(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2004-530348
(P2004-530348A)
(43)公表日　平成16年9月30日(2004.9.30)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/08	H04L 9/00	601C	5B017
G06F 12/14	G06F 12/14	320B	5D044
G11B 20/10	G06F 12/14	540C	5J104
	G11B 20/10	D	
	G11B 20/10	H	

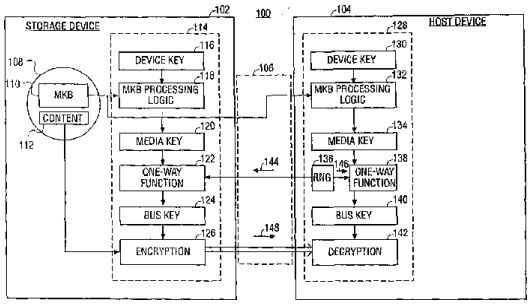
審査請求 未請求　予備審査請求 有　（全 39 頁）　最終頁に続く

(21)出願番号　特願2002-578500(P2002-578500)
(86)(22)出願日　平成14年3月7日(2002.3.7)
(85)翻訳文提出日　平成15年9月26日(2003.9.26)
(86)国際出願番号　PCT/US2002/007085
(87)国際公開番号　WO2002/080170
(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　09/823,423
(32)優先日　平成13年3月29日(2001.3.29)
(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　トゥロウ，ブレンダン
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】暗号鍵交換に基づくバス暗号化を提供する方法およびシステム

(57)【要約】
記憶媒体に記憶されたディジタル・コンテンツを無許可のコピーから保護するシステムを説明する。このシステムには、ナンスを生成する数ジェネレータ、暗号化サブシステム、および解読サブシステムが含まれる。暗号化サブシステムは、データ・バスを介して暗号化されたデータを送る前に暗号化バス鍵を使用して、鍵配布データ・ブロックを含む記憶媒体からアクセスされたデータを暗号化する。暗号化バス鍵は、鍵配布データ・ブロックの少なくとも一部、暗号化サブシステムに割り当てられた少なくとも１つのデバイス鍵、および数ジェネレータによって生成されたナンスに基づいて導出される。解読サブシステムは、データ・バスに結合されて、鍵配布データ・ブロックの少なくとも一部、解読サブシステムに割り当てられた少なくとも１つのデバイス鍵、および数ジェネレータによって生成されたナンスに基づいて導出される解読バス鍵を使用して、データ・バスを介して受け取った暗号化されたデータを解読する。



【特許請求の範囲】
【請求項１】
ナンスを生成する数ジェネレータと、
データ・バスを介して暗号化されたデータを送る前に、暗号化バス鍵を使用して、鍵配信データ・ブロックを含む記憶媒体からアクセスされるデータを暗号化する暗号化サブシステムとを有し、前記暗号化バス鍵が、鍵配信データ・ブロックの少なくとも一部、前記暗号化サブシステムに割り当てられた少なくとも１つのデバイス鍵、および数ジェネレータによって生成されたナンスに基づいて導出されるシステム。
【請求項２】
鍵配信データ・ブロックの少なくとも一部、前記解読サブシステムに割り当てられた少なくとも１つのデバイス鍵、および数ジェネレータによって生成されたナンスに基づいて導出される解読バス鍵を使用して、データ・バスを介して受け取られた前記暗号化されたデータを解読する、前記データ・バスに結合された解読サブシステムをさらに含む請求項１に記載のシステム。
【請求項３】
前記暗号化サブシステムが、
媒体鍵を計算するために、前記暗号化サブシステムに割り当てられた少なくとも１つのデバイス鍵を使用して記憶媒体から読み取られた鍵配信データ・ブロックの少なくとも一部を処理する処理ロジックと、
媒体鍵および数ジェネレータによって生成されたナンスに基づいて暗号化バス鍵を生成する１方向関数と、
前記暗号化バス鍵を使用して、前記記憶媒体からアクセスされたデータを暗号化する暗号化ロジックと
を含む請求項１に記載のシステム。
【請求項４】
前記解読サブシステムが、
媒体鍵を計算するために、前記解読サブシステムに割り当てられた少なくとも１つのデバイス鍵を使用して記憶媒体から読み取られた鍵配信データ・ブロックの少なくとも一部を処理する処理ロジックと、
前記媒体鍵および数ジェネレータによって生成されたナンスに基づいて解読バス鍵を生成する１方向関数と、
前記解読バス鍵を使用することによって、データ・バスを介して送られたデータを解読する解読ロジックと
を含む請求項２に記載のシステム。
【請求項５】
データ・バスを介して送られる前記データが数ジェネレータによって生成されたナンスに基づいて導出されるバス鍵を使用して暗号化され、送出の時に記録されると、データ・バスを介して送られる前記データを暗号化するために前記暗号化サブシステムによって使用されるものと同一のナンスへのアクセスを有さない解読サブシステムによってはその後にその記録されたデータを再生できなくなる請求項１に記載のシステム。
【請求項６】
前記鍵配信データ・ブロックが、暗号化されたデータのブロックを含む媒体鍵ブロックの形で実施される請求項２に記載のシステム。
【請求項７】
前記暗号化サブシステムが記憶媒体からのデータにアクセスすることができる記憶デバイスに実装され、前記解読サブシステムがその記憶デバイスからデータを検索することができるホスト・デバイスに実装される請求項２に記載のシステム。
【請求項８】
暗号化サブシステムに割り当てられるデバイス鍵および解読サブシステムに割り当てられるデバイス鍵の両方が損なわれていない場合に、前記暗号化サブシステムによって計算さ

れる前記媒体鍵が、解読サブシステムによって計算される媒体鍵と同一になる請求項２に記載のシステム。
【請求項９】
前記記憶媒体が、ディジタル多用途ディスク（ＤＶＤ）、ＣＤ－ＲＯＭ、光ディスク、光磁気ディスク、フラッシュベースのメモリ、磁気カード、および光カードから選択される請求項２に記載のシステム。
【請求項１０】
前記数ジェネレータが、前記解読サブシステム内に存在する乱数ジェネレータである請求項２に記載のシステム。
【請求項１１】
記憶デバイスが、記憶媒体から鍵配信データ・ブロックを読み取ること、
前記記憶デバイスが、媒体鍵を計算するために、少なくとも１つのデバイス鍵を使用して前記鍵配信データ・ブロックの少なくとも一部を処理すること、
前記記憶デバイスが、数ジェネレータによって生成されたナンスを取り出すこと、
前記記憶デバイスが、バス鍵を生成するために、１方向関数を使用して前記ナンスを前記媒体鍵と組み合わせること、
前記記憶デバイスが、記憶デバイスによって生成されたバス鍵を使用して記憶媒体から読み取られたデータを暗号化すること、
前記記憶デバイスが、暗号化されたデータをデータ・バスを介して送ること
を含む方法。
【請求項１２】
データ・バスを介して送られる前記データが、送出の時に記録されると、データ・バスを介して送られる前記データを暗号化するために記憶デバイスによって使用されるものと同一のナンスへのアクセスを有さないホスト・デバイスによってその後にその記録されたデータを再生できなくなるように、データ・バスを介して送られる前記データが、数ジェネレータによって生成されたナンスに基づいて導出されるバス鍵を使用して暗号化される請求項１１に記載の方法。
【請求項１３】
データ・バスを介して受け取られた暗号化されたデータを解読することをさらに含む請求項１１に記載の方法。
【請求項１４】
データ・バスを介して受け取られた暗号化されたデータの前記解読が、
ホスト・デバイスが、記憶媒体から鍵配信データ・ブロックを読み取ること、
前記ホスト・デバイスが、媒体鍵を計算するために、少なくとも１つのデバイス鍵を使用して鍵配信データ・ブロックの少なくとも一部を処理すること、
前記ホスト・デバイスが、数ジェネレータによって生成されたナンスを取り出すこと、
前記ホスト・デバイスが、バス鍵を生成するために、１方向関数を使用して前記媒体鍵をナンスと組み合わせること、
前記ホスト・デバイスが、ホスト・デバイスによって生成されたバス鍵を使用して、データ・バスを介して受け取られた前記暗号化されたデータを解読すること
を含む請求項１３に記載の方法。
【請求項１５】
前記ホスト・デバイスが、スクランブルされたコンテンツをスクランブル解除するのに必要なスクランブル解除鍵を前記記憶デバイスに要求すること、
前記記憶デバイスが、前記記憶デバイスによって生成された前記バス鍵を用いて、前記記憶媒体から読み取られた前記スクランブル解除鍵を暗号化し、その暗号化されたスクランブル解除鍵をホスト・デバイスに送ること、
前記ホスト・デバイスが、前記ホスト・デバイスによって生成された前記バス鍵を使用して、前記記憶デバイスから受け取った前記暗号化されたスクランブル解除鍵を解読すること、

