-only media, such as a DVD-ROM, by using a Validation Area (VA) region of a medium to validate the authenticity of the Keying Material to prevent the playback of unauthorized copies of content prerecorded on read-only media, is disclosed.

[0015] Keying Material as well as Validation Data used for validating the authenticity of the Keying Material are stored on read-only media. In one embodiment, a Validated Medium (i.e., a medium that comprises and uses a Validation Area to validate Keying Material, to be discussed), comprises Keying Material that may be directly written to the Validation Area of the medium. In this embodiment, Validation Data comprises the Keying Material itself.

[0016] In one alternative embodiment, a Validated Medium comprises Keying Material that may be written to a non-Validation Area (non-VA region) of the medium, and Validation Data related to that Keying Material is created and written to the Validation Area (VA region) of the medium.

[0017] In one variation of this alternative embodiment, Keying Material is written to a non-VA of the medium, and Validation Data comprises a copy of the Keying Material that is written to the VA region of the medium. In another variation, Keying Material is written to a non-VA of the medium, and Validation

Data comprises a function of the Keying Material that is written to the VA region of the medium.

[0018] In embodiments of the invention, a device for playing Validated Media is called a compliant device (hereinafter referred to as "compliant device" or simply "device", where a device that is non-compliant will be referred to as a "non-compliant device").

[0019] In one embodiment, a Validated Medium comprises Keying Material directly written to the VA region of the medium, where the Validation Data comprises the Keying Material, and a compliant device validates the Keying Material without finding correspondence between the Keying Material and the Validation Data by virtue of the Keying Material being in the VA region of the medium. Newer media may comprise Keying Material that is directly written to the VA region of the media, and would rely on compliant devices for playability.

[0020] In an alternative embodiment, a Validated Medium comprises Keying Material on a non-VA region of the medium, and Validation Data related to the Keying Material on the VA region of the medium, and a compliant device may validate the Keying Material without finding correspondence, or, alternatively, by finding correspondence between the Keying Material and the Validation Data as a prerequisite to validation. To preserve compatibility with non-compliant devices (which do not look for Validation Data in the VA region of media), newer media may comprise Keying Material 114 that is written to a non-VA region of a medium (where a non-compliant device would expect to find Keying Material 114, and where a compliant device would look for Keying Material 114 to validate), and write Validation Data to a VA region of a medium (where a compliant device would expect to find data for validating the Keying Material 114 that is in the non-VA region).

[0021] In summary, a compliant device may validate the authenticity of Keying Material in a Validated Medium without checking correspondence where the Keying Material is written to the VA region of the medium, such that the Validation Data comprises the Keying Material itself. It is also contemplated that a compliant device may validate the authenticity of Keying Material in a Validated

Medium without checking correspondence where Validation Data is written to the VA region of the medium, and Keying Material is written to the non-VA region of the medium.

[0022] Where no correspondence is checked, a compliant device relies on the properties of a VA region to establish that the Validation Data contained therein is correct, whether or not it corresponds to Keying Material 114 that may be written to the non-VA region of the medium. The Validation Data in the VA region may be used directly in protection schemes where the Validation Data comprises the Keying Material 114 itself (i.e., newer media relying on compliant devices); where the Validation Data comprises a copy of the Keying Material 114; or where a function exists for translating the Validation Data to the Keying Material 114, for example. At worst, if the Validation Data in the VA is incorrect, the resulting Keying Material 114 will form an incorrect cryptographic key, thereby preventing the content from being played in a compliant manner.

[0023] A compliant device may alternatively validate the authenticity of Keying Material 114 in a Validated Medium by finding correspondence between the Keying Material 114 and the Validation Data where Validation Data is written to the VA region of the medium, and Keying Material 114 is written to the non-VA region of the medium.

[0024] Where correspondence is checked and validated, a compliant device can be confident that there has been no tampering of the Keying Material 114 in the non-VA region of the medium, since it corresponds properly to the Validation data in the VA. If the Keying Material 114 and the Validation Data do not correspond in the latter case, then the compliant device assumes that the medium has been tampered with, and the device will not validate Keying Material 114 so as to prevent playback of the medium.

[0025] The present invention includes various operations, which will be described below. The operations of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the operations.

Alternatively, the operations may be performed by a combination of hardware and software.

[0026] The present invention may be provided as a computer program product which may include a machine-readable medium having stored thereon instructions which may be used to program a computer (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs (Compact Disc-Read Only Memories), and magneto-optical disks, ROMs (Read Only Memories), RAMs (Random Access Memories), EPROMs (Erasable Programmable Read Only Memories), EEPROMs (Electromagnetic Erasable Programmable Read Only Memories), magnetic or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions. Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer (e.g., a server) to a requesting computer (e.g., a client) by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection). Accordingly, herein, a carrier wave shall be regarded as comprising a machine-readable medium.

Terms

[0027] As used throughout this description, the following terms shall be accorded their respective meanings:

VA (Validation Area)

[0028] A VA is a portion of a medium that has physical properties that make it difficult to mimic using ordinary consumer recording equipment/media. A VA requires special manufacturing equipment to write, making its contents difficult to copy. Furthermore, since the VA is read using a physically different process from that used to read the other areas of a medium, a device can physically distinguish contents written to a VA from contents that may have been written by an ordinary recorder on ordinary recordable media. One example of a VA is the Burst Cutting Area of a DVD-ROM.

[0029] It should be understood by one of ordinary skill in the art that the term "VA" or "VA region" is to be construed as an area having the general properties described herein, and that the term "VA" or "VA region" shall not preclude other areas having the properties of a VA described herein from being construed as an equivalent of a VA.

Validated Medium

[0030] A Validated Medium is a medium on which the VA is used to validate Keying Material 114. A Validated Medium comprises Validation Data in the VA region of the medium. In embodiments of the invention, a medium is illegitimate, or unauthorized, if Keying Material 114 in a Validated Medium cannot be validated, as will be discussed further below.

[0031] A non-Validated Medium is merely a medium that does not comprise Validation Data in the VA region, but does not imply that the medium is an illegitimate, or unauthorized medium. In embodiments of the invention, a non-Validated Medium is played by a compliant device (as well as a non-compliant device) so as to preserve compatibility between compliant devices and legitimate, older media. These embodiments encourage consumers to buy newer devices, which will still play older media, but which will also prevent illegitimate discs from being played. Of course, it is also contemplated that compliant devices may prevent non-Validated Media from being played.