前記ホスト・デバイスが、前記ホスト・デバイスによって解読された前記スクランブル解除鍵を使用して、前記解読されたデータをスクランブル解除すること
をさらに含む請求項１４に記載の方法。
【請求項１６】
前記鍵配信データ・ブロックが、暗号化されたデータのブロックを含む媒体鍵ブロックの形で実施される請求項１１に記載の方法。
【請求項１７】
前記数ジェネレータが、ホスト・デバイス内に存在する乱数ジェネレータである請求項１４に記載の方法。
【請求項１８】
データおよび鍵配信データ・ブロックを含む記憶媒体にアクセスするとともに、処理ロジック、１方向関数、および暗号化ロジックを含む記憶デバイスであって、前記処理ロジックが媒体鍵を計算するために、前記記憶デバイスに割り当てられたデバイス鍵を使用して前記鍵配信データ・ブロックの少なくとも一部を処理し、前記１方向関数がバス鍵を作るために前記媒体鍵を数ジェネレータによって生成されたナンスと組み合わせ、前記暗号化論理が暗号化されたデータをデータ・バスを介して送る前に前記バス鍵を使用して記憶デバイスからアクセスされた前記データを暗号化する記憶デバイス。
を含む装置。
【請求項１９】
前記データ・バスを介して前記記憶デバイスに結合され、処理ロジック、１方向関数、および解読ロジックを含むホスト・デバイスであって、前記処理ロジックが媒体鍵を計算するために、前記ホスト・デバイスに割り当てられたデバイス鍵を使用して、前記鍵配信データ・ブロックの少なくとも一部を処理し、前記１方向関数がバス鍵を作るために前記媒体鍵を前記数ジェネレータによって生成された前記ナンスと組み合わせ、前記解読ロジックが前記バス鍵を使用してデータ・バスを介して受け取られた前記暗号化されたデータを解読するホスト・デバイスをさらに含む請求項１８に記載の装置。
【請求項２０】
データ・バスを介して送られる前記データが、送出の時に記録されると、データ・バスを介して送られる前記データを暗号化するために前記記憶デバイスによって使用されるものと同一のナンスへのアクセスを有さないホスト・デバイスによってその記録されたデータをその後に再生できなくなるように、データ・バスを介して送られる前記データが、数ジェネレータによって生成されたナンスに基づいて導出されるバス鍵を使用して暗号化される請求項１８に記載の装置。
【請求項２１】
記憶デバイスに割り当てられるデバイス鍵およびホスト・デバイスに割り当てられるデバイス鍵の両方が損なわれていない場合に、前記記憶デバイスによって計算される前記媒体鍵が、ホスト・デバイスによって計算される媒体鍵と同一になる請求項１９に記載の装置。
【請求項２２】
前記数ジェネレータが、前記ホスト・デバイス内に存在する乱数ジェネレータである請求項１９に記載の装置。
【請求項２３】
前記記憶デバイスが、ＤＶＤドライブの形で実施され、前記ホスト・デバイスが、ＤＶＤプレイヤまたはパーソナル・コンピュータのいずれかの形で実施される請求項１９に記載の装置。
【請求項２４】
前記記憶媒体が、ディジタル多用途ディスク（ＤＶＤ）、ＣＤ－ＲＯＭ、光ディスク、光磁気ディスク、フラッシュベースのメモリ、磁気カード、および光カードから選択される請求項１９に記載の装置。
【請求項２５】

前記記憶媒体が、スクランブルされたコンテンツを含むＤＶＤの形で実施される請求項１９に記載の装置。
【請求項２６】
前記鍵配信データ・ブロックが、暗号化されたデータのブロックを含む媒体鍵ブロックの形で実施される請求項１９に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、データ・バスを介して送られるデータの暗号化および解読に関し、詳細には、記憶媒体に記憶されたディジタル・コンテンツを無許可のコピーから保護する方法およびシステムに関する。
【背景技術】
【０００２】
スクランブル技法および暗号化／解読技法など、記憶媒体に記憶されたディジタル・コンテンツを無許可のコピーから保護するさまざまな技法が使用可能である。しかし、一部のコピー・プロテクション技法の保全性は損なわれており、そのようなコピー・プロテクション技法はもはや、著作権のある材料を無許可のコピーから保護するのに有効ではない。たとえば、ディジタル多用途ディスク（ＤＶＤ）技術の分野で、ＤＶＤビデオ・コンテンツをスクランブル化するｃｏｎｔｅｎｔ　ｓｃｒａｍｂｌｅ　ｓｙｓｔｅｍ（ＣＳＳ）の保全性が、最近、ハッカーによって損なわれ、ＤＶＤ－ＲＯＭドライブを備えるコンピュータを使用して、ＣＳＳ保護されたＤＶＤのコンテンツをスクランブル解除するソフトウェア・プログラムが現在入手可能である。
【０００３】
さらに、記憶媒体上のディジタル・コンテンツは、通常は、記憶デバイス（すなわち、記憶媒体からのデータにアクセスできるすべてのデバイス）からホスト・デバイス（すなわち、記憶デバイスからデータを検索することができるすべてのデバイス）へ、正しい機器を有する誰もがキャプチャすることのできる形でデータ・バスを介して送られる。送られるデータは、元のディジタル形式ではないものにすることができる（すなわち、データを、暗号化および／またはスクランブルすることができる）が、送出時にキャプチャされた暗号化されかつ／またはスクランブルされたデータのコピーは、合法的な記憶デバイスから来たものであるかのように、暗号化されたデータをホスト・デバイスに提示することによって再生可能となることがある。
【発明を実施するための最良の形態】
【０００４】
以下の説明では、本発明の完全な理解を提供するために、特定の詳細を示す。しかし、本発明を、これらの特定の詳細なしで実践できることは、当業者に明白であろう。他の場合には、本発明を不明瞭にしないように、周知の回路、構造、および技法は、詳細に示さない。
【０００５】
図１に、本発明の一実施形態による記憶媒体に記憶されたディジタル・コンテンツをコピーから保護するシステム１００を示す。コピー・プロテクション・システム１００には、バスを介する記憶デバイスとホスト・デバイスの間のデータ（たとえば、暗号化されたデータおよび／または暗号化されないデータ）の送出を行うために、データ・バス１０６を介してホスト・デバイス１０４に結合された記憶デバイス１０２が含まれている。記憶デバイス１０２は、記憶媒体１０８からのデータにアクセスすることができるどのようなデバイスでもよい。ホスト・デバイス１０４は、記憶デバイス１０２からデータを検索することができるすべてのデバイスとすることができる。記憶デバイス１０２は、ホスト・デバイス１０４と別のエンクロージャに配置された独立型デバイスでもよく、その代わりに、記憶デバイス１０２およびホスト・デバイス１０４を１つのエンクロージャに組み合わせることもできる。記憶デバイス１０２内に配置される記憶媒体１０８は、ディジタル多