Keying Material

[0032] Keying Material 114 comprises value(s) on which access to protected content depends. In content protected by CSS (to be discussed), Keying Material 114 may comprise Secure Disc Key Data; and in content protected by CPPM (to be discussed), Keying Material 114 may comprise an Album Identifier. Typically, the value is used as a key, or is used to form a cryptographic key, for decrypting encrypted content 112. While the value may be unique for every medium, it is typically unique for some set of media.

Validation

[0033] Keying Material 114 is validated when it is used to decrypt encrypted content 112 (or form the cryptographic key needed to decrypt content), thereby allowing playback of the read-only content.

[0034] Where correspondence is checked prior to validation, Keying Material 114 from the non-VA region of the medium is used if correspondence is found.

[0035] Where no correspondence is checked for validation, Keying Material 114 used to decrypt the encrypted content is derived from Validation Data. Where the Validation Data comprises the Keying Material 114 (i.e., they are one and the same), or where the Validation Data is a copy of the Keying Material 114 in the non-VA region, the Keying Material 114 is derived from the Validation Data by using the Validation Data itself.

[0036] In other cases, Keying Material 114 may be derived from the Validation Data by converting the Validation Data to the original Keying Material. For example, in some embodiments (such as in content protection schemes like CSS, to be discussed), Validation Data is a function of Keying Material 114, such that to use the original Keying Material 114 to decrypt the content, the same cryptographic function is used on the validation Data to form the original Keying Material 114.

Device

[0037] A device is any mechanism for playing back content on a read-only medium. For DVDs, such a mechanism comprises a DVD playback device, which may be a DVD player, or a DVD drive, for example.

Compliant Device

[0038] A compliant device is a device that will play a Validated Medium.

Introduction

[0039] Generally, as shown in the flowchart of FIG. 2, which begins at block 200, a compliant device playing a Validated Medium validates the Keying Material 114 in one of two ways. The compliant device may validate the Keying Material

114 by using Validation Data in the VA, shown in block 202, where the Validation Data may comprise the Keying Material 114 in the VA region; a copy of the Keying Material 114 in the non-VA region; or a function of Keying Material 114 that is written to the non-VA region (in which case the Validation Data is first subject to a function prior to being used to decrypt content, as discussed above). In the rare, or unlikely case that the Validation Data comprises some other value which will produce an incorrect cryptographic key, or does not comprise a value at all, a compliant device may still "validate" the Keying Material and use the value in the VA region, but an incorrect/invalid value in the VA region will prevent the content from being played.

[0040] Alternatively, a compliant device may compare Keying Material 114 written to a non-VA region of the medium to Validation Data written to a VA region of the medium, as shown in block 204. In block 206, it is determined if the Keying Material 114 and the Validation Data correspond. If they do not correspond, then the device does not validate the Keying Material 114 in block 208, thereby preventing the Keying Material 114 from being used to decrypt the encrypted content 112, and thereby preventing playback of the content. If the Keying Material 114 and the Validation Data 402 correspond, then in block 210, the device validates the Keying Material 114, allowing it to be used for decrypting the encrypted data 112. The method ends at block 212.

[0041] Given embodiments of this invention, the following outlines the different scenarios that may exist for playing media:

[0042] 1. Validated Medium is played on a compliant device: compliant devices recognize the VA region of a medium, and will therefore look for Validation Data in the VA. Keying Material 114 may be automatically validated, as shown in block 202 of FIG. 2 in newer media that rely solely on compliant devices, or where a particular implementation trusts the VA properties of the medium. Other implementations may choose to find correspondence between the Validation in the VA and Keying Material 114 in the non-VA prior to validating the Keying Material 114, as shown in block 206 of FIG. 2.

[0043] 2. Validated Medium is played on a non-compliant device: non-

compliant (i.e. older) devices may not recognize the VA region of a medium, or may simply not be designed to look for Validation Data in the VA. Such devices will use the Keying Material 114 in the non-VA region of the medium to decrypt the content in accordance with previous methods for decrypting.

[0044] 3. Non-Validated Medium is played on a compliant device: a compliant device will look for, but not find a BCA containing Validation Data. The device will, in this case, use the Keying Material 114 in the non-VA region to decrypt the content in accordance with previous methods for decrypting. (As discussed above, the device may alternatively prevent playback of the content on the medium.)

[0045] 4. Non-Validated Medium is played on a non-compliant device: a non-compliant device will use the Keying Material 114 in the non-VA region to decrypt the content in accordance with previous methods for decrypting.

[0046] In scenarios 2 and 4, a non-compliant device will not prevent the playback of unauthorized copies of media. In scenarios 2 and 3, prevention of unauthorized copies cannot be implemented with a Validated Medium or with a compliant device, but interoperability between new devices and old media (scenario 3), as well as old devices and new media (scenario 2), is maintained. To preserve compatibility with old devices and old media, the method of FIG. 2 can be modified as shown in FIG. 3, beginning at block 300.

[0047] At block 302, a determination is made as to whether the medium being read is a Validated Medium (the determination to be discussed in further detail). If the medium is not a Validated Medium, then at block 314 the compliant device does not look for Validation Data, but instead simply uses the Keying Material 114 in the non-BCA region of the medium to decrypt the content in accordance with previous methods for decrypting. This determination preserves interoperability between compliant devices and non-BCA validated media, such that if the medium being read is not a Validated Medium, then the compliant device will not necessarily prevent the non-Validated Medium from being played.

[0048] At blocks 306 and 308, the medium is determined to be a Validated

Medium. The compliant device may validate the Keying Material 114 by using the Validation Data in the VA (in certain cases, as discussed above), as shown in block 306. Since the VA has the special properties that make its contents difficult to copy, the compliant device has a certain degree of confidence that the data in the VA has not been tampered with.

[0049] The compliant device may alternatively validate the Keying Material 114 by comparing the Keying Material 114 in the non-VA region of the medium to the Validation Data in the VA of the medium, shown in block 308. Continuing to store Keying Material 114 in the non-VA region of the medium can be a means of preserving interoperability between Validated Media and non-compliant devices such that if a Validated Medium is read by a non-compliant device, which expects to find the Keying Material 114 in the non-VA of a given medium, the non-compliant device will not error out. Thus, a non-compliant device will look for Keying Material 114 in the non-VA of the medium and use that value to decrypt the content. A non-compliant device, however, has no mechanism for validating the authenticity of the Keying Material 114, even if the medium is a Validated Medium.

[0050] A compliant device, on the other hand, can validate the authenticity of the Keying Material 114 written to a Validated Medium. At block 310, a determination is made as to whether the Keying Material 114 corresponds to the Validation Data. If there is no correspondence (correspondence to be discussed), then at block 304 the compliant device does not validate the Keying Material 114, thereby preventing playback of the content. At block 312, if there is correspondence, then the compliant device validates the Keying Material 114. The method ends at block 316.

[0051] By embodiments of this invention, BCA validated media can prevent hackers from copying Keying Material 114 (and/or its associated Validation Data) that is stored on a DVD-ROM onto a DVD-R, for example, thereby making an unauthorized copy of the DVD-ROM on the DVD-R unplayable. On non-Validated Media, such as a non-Validated DVD, hackers can do this, for example, by:

[0052] • Writing Keying Material 114 to the Data Area 102 of the DVD-R

(specifically, the User Data Area of the DVD-R), but assigning it an address within the CDA 110 of the DVD-ROM such that a device cannot distinguish it from legitimate Keying Material 114 found on the original DVD-ROM.

[0053] • Directly writing valid Keying Material 114 from the DVD-ROM onto the CDA 110 of a non-compliant DVD-R disc.

[0054] As illustrated in FIG. 4, therefore, a Validated Medium 400 comprises a Validation Area 406 (VA) region and a non-VA region 404, where the VA region comprises Validation Data 402, and the non-VA region 404 comprises Encrypted Content 112. In some embodiments, the non-VA region 404 may additionally comprise Keying Material 114.

Exemplary Embodiments

[0055] Examples of media comprising a Validation Area 406 include DVD-ROMs (DVD-Read Only Memories). Several exemplary embodiments are described herein with reference to DVD media. Specifically, concepts related to this invention are described in relation to the following exemplary embodiments:

[0056] • DVD Content Protected By CPPM

[0057] • DVD Content Protected By CSS

[0058] • DVD Content Protected By CPPM/CSS

[0059] While these particular embodiments are described, it should be understood by one of ordinary skill in the art that the invention is not intended to be limited to these particular embodiments, and that general concepts of the invention are applicable to various embodiments not discussed herein.

[0060] The current state of these embodiments is discussed in this section ("Exemplary Embodiments"). General concepts of the invention as they relate to these exemplary embodiments are described in subsequent sections. Where appropriate, or where helpful to understanding the invention, the general concepts of the invention are illustrated with reference to these exemplary embodiments.

DVD Content Protected By CPPM

[0061] The Content Protection For Prerecorded Media (CPPM) specification defines a robust and renewable method for protecting content distributed on prerecorded (read-only) media types. In one exemplary embodiment, a specification is defined for using CPPM technology to protect DVD-Audio content distributed on read-only DVD (DVD-ROM) discs.

[0062] Generally, each CPPM compliant DVD-Audio playback device (such as a hardware DVD player, or a software player used in conjunction with a computer equipped with a DVD drive) is given a set of 16 Device Keys denoted K_{d_0}, K_{d_1}, ..., K_{d_15}. These keys are provided by the 4C Entity, LLC, and are for use in processing the MKB (Media Key Block) to calculate the Media Key (K_m). Key sets may either be unique per device, or used commonly by multiple devices.

[0063] Each side of a disc with CPPM protected DVD-Audio content contains:

[0064] • Keying Material 114 called an Album Identifier (ID_{album}) prerecorded in the Lead-In Area 104 (specifically, the Non-User Data Area).

[0065] • A Media Key Block (MKB) prerecorded as a specific file in the Data Area 102.

[0066] •Encrypted Content 112 prerecorded as specific files in the Data Area 102.

[0067] For purposes of this invention, the Album Identifier is described in further detail below; however, since the MKB and Encrypted Content 112 concepts are not pertinent to embodiments of this invention other than as described above, they are not discussed any further. For a detailed explanation of how an Album Identifier is used in conjunction with a Media Key Block to prevent unauthorized copying of content protected by CPPM, one can refer to the document entitled "CONTENT PROTECTION FOR PRERECORDED MEDIA SPECIFICATION, DVD BOOK" published by the 4C Entity, LLC, Revision 0.93, dated January 31, 2001.

[0068] Each side of a disc with CPPM Protected DVD-Audio content

contains a 64-bit Album Identifier (ID_{album}), which is placed in the Non-Data Area 104 by the disc manufacturer. Specifically, the Album Identifier is placed in bytes 80 through 87 of Control Data Area 110 Sector #2. The most significant 8 bits of the Album Identifier (stored in byte 80) are currently defined to have a value of zero. For forward compatibility, a non-zero value in these 8 bits is not considered an error. For the remaining 56 bits, the content provider individually assigns a secret, unpredictable (e.g., random) value to each DVD-audio album to be protected using CPPM. At the content provider's option, all pressings of a given album may contain the same ID_{album} value, or different values may be assigned for different pressings.

[0069] The role of the Album Identifier is not that of individual media identification. Rather, it serves as an album-specific value that is integrated into CPPM cryptographic key management, and placed in a location that is not writeable on compliant DVD recordable-rewriteable media. In a PC (personal computer) system, the Album Identifier is accessed using the DVD drive authentication protocol. For consistency with other non-CPPM uses of that protocol, the confidentiality of the data in Control Data Area 110 Sector #2, including the Album Identifier value, should be maintained.

DVD Content Protected By CSS

[0070] Content Scramble System (CSS) is a data scrambling and authentication scheme intended to prevent copying DVD-Video files directly from the disc.

[0071] The CSS scrambling algorithm exchanges keys with the drive unit to generate an encryption key that is then used to obfuscate the exchange of disc keys and title keys that are needed to descramble data from the disc. DVD players have CSS circuitry that decrypts the data before it's decoded and displayed. On the computer side, DVD decoder hardware and software must include a CSS decryption module. All DVD drives have extra firmware to exchange authentication and decryption keys with the CSS module in the computer.