用途ディスク（ＤＶＤ）、ＣＤ－ＲＯＭ、光ディスク、光磁気ディスク、フラッシュベースのメモリ、フロッピ・ディスク、ハード・ドライブ、読取専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気カード、または光カードを含むがこれに制限されない、ディジタル・コンテンツを記憶するのに適するすべてのタイプの取外し可能または取外し不能の記憶媒体とすることができる。

【０００６】

コピー・プロテクション・システム１００を実施するために、媒体製造業者は、記憶媒体のそれぞれに、許可された実体（すなわち、コピー・プロテクション・システムの確立および管理の責任を負う実体）によって生成された鍵配信データ・ブロック（ｋｅｙ　ｄｉｓｔｒｉｂｕｔｉｏｎ　ｄａｔａ　ｂｌｏｃｋ）（たとえば、媒体鍵ブロック（ｍｅｄｉａ　ｋｅｙ　ｂｌｏｃｋ）「ＭＫＢ」１１０）を配置する。一実施形態では、ＭＫＢ１１０が、記憶媒体に組み込むことができる暗号化された鍵のブロックであり、記憶媒体からのコンテンツにアクセスする記憶デバイスが、ＭＫＢの一部を処理して、バスを介してデータを送る前にデータを暗号化するのに使用することができる秘密鍵を計算できるようになる。記憶媒体からのコンテンツを再生するホスト・デバイスも、ＭＫＢの一部にアクセスし、処理して、バスを介して送られるデータを正しく解読するために同一の秘密鍵を計算することができる。

【０００７】

図１を参照するとわかるように、記憶デバイス１０２に、本発明の一態様による、無許可のコピーを防ぐためにバス１０６を介してホスト・デバイス１０４にデータを送る前に、記憶媒体１０８から読み取られたコンテンツを暗号化する暗号化サブシステム１１４が含まれる。暗号化システム１１４には、１セットのデバイス鍵１１６、ＭＫＢ処理ロジック１１８、１方向関数１２２、および暗号化ロジック１２６が含まれる。１セットのデバイス鍵１１６は、製造時に各記憶デバイスに割り当てられる。これらのデバイス鍵は、許可された実体によって提供され、秘密の媒体鍵１２０を計算するために記憶媒体１０８に組み込まれるＭＫＢ１１０の一部を処理するのに、ＭＫＢ処理ロジック１１８によって使用される。デバイス鍵１１６は、個別の記憶デバイスそれぞれに一意とするか、複数の記憶デバイスによって共通で使用することができる。一実施形態では、ＭＫＢ、デバイス鍵、およびＭＫＢ処理ロジックは、デバイス鍵が損なわれていない限り、どの互換デバイスが記憶媒体にアクセスするのに使用されるかに無関係に、同一の秘密媒体鍵が生成されるように構成される。

【０００８】

記憶デバイス１０２に接続されたホスト・デバイス１０４には、本発明の一実施形態による、記憶デバイスから供給されるデータを解読する解読サブシステム１２８が含まれている。解読サブシステム１２８には、デバイス鍵１３０のそれ自体のセットおよびＭＫＢ処理ロジック１３２が含まれて、デバイス鍵のそれ自体のセットを使用して秘密の媒体鍵１３４を計算するためにＭＫＢ１１０が処理される。ホスト・デバイス１０４に割り当てられるデバイス鍵１３０のセットは、記憶デバイス１０２に割り当てられるデバイス鍵１１６と異なるものとすることができるが、ホスト・デバイス１０４によって生成される媒体鍵１３４は、記憶デバイス１０２によって生成される媒体鍵１２０と媒体鍵１３４のどちらのセットも損なわれていないならば、媒体鍵１２０と同一にすることができる。

【０００９】

コピー・プロテクション・システム１００には、乱数またはシーケンス番号（以下では「ナンス」と称する）を生成し、そのコピーを記憶デバイス１０２に送る乱数ジェネレータ１３６も含まれる。記憶デバイス１０２は、ホスト・デバイス１０４から受け取ったナンス１４４を、１方向関数１２２を使用して媒体鍵１２０と組み合わせ、その結果（すなわちバス鍵１２４）を暗号化ロジック１２６に返す。１方向関数１２２は、媒体鍵１２０およびナンス１４４を入力することによってバス鍵１２４を生成できるが、バス鍵１２４およびナンス１４４から媒体鍵１２０を判定することが計算的に不可能になるように構成される。ナンス１４４が、ホスト・デバイス１０４から記憶デバイス１０２に供給される時

に、ナンス１４６は、ホスト・デバイス１０４内に存在する１方向関数１３８によってもアクセスされて、媒体鍵１３４およびナンス１４６を組み合わせて、解読ロジック１４２によって使用されるそれ自体のバス鍵１４０が作られる。同一の１方向関数が、記憶デバイス１０２およびホスト・デバイス１０４の両方によって使用されるので、両方のデバイスがバス鍵の生成に同一の媒体鍵およびナンスを使用する限り、記憶デバイスおよびホスト・デバイスの両方が、同一のバス鍵を生成することに留意されたい。

【００１０】

一実施形態では、ある種の耐タンパ（ｔａｍｐｅｒ　ｒｅｓｉｓｔａｎｔ）方式を使用して、暗号化サブシステム１１４内および解読サブシステム１２８内の論理構成要素を密に結合し、その結果、これらの論理要素の間を流れる秘密の鍵およびデータを外部からアクセス不能にする。これに関して、暗号化サブシステム内および解読サブシステム内を流れるデータは耐タンパ方式によって保護されるが、記憶デバイス１０２をホスト・デバイス１０４に接続するデータ・バス１０６を保護されないものとすることができ、攻撃者によるアクセスを許すものとすることができる。悪意のあるコピーに対する保護のないデータ・バス１０６を介して送られるデータを保護するために、記憶媒体１０８から読み取られたディジタル・コンテンツ１１２は、データ・バス１０６を介してホスト・デバイス１０４に送られる前に、バス鍵１２４を用いて暗号化ロジック１２６によって暗号化される。したがって、正しいバス鍵を有するホスト・デバイス１０４だけが、データ・バス１０６を介して送られる暗号化されたデータ１４８を正しく解読することができる。

【００１１】

有利なことに、本発明のコピー・プロテクション・システム１００は、「リプレイ」攻撃（ｒｅｐｌａｙ　ａｔｔａｃｋ）に抵抗するのに効果的である。リプレイ攻撃では、攻撃者が、記憶デバイス１０２からホスト・デバイス１０４に進む暗号化されたデータ１４８を転送し、暗号化されたデータを記録可能媒体に記録する。さらに、ホスト・デバイス１０４が、記憶媒体１０８に組み込まれたＭＫＢ１１０にアクセスする時に、攻撃者は、ＭＫＢ１１０も同一の記録可能媒体に記録する。合法的な記憶デバイスから来たものであるかのように、暗号化されたデータをホスト・デバイスに提示することによって、送出の時にキャプチャされたＭＫＢ１１０および暗号化されたデータ１４８のコピーを、普通のメディア・プレイヤ・システムで再生することができる。しかし、本発明では、暗号化されたデータの再生中に解読バス鍵を生成するためにホスト・デバイスによって使用されるナンス値が、暗号化の時に暗号化バス鍵を生成するために記憶デバイスによって使用されるナンス値と異なるので、このタイプのリプレイ攻撃が妨げられる。言い換えると、ナンスを使用してバス鍵を生成することによって、暗号化されたデータの後続のアクセス中にホスト・デバイス１０４が入手するバス鍵１４０は、暗号化されたデータを暗号化するのに前に使用されたバス鍵１２４と異なる可能性が非常に高く、したがって、ホスト・デバイスは、暗号化されたデータを正しく解読することができない。