DVD Content Protected By CPPM/CSS

[0072] On combination discs that include both CPPM and CSS content, the CDA 110 contains not only the CPPM Album Identifier, but also the Secure Disc Key Data, which must be kept secret.

Determining If A Medium Is A BCA Validated Medium

[0073] As used herein, media which uses the Validation Area 406 to validate Keying Material 114 is referred to as Validated Media 400. There are various methods for determining if a medium is a Validated Medium 400. For example, in one embodiment of the invention, a medium is a prerecorded DVD with CPPM protected content. In DVD's, the VA region 406 of the media is referred to as the Burst Cutting Area (BCA), and where the DVD uses the CPPM protection scheme, Keying Material 114 comprises an Album Identifier. The Album Identifier is written to a non-BCA region, specifically the Control Data Area 110 of the Lead-in Area 104. As mentioned previously, the Album Identifier is an 8-byte (64-bit) value. Under the current state of the art, the most significant 8 bits are set to 0.

[0074] To implement embodiments of the invention using DVD protected by CPPM, the most significant 8 bits are used to indicate that a medium is a Validated Medium 400 by setting any one or more of those bits to 1. Thus, when a device determines whether a CPPM protected medium is a Validated Medium 400, it examines the Album Identifier to determine if its most significant bit, for example, is set to 1. If it is, then the device is triggered to look for Validation Data 402 in the Validation Area 406 (specifically, the BCA) of the medium 400. Otherwise, the medium is not a Validated Medium 400, and the device will simply use the Keying Material 114 in the non-VA region of the medium to decrypt the content in accordance with previous methods.

[0075] In other embodiments, such as where Secure Disc Key Data is written to the non-VA region of a medium, other methods may be used to determine if the medium is a Validated Medium 400. Generally, some sort of trigger is used, which would typically involve setting some data item that is

currently reserved or unused to a value other than its currently defined value. In embodiments of the invention, the data item that is used as a trigger is integrated with the Keying Material 114, such that a compliant device can also determine whether the trigger value has been tampered with when validating the Keying Material 114.

[0076] For example, in content protected by CPPM, since the cryptographic key for decrypting content is dependent on the Album Identifier, any attempt to tamper with the Album Identifier will prevent it from producing the correct cryptographic key, thereby preventing the content from being played. Thus, if a hacker tries to thwart the scheme by flipping the most significant bit from 1 to 0 (in reference to the example above), the hacker will also change the Album Identifier. Although a compliant device will bypass validation, it will still use the Album Identifier in an attempt to decrypt the content, but since the Album Identifier has been tampered with, it will not produce the correct key for decrypting the content.

Keying Material

[0078] Keying Material 114 is a value or set of values that is written to a medium 100, 400 containing protected content, and upon which access to the content depends. For example, on DVD-Audio media protected by CPPM (Content Protection For Prerecorded Media), Keying Material 114 comprises an Album Identifier, which is an 8-byte (64-bit) value that is assigned individually and randomly to each album to be protected, and which is used in forming the cryptographic key needed to decrypt content on the medium, discussed *supra*. On DVD-Video media protected by CSS (Content Scramble System), Keying Material 114 comprises Secure Disc Key Data. On Media using a combination CSS/CPPM protection scheme, both an Album Identifier and Secure Disc Key Data are present.

[0079] Keying Material 114 that is used to decrypt content (either by using it directly, or by forming a cryptographic function to decrypt the content) can be derived from the Validation Data that is in the VA region, or it can be used directly from the non-VA region, as explained in the section entitled "Validation", *supra*.

Validation Data

[0080] Validation Data 402 is data that enables a playback device to verify that the Keying Material 114 read from the medium is authentic (i.e. is not an unauthorized copy written using widely available recording equipment and recordable media).

[0081] The nature and location of the Validation Data 402 varies depending upon the type of protection enabled for a given Validated Medium 400. In some cases, the Validation Data 402 may comprise the Keying Material 114 itself, and in other cases, the Validation Data 402 may comprise a copy of the Keying Material 114, or a cryptographic function of the Keying Material 114. Examples follow for each of the exemplary embodiments discussed above. In embodiments of the invention described herein, Validation Data 402 is written to the VA region 406 of a medium.

DVD Content Protected By CPPM

[0082] On Validated Media protected by CPPM where the Keying Material 114 comprises an Album Identifier, the Validation Data 402 comprises a copy of the Album Identifier.

DVD Content Protected By CSS or CPPM/CSS

[0083] On Validated Media where content is protected by CSS, and where content is protected by a combination scheme of CPPM/CSS, the Secure Disc Key Data are to be kept secret. Consequently, all values in CDA 110 sectors containing Secure Disc Key Data (possibly including sector #2 containing the Album Identifier) must be secret, due to the way that the sectors are scrambled during transfer from drive to host, for instance. However, storing a copy of the Album Identifier in the VA region 406 would make the value of the Secure Disc Key Data obvious (where a combination CPPM/CSS scheme is used), since the standard drive interface permits the BCA region 406 to be read in the clear.

[0084] Thus, in the case of content protected by CSS, where the Keying Material 114 comprises Secure Disc Key Data, the Validation Data 402 comprises

a function on the Secure Disc Key Data. Where content is protected by a combination scheme, and the Keying Material 114 comprises both the Album Identifier and Secure Disc Key Data, Validation Data 402 comprises a function on the Album Identifier, as well as a function on the Secure Disc Key Data.

[0085] By using a one-way cryptographic function on a value to create the Validation Data 402, rather than using the given value itself, the value is prevented from being discovered by reading the VA region 406. At the same time, it permits devices to compare the Validation Data 402 in the BCA region 406 to the Keying Material 114 in the CDA 110, as described below in the section entitled "Determining Correspondence".

Other Content Protection Formats

[0086] New content protection formats and schemes for reading media can be designed by simply placing Keying Material 114 in the VA region of the medium, such that the Validation Data 402 comprises the Keying Material 114. Since the VA region has special properties that make mimicking that region very difficult, compliant devices can have a high degree of confidence that the data in the VA region has not been tampered with.