【００１２】

一実施形態では、デバイス鍵のセットがコピー・プロテクション・システムの保全性を脅かす形で損なわれる場合に、更新されたＭＫＢを含む新しい媒体鍵を公開することができ、これによって、デバイス鍵の損なわれたセットは誤った媒体鍵を計算することになり、これによって、新しい媒体を扱う能力が取り消される。これは、デバイス鍵の損なわれたセットを有するデバイスが、もはや新しい媒体鍵と共に機能しなくなるが、有効なデバイス鍵を有する他の既存の準拠デバイスが、新しい媒体を扱い続けるようになることを意味する。

【００１３】

公開鍵配信システムから秘密鍵を得るさまざまな方法があること、媒体鍵ブロック（ＭＫＢ）の使用が暗号鍵配信の１例にすぎず、公開鍵管理の詳細が異なる応用例の間で異なる可能性があることに留意されたい。これに関して、他のタイプの公開鍵配信システムを、本発明のコピー・プロテクション・システムと共に使用することができる。そのような公開鍵配信システムは、本発明の範囲および企図に含まれる。

【００１４】
図３を参照すると、本発明の一実施形態による、バスを介してデータを送る前のデータ暗号化のオペレーションが示されている。準拠記憶媒体が、記憶デバイス内に置かれる時に、媒体鍵を計算する責任を負うＭＫＢ処理ロジックが、記憶媒体からのＭＫＢにアクセスする（ブロック３００）。次に、ＭＫＢ処理ロジックが、記憶デバイスに割り当てられたデバイス鍵のセットおよび記憶媒体から読み取られたＭＫＢを使用して、媒体鍵を生成する（ブロック３１０）。一実施形態では、ＭＫＢに、暗号化されたデータのブロックが含まれ、暗号化されたデータのそれぞれが異なる鍵を用いて暗号化された秘密媒体鍵である。各デバイス鍵は、所定のビット・サイズのデータ（たとえば５６ビット・データ）とすることができ、そのデータに、ＭＫＢデータ・ブロック内のどの暗号化されたデータがデバイス鍵によって解読されるように構成されたものであるかを示すのに使用されるインデックス番号が含まれる。デバイス鍵を使用して、ＭＫＢの指定された部分を解読することによって、秘密媒体鍵を入手することができる。これは、ＭＫＢに含まれる秘密媒体鍵を、デバイス鍵の合法的なセットを有する任意のデバイスによって入手できることを意味する。準拠記憶媒体が、記憶デバイス内に置かれた後に、すべての暗号化が行われる前に、ホスト・デバイスが、ナンス（たとえば乱数）を生成し、そのナンスを記憶デバイスに送る。暗号化サブシステムは、ホスト・デバイスによって送られたナンスを受け取り（ブロック３２０）、１方向関数を使用して、そのナンスを上で入手した媒体鍵と組み合わせてバス鍵を作る（ブロック３３０）。得られたバス鍵を使用して、暗号化サブシステムが記憶媒体から読み取られたディジタル・コンテンツを暗号化し、暗号化されたデータをバスを介してホスト・デバイスに出力する（ブロック３４０）。

【００１５】
図４を参照すると、本発明の一実施形態による、バスを介して送られたデータの解読のオペレーションが示されている。ホスト・デバイスが、記憶デバイス内の記憶媒体へのアクセスを必要とする時に、ホスト・デバイスの解読サブシステム内にあるＭＫＢ処理ロジックが記憶媒体からＭＫＢを読み取る（ブロック４００）。次に、ブロック４１０で、ＭＫＢ処理ロジックが、ホスト・デバイスに割り当てられたデバイス鍵のセットおよび記憶媒体から読み取られたＭＫＢを使用して、媒体鍵を生成する。前に注記したように、解読サブシステムは、ナンスを生成し（ブロック４２０）、そのコピーを暗号化サブシステムに送り（ブロック４３０）、ナンスのもう１つのコピーを解読サブシステムの１方向関数に送る。次に、解読サブシステムが、１方向関数を使用してナンスと媒体鍵を組み合わせてバス鍵を作る（ブロック４４０）。バス鍵が、解読サブシステムによって使用されて、バスを介して送られた暗号化されたデータが解読される（ブロック４５０）。

【００１６】
図２に、本発明の一実施形態による、ディジタル多用途ディスク（ＤＶＤ）を無許可のコピーから保護するシステム２００を示す。この実施形態では、コピー・プロテクション・システム２００が、上で説明したように媒体鍵ブロック（ＭＫＢ）２１０を使用して、ＤＶＤ２０８のスクランブルされたコンテンツ２１２をパッチして、追加のコピー・プロテクションを提供する。これに関して、新しい準拠ＤＶＤのフォーマットは、ＭＫＢ２１０がディスクの新しいデータ要素として導入されることを除いて、変更されないまま（すなわち、ｃｏｎｔｅｎｔ　ｓｃｒａｍｂｌｅ　ｓｙｓｔｅｍ（ＣＳＳ）スクランブルがまだ使用される）にすることができる。前に注記したように、ＭＫＢ２１０は、異なる個々に割り当てられたデバイス鍵を使用する異なるデバイスが、媒体鍵と称する共通の秘密鍵を抽出できるようにする暗号化されたデータのブロックである。ＭＫＢ２１０を使用して、スクランブルされたＤＶＤデータ２１２をパッチすることによって、プロテクション・システムを更新することが可能になる（すなわち、デバイス鍵のセットが、将来に損なわれる場合に、損なわれたデバイス鍵のセットをシステムから排除する新しいＭＫＢを使用することができる）。

【００１７】
本発明のコピー・プロテクション・システム２００の一部として、新しい準拠ＤＶＤドラ

イブ２０２は、デバイス鍵２１８、ＭＫＢ処理ロジック２２０、１方向関数２２４、および、ＭＫＢを処理し、秘密の媒体鍵２２２を抽出するのに必要な暗号化ロジック２２８を備えて、媒体鍵２２２およびナンス２５０に基づいてバス鍵２２６を計算し、バス鍵２２６を使用して、ＣＳＳスクランブルされたＤＶＤ２０８上のデータ２１２を暗号化する。ホスト・コンピュータ２０４（たとえば、ホストＰＣまたはＤＶＤプレイヤ）のＤＶＤビデオ・プレイヤ・ソフトウェア２３０も、これらの追加の特徴を備えて、秘密の媒体鍵２３６を計算するためにデバイス鍵２３２のそれ自体のセットを使用してＭＫＢ２１０にアクセスし、処理し、媒体鍵２３６およびナンス２５２に基づいてバス鍵２４２を計算し、バス鍵２４２を使用して、ＤＶＤドライブ２０２によって送られたデータ２５４を解読する。

【００１８】

新しい準拠ＤＶＤ－Ｖｉｄｅｏディスク２０８が、ＤＶＤドライブ２０２に挿入される時に、下記の鍵交換手順がＤＶＤドライブ２０２とホストＰＣ２０４の間で行われる。ＤＶＤドライブ２０２が、媒体鍵２２２を計算するためにＭＫＢ２１０を読み取り、かつそのデバイス鍵２１８を使用する。ホストＰＣ２０４で動作するＤＶＤビデオ・プレイヤ・ソフトウェア２３０が必要なコマンドをＤＶＤドライブ２０２に送って、媒体鍵２３６を計算するためにＤＶＤドライブ２０２がＭＫＢ２１０を読み取り、かつそのデバイス鍵２３２を使用できるようにする。ＤＶＤビデオ・プレイヤ・ソフトウェア２３０は、ランダムな数（ナンス）２３８を選択し、予め決めたコマンドを使用してその数をＤＶＤドライブ２０２に送る。ＤＶＤドライブ２０２およびＤＶＤビデオ・プレイヤ・ソフトウェア２３０の両方が、共通のバス鍵２２６および２４２を計算するが、このバス鍵は、媒体鍵およびナンスの暗号１方向関数から導出される。その後、ＤＶＤビデオ・プレイヤ・ソフトウェア２３０は、ＤＶＤドライブ２０２に要求を送って、スクランブル解除鍵２１４（たとえばＣＳＳ鍵）およびＣＳＳスクランブルされたコンテンツ２１２をディスク２０８から読み取る。ＣＳＳ鍵２１４またはＣＳＳスクランブルされたコンテンツ２１２をホストＰＣ２０４に送る前に、ＤＶＤドライブ２０２は、まず、堅牢な暗号およびバス鍵２２６を使用して、これらを暗号化する。データを受け取る時に、ＤＶＤビデオ・プレイヤ・ソフトウェア２３０は、同一の暗号およびバス鍵２４２を使用して、これらを解読し、そのデータをスクランブル解除ロジック２４６に転送する。スクランブル解除ロジック２４６は、スクランブル解除鍵２１４を使用して、データをスクランブル解除し、そのデータを圧縮解除ロジック２４８に転送する。

【００１９】

媒体鍵およびバス鍵の計算に関して、および、ＣＳＳ鍵およびＣＳＳスクランブルされたコンテンツのバス暗号化およびバス解読に関して、大きい鍵サイズを有する堅牢な暗号が使用される。一実施形態では、この暗号はＣ２暗号であり、鍵サイズは５６ビットである。

【００２０】

この実施形態で、本発明のコピー・プロテクション・システムは、古いＣＳＳ方式の回りを堅牢なプロテクション方式で「ラップする」ことによって、ＤＶＤ－Ｖｉｄｅｏコンテンツの保護を劇的に改善することができる。これは、デバイス鍵が将来に損なわれる場合の更新を提供するＭＫＢ技術を使用し、リプレイ攻撃に対する保護のためにナンスを追加することによって単純で新規な形で達成される。

【００２１】

図５を参照すると、本発明の一実施形態による、ＤＶＤコンテンツの解読およびスクランブル解除の動作が示されている。ＤＶＤがＤＶＤ－ＲＯＭドライブに挿入された時に、ホストＰＣで動作するＤＶＤビデオ・プレイヤ・ソフトウェアは、スクランブルされたコンテンツをスクランブル解除するのに必要なスクランブル解除鍵または秘密データ（たとえばＣＳＳ鍵）をＤＶＤドライブに要求する（ブロック５００）。次に、ブロック５１０で、ＤＶＤドライブがディスクから読み取ったＣＳＳ鍵をバス鍵を用いて暗号化し、ホストＰＣに送る。ＣＳＳ鍵はバスを介してホストＰＣに送られる前に暗号化される。前に述べ

たように、損なわれていないデバイス鍵のセットを有するホストＰＣによって計算されたバス鍵を使用してＣＳＳ鍵を暗号化する。これに関して、暗号化されたＣＳＳ鍵を受け取ったならば、ホストＰＣで動作するＤＶＤビデオ・プレイヤ・ソフトウェアは、バス鍵を用いてＣＳＳ鍵を解読する（ブロック５２０）。次に、ブロック５３０で、ＤＶＤビデオ・プレイヤ・ソフトウェアが、ＣＳＳスクランブルされたコンテンツを読み取る要求をＤＶＤドライブにディスパッチする。コンテンツをホストＰＣに送る前に、ＤＶＤドライブは、バス鍵を使用してスクランブルされたコンテンツを暗号化し、その暗号化されたデータをホストＰＣに送る（ブロック５４０）。コンテンツを受け取る時に、ＤＶＤプレイヤ・ソフトウェアは、まず、バス鍵を使用してデータを解読する（ブロック５５０）。解読ロジックの出力が、スクランブル解除ロジックに供給され、スクランブル解除ロジックは、前に入手したＤＳＳ鍵を使用してＣＳＳスクランブル解除処理を実行する（ブロック５６０）。

【００２２】

本発明の前述の実施形態を説明し、図示したが、本発明の趣旨および範囲に含まれる、提案されたものおよびその他の変形形態および修正形態を、本発明に関係する技術分野の当業者が思い浮かべることができることを理解されたい。したがって、本発明の範囲は、請求項で示されているものに従って定義される。

【図面の簡単な説明】

【００２３】

【図１】本発明の一実施形態による、記憶媒体に記憶されたディジタル・コンテンツをコピーから保護するシステムのブロック図である。

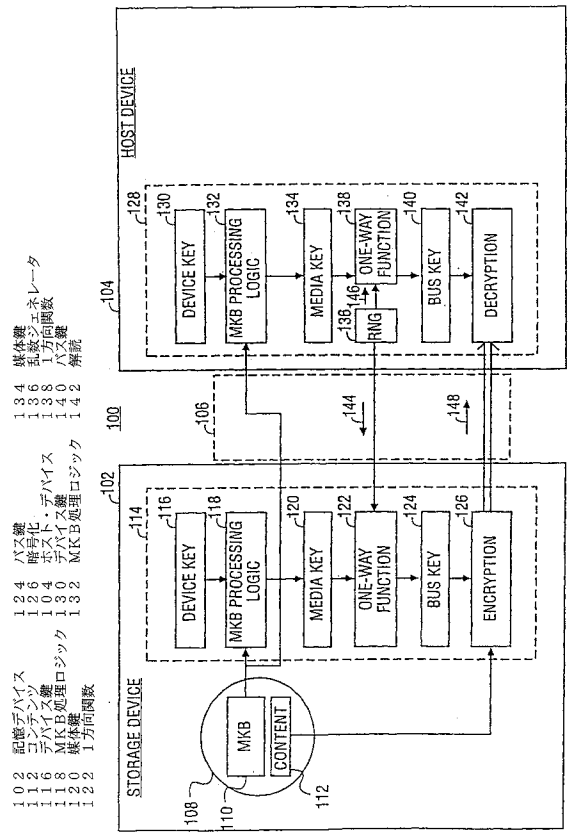
【図２】本発明の一実施形態による、ＤＶＤを悪意のあるコピーから保護するシステムのブロック図である。

【図３】本発明の一実施形態による、バスを介してデータを送る前のデータの暗号化の流れ図である。

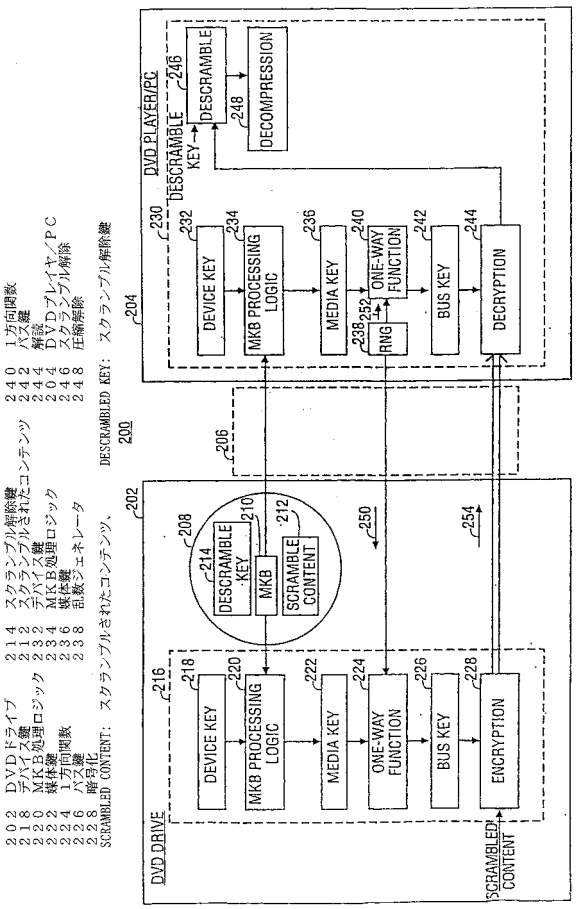
【図４】本発明の一実施形態による、バスを介して送られたデータの解読の流れ図である。