[0087] Alternately, new formats might be designed with Keying Material in the non-VA region of the medium, and Validation Data (possibly a copy of the Keying Material itself) in the BCA. This approach would allow providers of content on the new format to choose whether or not to include the Validation Data in the BCA (i.e. a trade-off between increased protection against unauthorized copies, versus the added manufacturing cost of including the BCA).

Determining Correspondence

[0088] As shown in FIG. 5, correspondence relates to whether a device 500 can validate Keying Material 114 by comparing the Keying Material 114 written to the non-VA region of a medium to Validation Data 402 in the VA region of the medium. In embodiments of the invention, correspondence is determined where Keying Material 114 is placed in non-VA region 404 of the medium, rather than just placing it in the more secure VA region 406, and where the scheme for a

given compliant device does not automatically validate Validation Data 402 written to the VA region 406.

[0089] Assuming a compliant device, and a BCA validated medium 400 in one embodiment described above, the device 500 retrieves 506 the Keying Material 114 from the non-VA region 404 (e.g. the Control Data Area 110 of the Lead-in Area 104 on a DVD), and also retrieves the Validation Data 402 from the VA region 406.

[0090] A comparator 502 in the device 500 compares the Keying Material 114 to the Validation Data 402. If the values correspond, then a validator 504 in the device 500 validates the authenticity of the Keying Material 114, allowing the Keying Material 114 to be used for decrypting the content 112. Although the comparator 502 and the validator 504 are shown as separate entities in the device 500, it should be understood by one of ordinary skill in the art that such a depiction is for illustrative purposes only, and that the functionality may be combined into a single entity, and may alternatively be an entity distinct from the device itself.

[0091] Correspondence between Keying Material 114 and Validation Data 402 can be determined in a number of ways, depending upon the type of Keying Material 114 and Validation Data 402 used in a particular embodiment. Examples of making this determination in exemplary embodiments of the invention are described below.

DVD Content Protected by CPPM

[0092] For content protected by CPPM, correspondence exists between the Keying Material 114 and the Validation Data 402 if the Album Identifier in the non-VA region 404 (e.g., the Control Data Area 110 on a DVD) matches a copy of the Album Identifier in the BCA region 406. If the two values match, as determined by the comparator 502, then the device 500 validator 504 authenticates the Album Identifier, which can then be used to decrypt the medium content 112.

DVD Content Protected by CSS

[0093] For content protected by CSS, correspondence exists between the Keying Material 114 and the Validation Data 402 if a function of the Secure Disc Key Data in the non-VA region 404 (e.g., the Control Data Area 110 on a DVD) matches Validation Data 402 (i.e., a function of the Secure Disc Key Data) in the VA. A one-way cryptographic function, for example, of one of the Secure Disc Key Data values from the CDA 110 is written to the VA region 406, such that when a device 500 reads the Secure Disc Key Data value from the non-VA region 404, it uses the same one-way cryptographic function on that value.

[0094] The device 500 compares the calculated value as determined by the comparator 502, for example, and compares it to the Validation Data found in the VA region 406. If the values match, then the device 500 validator 504 authenticates the Secure Disc Key Data values, which can then be used to decrypt the medium content 112.

DVD Content Protected by CPPM/CSS

[0095] For content protected by a combination of CPPM/CSS, correspondence exists between the Keying Material 114 and the Validation Data 402 if a function of the Album Identifier in the non-VA region 404 (e.g., the Control Data Area 110 on a DVD) matches Validation Data 402 (i.e., function of the Secure Disc Key Data and function of the Album Identifier) in the VA. A one-way cryptographic function of one of the Album Identifier from CDA 110 Sector #2, and a one-way cryptographic function of the Secure Disc Key Data are written to the BCA region 406, such that when a device reads the Album Identifier and the Secure Disc Key Data from the CDA, it uses the same one-way cryptographic function on those values.

[0096] The device 500 calculates the function on the Album Identifier and on the Secure Disc Key Data from the non-BCA region 404 and compares the calculated values to the Validation Data found in the BCA region 406. If the values match, then the device 500 validator 504 authenticates the Album Identifier and Secure Disc Key Data, which can then be used to decrypt the medium content 112.

Conclusion

[0097] Thus, embodiments of the invention provide a robust means of validating Keying Material 114 to protect content, such as prerecorded CPPM or CSS content on DVD-ROM media, against unauthorized copying. The enhanced protection is enabled by new discs and new devices that use the invention. At the same time, full interoperability among new and old devices, and new and old media is maintained.

[0098] In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

[0099] For example, while several exemplary embodiments have been described, it should be understood by one of ordinary skill in the art that concepts of this invention can be applied to other types of content, content protection systems, and media formats. For example, while the exemplary embodiments described herein are specific to DVD media as they relate to some of their current forms of protection (i.e. CPPM, CSS), one of ordinary skill in the art would understand that the read-only media described herein comprises a VA region and a non-VA region, and may not necessarily comprise all regions found in a DVD media.

[00100] Furthermore, while embodiments of the invention described herein refer to an area called the Validation Area, it should be understood that the Validation Area is an area having characteristics described herein, and that such an area is not limited to areas that are called, or that contain the term, Validation Area. As an example, DVD-ROMs comprise a Validation Area called a Burst Cutting Area.

[00101] While a one-way cryptographic function is discussed herein, it is also contemplated that a two-way cryptographic function may be used. For example, where no correspondence is checked, and Validation Data comprises a function of

Keying Material, a two-way cryptographic function may be used which would convert the Validation Data back to its original Keying Material.

WHAT IS CLAIMED IS:

1. A method comprising:

reading validation data from a validation area (VA) region of a medium having encrypted content;

determining keying material used to decrypt the encrypted content by deriving the keying material from the validation data; and

using the keying material to decrypt the encrypted content.

2. The method of claim 1, wherein the keying material is derived from the validation data by using the validation data itself where the validation data comprises the keying material.

3. The method of claim 1, wherein the keying material is derived from the validation data by using the validation itself where the validation data is a copy of the keying material that is written to the non-VA region of the medium.

4. The method of claim 3, wherein the medium uses CPPM (Content Protection For Prerecorded Media) format to protect the content, and:

the keying material comprises an album identifier that is written to the non-VA region of the medium; and

the validation data comprises a copy of the album identifier.

5. The method of claim 1, wherein the keying material is derived from the validation data by converting the validation data in the VA region into the keying material in the non-VA region.

6. The method of claim 5, wherein the converting the validation data into the keying material comprises using a function for converting the validation

data into the keying material, the reverse function having been used to create the validation data from the keying material.

7. The method of claim 6, wherein the medium uses CSS (Content Scramble System) format to protect the content, and:

the keying material comprises Secure Disc Key Data that is written to the non-VA region of the medium; and

the validation data comprises a cryptographic function on the Secure Disc Key Data.

8. The method of claim 6, wherein decrypting the encrypted content comprises using the keying material to form a cryptographic key to decrypt the encrypted content.

9. The method of claim 6, wherein the medium comprises a DVD (Digital Versatile Disc), and the VA comprises a burst cutting area of the DVD.

10. A method comprising:

determining if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium;

if the medium is a Validated Medium, determining keying material used to decrypt the encrypted content by deriving the keying material from the validation data; and

validating the keying material.

11. The method of claim 10, wherein said determining if the validation data exists in the VA region comprises determining if a trigger has been set.

12. The method of claim 11, wherein said determining if the trigger has been set comprises determining if the most significant bit of the keying material is set to 1.

13. The method of claim 10, wherein the keying material is derived from the validation data by using the validation data itself where the validation data comprises the keying material.

14. The method of claim 10, wherein the keying material is derived from the validation data by using the validation itself where the validation data is a copy of the keying material that is written to the non-VA region of the medium.

15. The method of claim 10, wherein the keying material is derived from the validation data by converting the validation data in the VA region into the keying material in the non-VA region.

16. The method of claim 10, wherein the medium comprises a DVD (Digital Versatile Disc), and the VA comprises a burst cutting area of the DVD.

17. A method comprising:

determining if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium, the medium additionally having keying material written to a non-VA region of the medium;

if the medium is a Validated Medium, determining if the validation data and the keying material correspond; and

if the validation data and the keying material correspond, using the keying material in the non-VA region to decrypt the encrypted content.

18. The method of claim 17, wherein said determining if the medium is a Validated Medium comprises determining if a trigger has been set.

19. The method of claim 18, wherein said determining if the trigger has been set comprises determining if the most significant bit of the keying material is set to 1.

20. The method of claim 17, wherein the medium comprises a DVD-ROM (Digital Video Disc - Read Only Memory).

21. The method of claim 17, wherein said determining if the validation data and the keying material correspond comprises determining if the validation data and the keying material match.

22. The method of claim 21, wherein the medium uses CPPM (Content Protection For Prerecorded Media) format to protect the content, and:

the keying material comprises an album identifier that is written to the non-VA region of the medium; and

the validation data comprises a copy of the album identifier.

23. The method of claim 17, wherein said determining if the validation data and the keying material correspond comprises determining if a cryptographic function on the keying material matches the validation data.

24. The method of claim 23, wherein the medium uses CSS (Content Scramble System) format to protect the content, and:

the keying material comprises Secure Disc Key Data that is written to the non-VA region of the medium; and

the validation data comprises a cryptographic function on the Secure Disc Key Data.

25. The method of claim 17, wherein the medium comprises a DVD (Digital Versatile Disc), and the VA comprises a burst cutting area of the DVD.

26. A method comprising:

determining if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium; and

if the medium is a Validated Medium, then performing one of the following:

determining keying material used to decrypt the encrypted content by deriving the keying material from the validation data, and then validating the keying material; and

determining if the validation data and the keying material correspond, and validating the keying material if the validation data corresponds to the keying material.

27. The method of claim 26, wherein the keying material is derived from the validation data by using the validation data itself where the validation data comprises the keying material.

28. The method of claim 26, wherein the keying material is derived from the validation data by using the validation itself where the validation data is a copy of the keying material that is written to the non-VA region of the medium.

29. The method of claim 26, wherein the keying material is derived from the validation data by converting the validation data in the VA region into the keying material in the non-VA region.

30. The method of claim 26, wherein the medium comprises a DVD-ROM (Digital Video Disc - Read Only Memory).

31. The method of claim 26, wherein the VA comprises a burst cutting area.

32. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

determine if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium; and

if the medium is a Validated Medium, then perform one of the following:

determine keying material used to decrypt the encrypted content by deriving the keying material from the validation data, and then validate the keying material; and

determine if the validation data and the keying material correspond, and validate the keying material if the validation data corresponds to the keying material.

33. The machine-readable medium of claim 32, wherein the encrypted content is protected using CPPM (Content Protection for Prerecorded Media) format, and the keying material comprises an album identifier, and the validation data comprises a copy of the album identifier.

34. The machine-readable medium of claim 32, wherein the content is protected by CSS (Content Scrambling System), and:

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

35. An apparatus comprising:

at least one processor; and

a machine-readable medium having instructions encoded thereon, which when executed by the processor, are capable of directing the

processor to:

determine if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium; and

if the medium is a Validated Medium, then perform one of the following:

determine keying material used to decrypt the encrypted content by deriving the keying material from the validation data, and then validate the keying material; and

determine if the validation data and the keying material correspond, and validate the keying material if the validation data corresponds to the keying material.

36. The apparatus of claim 35, wherein the encrypted content is protected using CPPM (Content Protection for Prerecorded Media) format, and the keying material comprises an album identifier, and the validation data comprises a copy of the album identifier.

37. The apparatus of claim 35, wherein the content is protected by CSS (Content Scrambling System), and:

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

38. An apparatus comprising:

means for determining if a medium having encrypted content is a Validated Medium by determining if validation data exists in a validation area (VA) region of the medium; and

if the medium is a Validated Medium, then means for performing one of the following:

determining keying material used to decrypt the encrypted content by deriving the keying material from the validation data, and then validating the keying material; and

determining if the validation data and the keying material correspond, and validating the keying material if the validation data corresponds to the keying material.

39. The apparatus of claim 38, wherein the encrypted content is protected using CPPM (Content Protection for Prerecorded Media) format, and the keying material comprises an album identifier, and the validation data comprises a copy of the album identifier.