【図５】本発明の一実施形態による、ＤＶＤコンテンツの解読およびスクランブル解除の流れ図である。

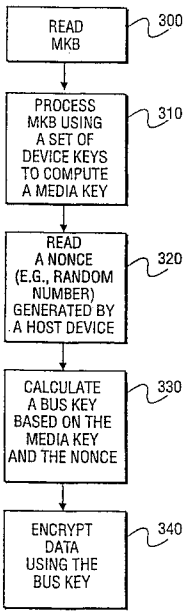
【図１】



【図２】

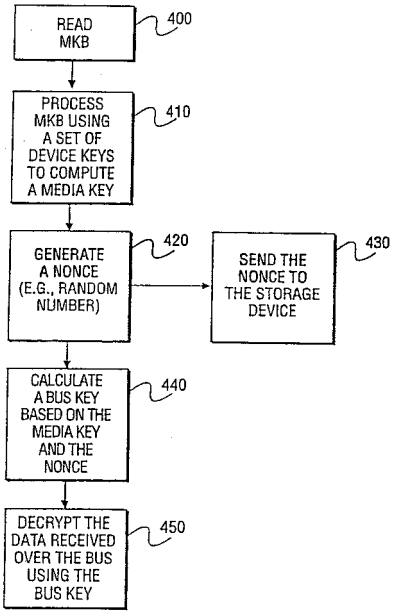


【図３】



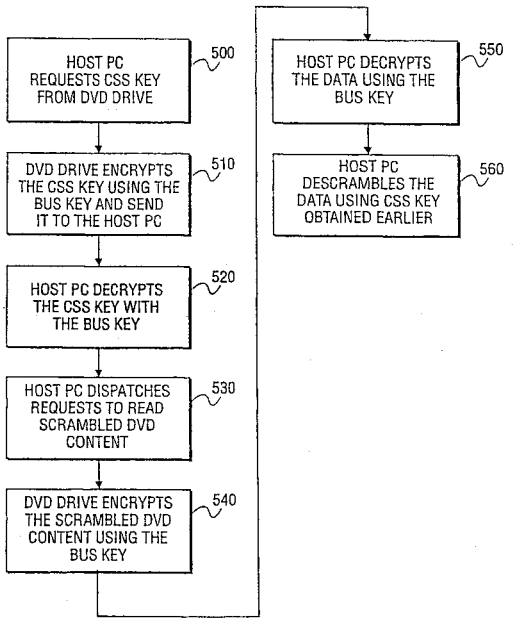
３００　ＭＫＢを読み取る
３１０　デバイス鍵のセットを使用してＭＫＢを処理して、媒体鍵を計算する
３２０　ホスト・デバイスによって生成されたナンス（たとえば乱数）を読み取る
３３０　媒体鍵およびナンスに基づいてバス鍵を計算する
３４０　バス鍵を使用してデータを暗号化する

【図４】



４００　ＭＫＢを読み取る
４１０　デバイス鍵のセットを使用してＭＫＢを処理して、媒体鍵を計算する
４２０　ナンス（たとえば乱数）を生成する
４３０　ナンスを記憶デバイスに送る
４４０　媒体鍵およびナンスに基づいてバス鍵を計算する
４５０　バス鍵を使用して、バスを介して受け取ったデータを解読する

【図５】



５００　ホストＰＣが、ＤＶＤドライブにＣＳＳ鍵を要求する
５１０　ＤＶＤドライブが、バス鍵を使用してＣＳＳ鍵を暗号化し、ホストＰＣに送る
５２０　ホストＰＣが、バス鍵を用いてＣＳＳ鍵を解読する
５３０　ホストＰＣが、スクランブルされたＤＶＤコンテンツを読み取る要求をディスパッチする
５４０　ＤＶＤドライブが、バス鍵を使用して、スクランブルされたＤＶＤコンテンツを暗号化する
５５０　ホストＰＣが、バス鍵を使用してデータを解読する
５６０　ホストＰＣが、前に入手したＣＳＳ鍵を使用して、データをスクランブル解除する

【国際公開パンフレット】

(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 02/080170 A2

(51) International Patent Classification⁷: G11B 20/00

(21) International Application Number: PCT/US02/07085

(22) International Filing Date: 7 March 2002 (07.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/823,423 29 March 2001 (29.03.2001) 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.**; Blakely, Sokoloff, Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 et al. (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:
without international search report and to be republished upon receipt of that 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.

WO 02/080170 A2

(54) Title: METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE

(57) Abstract: A system is described for protecting digital content stored on a storage medium from unauthorized copying. The system includes a number generator to generate a nonce, an encryption subsystem and a decryption subsystem. The encryption subsystem encrypts data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus. The encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to the encryption subsystem and the nonce generated by the number generator. The decryption subsystem is coupled to the data bus to decrypt the encrypted data received over the data bus using a decryption bus key derived based on at least a portion of the key distribution data block, at least one device key assigned to the decryption subsystem and the nonce generated by the number generator.

METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention generally relates to encrypting and decrypting data transmitted over a data bus, and in particular, to a method and system for protecting digital content stored on a storage medium from unauthorized copying.

Description of the Related Art

[0002] A variety of techniques are available for protecting digital contents stored on a storage medium from unauthorized copying such as scrambling and encryption/decryption techniques. However, the integrity of some copy protection techniques has been compromised and such copy protection techniques are no longer effective against unauthorized copying of copyrighted material. For example, in the field of digital versatile disc (DVD) technology, the integrity of content scramble system (CSS) for scrambling DVD video contents has been recently compromised by hackers, and software programs are now available that can descramble the contents of CSS-protected DVDs, using a computer equipped with a DVD-ROM drive.

[0003] Additionally, digital contents on a storage medium is usually transmitted from a storage device (i.e., any device capable of accessing data from a storage medium) to a host device (i.e., any device capable of retrieving data from the storage device) over a data bus in a form that can be captured by anyone having the proper equipment. Although the data transmitted may not be in its original digital form (i.e., data may be encrypted and/or scrambled), a copy of the encrypted and/or scrambled data captured at the time of the transmission may still be playable by presenting the encrypted data to a host device as though it was coming from a legitimate storage device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Figure 1 is a block diagram of a system for protecting digital content stored on a storage medium from copying according to one embodiment of the present invention.

[0005] Figure 2 is a block diagram of a system for protecting DVDs from malicious copying according to one embodiment of the invention.

[0006] Figure 3 is a flowchart of encrypting data prior to transmitting the data over a bus according to one embodiment of the invention.

[0007] Figure 4 is a flowchart of decrypting data transmitted over a bus according to one embodiment of the invention.

[0008] Figure 5 is a flowchart of decrypting and descrambling DVD contents according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0009] In the following description, specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known circuits, structures and techniques have not been shown in detail in order to avoid obscuring the present invention.

[00010] Figure 1 depicts a system 100 for protecting digital content stored on a storage medium from copying according to one embodiment of the present invention. The copy protection system 100 includes a storage device 102 coupled to a host device 104 via a data bus 106 to enable transmission of data (e.g., encrypted and/or non-encrypted data) between the storage and host devices through the bus. The storage device 102 may be any device capable of accessing data from a storage medium 108. The host device 104 may be any device capable of retrieving data from the storage device 102. The storage device 102 may be a stand-alone device arranged in an enclosure separate from the host device 104 or alternatively, the storage device 102 and the host device 104 may be combined

into one enclosure. The storage medium 108 placed within the storage device 102 may be any type of a removable or non-removable storage medium suitable for storing digital content including, but not limited to, digital versatile discs (DVDs), CD-ROMs, optical discs, magneto-optical discs, flash-based memory, floppy disks, hard drives, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards.

[00011] To implement the copy protection system 100, media manufacturers will place a key distribution data block (e.g., media key block "MKB" 110) generated by an authorized entity (i.e., an entity responsible for establishing and administering the copy protection system) on each piece of storage media. In one embodiment, the MKB 110 is a block of encrypted keys that can be embedded in a storage medium such that storage devices that access the content from the storage medium are able to process portion(s) of the MKB to compute a secret key that can be used to encrypt the data prior to transmitting the data over the bus. The host device that plays the content from the storage medium also accesses and processes portion(s) of the MKB to compute the same secret key to properly decrypt the data transmitted over the bus.

[00012] As seen by referring to figure 1, the storage device 102 includes an encryption subsystem 114 according to one embodiment of the invention to encrypt the content read from the storage medium 108 prior to transmitting the data over the bus 106 to the host device 104 to prevent unauthorized copying. Included in the encryption system 114 is a set of device keys 116, a MKB processing logic 118, a one-way function 122 and an encryption logic 126. The set of device keys 116 has been assigned to each storage device when manufactured. These device keys are provided by the authorized entity and are used by the MKB processing logic 118 to process portion(s) of the MKB 110 embedded in the storage medium 108 to compute a secret media key 120. The device keys 116 may either be unique to each individual storage device, or used commonly by multiple storage devices. In one embodiment, the MKB, the device keys and the MKB processing logic are configured such that the same secret media key will be

generated regardless of which compliant device is used to access the storage medium so long as its device keys have not been compromised.

[00013] The host device 104 connected to the storage device 102 includes a decryption subsystem 128 according to one embodiment of the invention to decrypt the data supplied from the storage device. Included in the decryption subsystem 128 are its own set of device keys 130 and a MKB processing logic 132 to process the MKB 110 using its own set of device keys to compute a secret media key 134. Although the set of device keys 130 assigned to the host device 104 may be different from the device keys 116 assigned to the storage device 102, the media key 134 generated by the host device 104 will be the same as the media key 120 generated by the storage device 102 provided that neither sets of device keys have been compromised.

[00014] Also included in the copy protection system 100 is a random number generator 136 to generate a random or sequential number (referred hereinafter as "nonce") and send a copy of it to the storage device 102. The storage device 102 combines the nonce 144 received from the host device 104 with the media key 120 using the one-way function 122 and returns the result (i.e., bus key 124) to the encryption logic 126. The one-way function 122 is configured such that the bus key 124 can be generated by inputting the media key 120 and the nonce 144, however, determining the media key 120 from the bus key 124 and nonce 144 is computationally infeasible. When the nonce 144 is supplied from the host device 104 to the storage device 102, the nonce 146 is also accessed by the one-way function 138 residing within the host device 104 to combine the media key 134 and the nonce 146 to produce its own bus key 140 to be used by the decryption logic 142. It should be noted that since the same one-way function is used by the storage device 102 and host device 104, both storage and host devices will generate the same bus key provided that same media key and nonce was used by both devices to generate the bus key.

[00015] In one embodiment, some sort of a tamper resistant scheme is employed to tightly couple the logical components within the encryption

subsystem 114 and the decryption subsystem 128 so that secret keys and data flowing between the logical components are not accessible from outside. In this regard, the data flowing within the encryption and decryption subsystems are protected by a tamper resistant scheme; however, the data bus 106 connecting the storage device 102 to the host device 104 may be unsecured and may be susceptible to access by an attacker. To protect the data transmitted over the data bus 106 which may be non-secured against malicious copying, the digital content 112 read from the storage medium 108 is encrypted by the encryption logic 126 with the bus key 124 prior to transmitting over the data bus 106 to the host device 104. In this regard, only the host device 104 with the correct bus key can properly decrypt the encrypted data 148 transmitted over the bus 106.

[00016] Advantageously, the copy protection system 100 of the present invention is effective in resisting against "Replay" attack. In replay attack, an attacker reroutes the encrypted data 148 going from the storage device 102 to the host device 104 and records the encrypted data onto a recordable medium. Additionally, when the host device 104 accesses the MKB 110 embedded in the storage medium 108, the attacker also records the MKB 110 onto the same recordable medium. The copy of the MKB 110 and encrypted data 148 captured at the time of transmission may be played on a conventional media player system by presenting the encrypted data to the host device as though it was coming from a legitimate storage device. However, in the present invention, since the nonce value used by the host device to generate its decryption bus key during replay of the enciphered data will be different than the nonce value used by the storage device to generate its encryption bus key at the time of enciphering, this type of replay attack will be prevented. In other words, by using the nonce to generate the bus keys, the bus key 140 obtained by the host device 104 during subsequent access of the enciphered data will most likely be different than the bus key 124 that was previously used to encrypt the enciphered data and therefore the host device will not be able to properly decrypt the enciphered data.

[00017] In one implementation, if a set of device keys is compromised in a

way that threatens the integrity of the copy protection system, new media can be released containing an updated MKB that causes the compromised set of device keys to calculate an incorrect media key, thereby revoking its ability to work with the new media. This means that devices with the compromised set of device keys will no longer function with new media while other existing compliant devices with valid device keys will continue to work with new media.

[00018] It should be noted that there are a variety of ways to derive a secret key from public key distribution system and that the usage of media key block (MKB) is just one example of distributing cryptographic keys and the details of public key management may vary among different applications. In this regard, other types of public key distribution system can be utilized with the copy protection system of the present invention. Such is within the scope and contemplation of the present invention.

[00019] Referring to Figure 3, the operations of encrypting data prior to transmitting the data over a bus according to one embodiment of the invention are shown. When a compliant storage medium is placed within the storage device, the MKB processing logic responsible for computing a media key accesses the MKB from the storage medium (block 300). Then, the MKB processing logic generates a media key using a set of device keys assigned to the storage device and the MKB read from the storage medium (block 310). In one implementation, the MKB comprises a block of encrypted data, where each encrypted data is a secret media key encrypted with a different key. Each device key may be data of a predefined bit size (e.g., 56 bit data) that includes an index number used to indicate which encrypted data within the MKB data block the device key is configured to decrypt. By decrypting the designated portion of the MKB using the device key, a secret media key may be obtained. This means that the secret media key contained in the MKB can be obtained by any device that has a legitimate set of device keys. After the compliant storage medium has been placed in the storage device and prior to any encryption taking place, the host device generates a nonce (e.g., a random number) and sends the nonce to the

storage device. The encryption subsystem receives the nonce sent by the host device (block 320) and combines it with the media key obtained above using a one-way function to produce a bus key (block 330). Using the bus key obtained, the encryption subsystem encrypts the digital content read from the storage medium and outputs the encrypted data to the host device through the bus (block 340).

[00020] Referring to Figure 4, the operations of decrypting data transmitted over a bus according to one embodiment of the invention are shown. When the host device needs to access the storage medium in the storage device, the MKB processing logic residing within the decryption subsystem of the host device reads the MKB from the storage medium (block 400). Then in block 410, the MKB processing logic generates a media key using a set of device keys assigned to the host device and the MKB read from the storage medium. As noted earlier, the decryption subsystem generates a nonce (block 420) and sends a copy of it to the encryption subsystem (block 430) and sends another copy of it to the one-way function of the decryption subsystem. Then, the decryption subsystem combines the nonce and the media key by using the one-way function to produce a bus key (block 440). The bus key is used by the decryption subsystem to decrypt the encrypted data transmitted over the bus (block 450).