40. The apparatus of claim 38, wherein the content is protected by CSS (Content Scrambling System), and:

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

41. An apparatus comprising:

encrypted content; and

keying material; and

validation data written to a validation area (VA) region of the medium, the validation data being used to validate the authenticity of the keying material.

42. The apparatus of claim 41, wherein the encrypted content uses Content Protection For Prerecorded Media (CPPM) format, and the validation data

comprises an album identifier that is used to form a cryptographic key for decrypting the content.

43. The apparatus of claim 41, wherein the keying material is written to a non-VA region of the medium.

44. The apparatus of claim 41, wherein the apparatus comprises a DVD-ROM (Digital Video Disc - Read Only Memory).

45. The method of claim 41, wherein the VA comprises a burst cutting area.

46. An apparatus, comprising:

a first module to determine if validation data exists in a validation area (VA) region of a medium, the medium having keying material for decrypting encrypted content on the medium, and the validation data being used to validate the authenticity of the keying material; and

a second module to process the medium, if validation data exists in the VA region, by performing one of the following:

using keying material derived from the VA region of the medium to decrypt the encrypted content; and

finding correspondence between the validation data and the keying material, and if correspondence is found, using the keying material to decrypt the encrypted content.

47. The apparatus of claim 46, wherein the first module determines if validation data exists in a VA region of the medium by determining if a trigger is set.

48. The apparatus of claim 47, wherein the trigger is set if the most significant bit of the keying material is set to 1.

49. The apparatus of claim 46, wherein the validation data corresponds to the keying material if the keying material matches the validation data.

50. A system comprising:

a medium having:

encrypted content;

keying material; and

validation data written to a VA region of the medium.

a device coupled to the medium to play the encrypted content by performing one of the following:

using the keying material derived from the VA region of the medium to decrypt the encrypted content; and

determining if the validation data corresponds to the keying material, and if the validation data corresponds to the keying material, then using the keying material to decrypt the encrypted content.

51. The system of claim 50, wherein the content is protected by CPPM (Content Protection For Prerecorded Media), and the keying material has an album identifier that is used to form a cryptographic key for decrypting the content.

52. The system of claim 50, wherein the content is protected by CSS (Content Scrambling System), and:

the keying material comprises Secure Disc Key Data; and

the validation data comprises a function on the Secure Disc Key Data.

53. A system comprising:

a medium having:

encrypted content; and

keying material; and

a device coupled to the medium to decrypt the encrypted content if the

medium is a Validated Medium, and the authenticity of the keying material is validated.

54. The system of claim 53, wherein the authenticity of the keying material is validated by one of the following:

using the keying material derived from the VA region of the medium; and

determining that the validation data corresponds to the keying material.

55. The system of claim 54, wherein the validation data corresponds to the keying material if the keying material matches the validation data.

56. The system of claim 54, wherein the validation data corresponds to the keying material if a function of the keying material matches the validation data.

57. The system of claim 53, wherein the medium comprises a DVD-ROM (Digital Video Disc - Read Only Memory).

58. The method of claim 53, wherein the VA comprises a burst cutting area.

59. The system of claim 53, wherein said determining if the validation data exists in the VA region comprises determining if a trigger has been set.

60. The system of claim 59, wherein said determining if the trigger has been set comprises determining if the most significant bit of the keying material is set to 1.

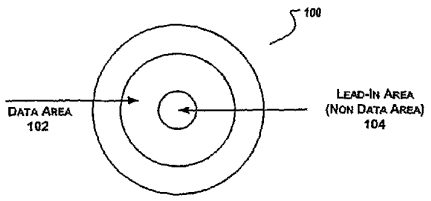

100
DATA AREA
102
LEAD-IN AREA
(NON DATA AREA)
104

FIG. 1A

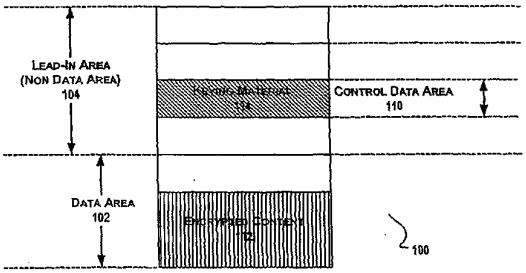

LEAD-IN AREA
(NON DATA AREA)
104
CONTROL DATA AREA
110
DATA AREA
102
100

FIG. 1B

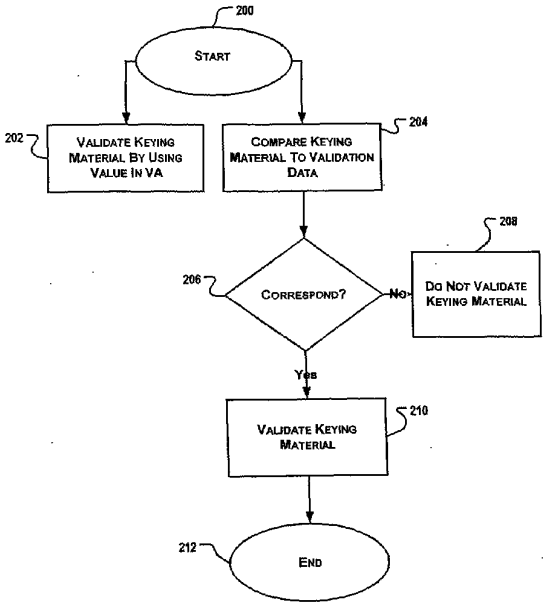

200
START
202
VALIDATE KEYING MATERIAL BY USING VALUE IN VA
204
COMPARE KEYING MATERIAL TO VALIDATION DATA
206
CORRESPOND?
No
208
DO NOT VALIDATE KEYING MATERIAL
Yes
210
VALIDATE KEYING MATERIAL
212
END

FIG. 2

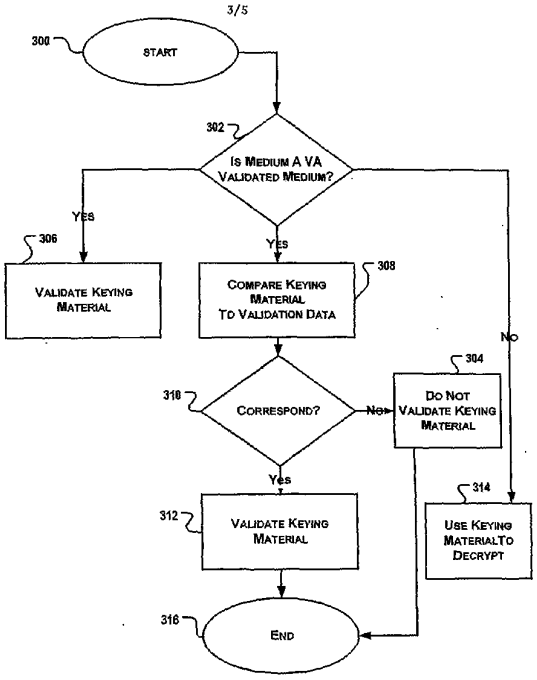

300
START
302
IS MEDIUM A VA VALIDATED MEDIUM?
YES
YES
No
306
VALIDATE KEYING MATERIAL
308
COMPARE KEYING MATERIAL TO VALIDATION DATA
310
CORRESPOND?
No
304
DO NOT VALIDATE KEYING MATERIAL
Yes
312
VALIDATE KEYING MATERIAL
314
USE KEYING MATERIAL TO DECRYPT
316
END

FIG. 3

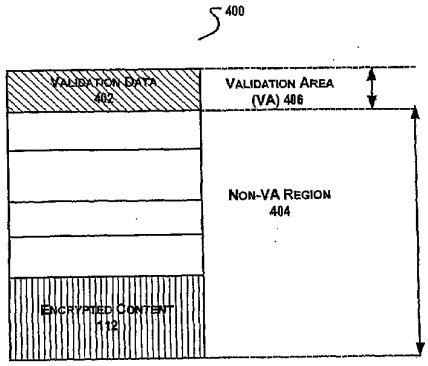

400
VALIDATION DATA 402
VALIDATION AREA (VA) 406
NON-VA REGION 404
ENCRYPTED CONTENT 712

FIG. 4

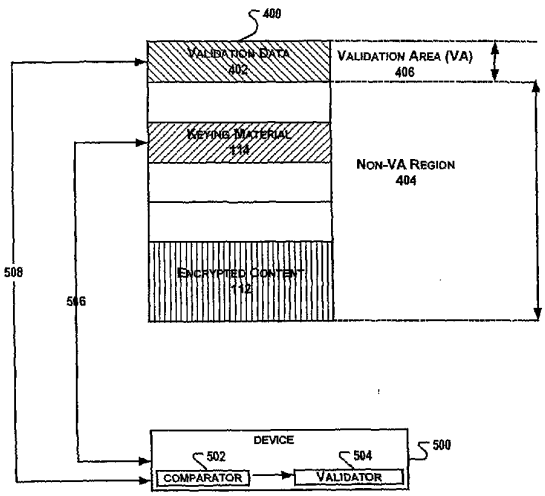

400
VALIDATION DATA
402
VALIDATION AREA (VA)
406
KEYING MATERIAL
114
NON-VA REGION
404
ENCRYPTED CONTENT
112
508
506
DEVICE
500
502
504
COMPARATOR
VALIDATOR

FIG. 5

【国際調査報告】

［書類名］国際公開パンフレット ［受付日］平14.10.17 平15.12.18 15:04
PCT/US02/08971 ［特許］特願2002-578501(平14.03.22) 8884

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/08971

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	INTEL CORPORATION ET AL: "Content Protection for Recordable Media Specification: DVD Book, Revision 0.94" 4C ENTITY, 18 October 2000 (2000-10-18), XP002167964	1,5,6, 8-10, 15-17, 23,25, 26,29, 31,32, 35,38, 41,43, 45,46, 50,53, 54,56,58
Y	page 4.1 -page 6.10	2,3,13, 14,21, 27,28, 49,55
A		4,7,22, 24,33, 34,36, 37,39,

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 June 2002	28/06/2002
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL- 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Ogor, M

(L)60301800135

［書類名］国際公開パンフレット ［受付日］平14.10.17 平15.12.18 15:04
PCT/US02/08971 ［特許］特願2002-578501(平14.03.22) 8884

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 02/08971

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
		40,51,52
Y	EP 0 984 346 A (HITACHI EUROP LTD) 8 March 2000 (2000-03-08)	2,3,13, 14,21, 27,28, 49,55
A	column 2, line 29 - line 43 column 4, line 22 - line 58	20,30, 44,57
X	INTEL CORPORATION ET AL: "Content Protection for Prerecorded Media Specification, DVD Book, Revision 0.93" 4C ENTITY, 31 January 2001 (2001-01-31), pages i-2.9, XP002202232 cited in the application	1,50
A	page 2.1 -page 2.9	3,4,17, 21,22, 41-45, 51-53, 57,58
P,X	WO 01 95327 A (KONINKL PHILIPS ELECTRONICS NV) 13 December 2001 (2001-12-13)	1,5,6, 8-10, 15-17, 20,23, 25,26, 29-32, 35,38, 41, 43-46, 50,53, 54,56-58
	page 1, line 12 - line 28 page 2, line 7 - line 10 page 2, line 23 -page 3, line 4 page 3, line 27 -page 4, line 27	

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

［書類名］国際公開パンフレット ［受付日］平14.10.17 平15.12.18 15:04
PCT/US02/08971 ［特許］特願2002-578501(平14.03.22) 8884

3

INTERNATIONAL SEARCH REPORT

In ternational Application No
PCT/US 02/08971

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0984346	A	08-03-2000	EP 0984346 A1		08-03-2000
			JP 2000076141 A		14-03-2000
WO 0195327	A	13-12-2001	AU 6391701 A		17-12-2001
			CZ 20020408 A3		15-05-2002
			WO 0195327 A2		13-12-2001
			NO 20020528 A		21-03-2002
			US 2001049662 A1		06-12-2001

Form PCT/ISA/210 (patent family annex) (July 1998)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZM,ZW

Ｆターム(参考) 5D029 MA31
5D044 BC03 CC06 DE50 DE53 GK08 GK11 GK17 HL02 HL08
5D090 AA01 BB02 CC04 CC14 DD03 DD05 GG16 GG32