[00021] Figure 2 depicts a system 200 for protecting digital versatile discs (DVDs) from unauthorized copying according to one embodiment of the invention. In this embodiment, the copy protection system 200 uses the media key block (MKB) 210 as described above to patch scrambled contents 212 of DVD 208 to provide additional copy protection. In this regard, the format of new compliant DVDs may remain unchanged (i.e., content scramble system (CSS) scrambling is still used), except that a MKB 210 is introduced as a new data element on the disc. As noted earlier, the MKB 210 is a block of encrypted data that allows different devices using different individually-assigned device keys to extract a common secret key, called the media key. The usage of MKB 210 to patch scrambled DVD data 212 enables a protection system to be renewed (i.e., if

a set of device keys is compromised in the future, a new MKB can be used that excludes just that set of compromised device keys from the system).

[00022] As part of the copy protection system 200 of the invention, new compliant DVD drives 202 are equipped with device keys 218, MKB processing logic 220, one-way function 224 and encryption logic 228 necessary to process the MKB and extract its secret media key 222, to calculate a bus key 226 based on the media key 222 and a nonce 250, and encrypt the data 212 on the DVD 208, which is CSS scrambled, using the bus key 226. The DVD video player software 230 of the host computer 204 (e.g., host PC or DVD player) is also equipped with these additional features to access and process MKB 210 using its own set of device keys 232 to compute a secret media key 236, to calculate a bus key 242 based on the media key 236 and the nonce 252, and decrypt the data 254 transmitted by the DVD drive 202 using the bus key 242.

[00023] When a new compliant DVD-Video disc 208 is inserted into the DVD drive 202, the following key exchange procedure occurs between the DVD drive 202 and host PC 204. The DVD drive 202 reads the MKB 210 and uses its device keys 218 to calculate the media key 222. The DVD video player software 230 running on the host PC 204 sends the necessary command to the DVD drive 202 to allow it to also read the MKB 210 and use its device keys 232 to calculate the media key 236. The DVD video player software 230 selects a number (nonce) at random 238, and sends that number to the DVD drive 202 using a predefined command. The DVD drive 202 and DVD video player software 230 both calculate a common bus key 226, 242, which is derived from a cryptographic one-way function of the media key and nonce. Subsequently, the DVD video player software 230 sends requests to the DVD drive 202 to read the descramble keys 214 (e.g., CSS keys) and CSS-scrambled content 212 from the disc 208. Before sending the CSS keys 214 or CSS-scrambled content 212 to the host PC 204, the DVD drive 202 first encrypts them using a robust cipher and the bus key 226. Upon receipt of the data, the DVD video player software 230 decrypts them using the same cipher and bus key 242 and forwards the data to the descramble logic 246. The

descramble logic 246 uses the descramble keys 214 to descramble the data and forwards the data to a decompression logic 248.

[00024] For the calculation of the media key and bus key, and for the bus encryption and decryption of the CSS keys and CSS-scrambled content, a robust cipher with a large key size is used. In one implementation, the cipher is the C2 cipher, and the key size is 56 bits.

[00025] In this embodiment, the copy protection system of the present invention dramatically improves the protection for DVD-Video content by "wrapping" a robust protection scheme around the old CSS scheme. This is accomplished in a simple and novel way, using MKB technology to provide for renewal in the event that device keys are compromised in the future, and adding a nonce to protect against replay attacks.

[00026] Referring to Figure 5, the operations of decrypting and descrambling DVD contents according to one embodiment of the invention are shown. When a DVD is inserted in the DVD-ROM drive, the DVD video player software running in the host PC may request descramble keys or secret data (e.g., CSS keys) required for descrambling the scrambled content from the DVD drive (block 500). Then in block 510, the DVD drive encrypts the CSS keys read from the disc with bus key and sends them to the host PC. The CSS keys are encrypted prior to sending them over the bus to the host PC. The CSS keys are encrypted using the bus key that can also be computed by the host PC having a set of non-compromised device keys as previously discussed. In this regard, once the encrypted CSS keys have been received, the DVD video player software running in the host PC decrypts the CSS keys with the bus key (block 520). Then in block 530, the DVD video player software dispatches requests to read the CSS-scrambled content to the DVD drive. Before sending the content to the host PC, the DVD drive encrypts the scrambled content using the bus key and sends the encrypted data to the host PC (block 540). Upon receipt of the content, the DVD video player software first decrypts the data using the bus key (block 550). The output of the decryption logic is supplied to the descramble logic which performs

the CSS descramble process using the DSS keys obtained earlier (block 560).

[00027] While the foregoing embodiments of the invention have been described and shown, it is understood that variations and modifications, such as those suggested and others within the spirit and scope of the invention, may occur to those skilled in the art to which the invention pertains. The scope of the present invention accordingly is to be defined as set forth in the appended claims.

CLAIMS

What is claimed is:

1. A system comprising:

a number generator to generate a nonce; and

an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus, wherein said encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to said encryption subsystem and the nonce generated by the number generator.

2. The system of claim 1, further comprising a decryption subsystem coupled to said data bus to decrypt said encrypted data received over the data bus using a decryption bus key derived based on at least a portion of the key distribution data block, at least one device key assigned to said decryption subsystem and the nonce generated by the number generator.

3. The system of claim 1, wherein said encryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said encryption subsystem to compute a media key;

a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator; and

an encryption logic to encrypt data accessed from said storage medium using said encryption bus key.

4. The system of claim 2, wherein said decryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said decryption subsystem to compute a media key;

a one-way function to generate the decryption bus key based on said media key and the nonce generated by the number generator; and

a decryption logic to decrypt data transmitted over the data bus by using said decryption bus key.

5. The system of claim 1, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus.

6. The system of claim 2, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

7. The system of claim 2, wherein said encryption subsystem is implemented in a storage device capable of accessing data from a storage medium and said decryption subsystem is implemented in a host device capable of retrieving data from said storage device.

8. The system of claim 2, wherein said media key computed by the said encryption subsystem will be the same as the media key computed by the decryption subsystem provided that neither the device key assigned to the encryption subsystem nor the device key assigned to the decryption subsystem have been compromised.

9. The system of claim 2, wherein said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card.

10. The system of claim 2, wherein said number generator is a random number generator residing within said decryption subsystem.

11. A method comprising:

a storage device reading a key distribution data block from a storage medium;

the storage device processing at least a portion of said key distribution data block using at least one device key to compute a media key;

the storage device fetching a nonce generated by a number generator;

the storage device combining said nonce with said media key using a one-way function to generate a bus key;

the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and

the storage device transmitting the encrypted data over a data bus.

12. The method of claim 11, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a host device that does not have access to the same nonce used by the storage device to encrypted said data transmitted over the data bus.

13. The method of claim 11, further comprising decrypting the encrypted data received over the data bus.

14. The method of claim 13, wherein said decrypting the encrypted data received over the data bus comprises:

a host device reading the key distribution data block from the storage medium;

the host device processing at least a portion of the key distribution data block using at least one device key to compute a media key;

the host device fetching the nonce generated by the number generator;

the host device combining said media key with the nonce using a one-way function to generate a bus key; and

the host device decrypting said encrypted data received over the data bus using the bus key generated by the host device.

15. The method of claim 14, further comprising:

the host device requesting a descramble key required for descrambling scrambled content from said storage device;

the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device;

the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device.

the host device descrambling said decrypted data using said descramble key decrypted by said host device.

16. The method of claim 11, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

17. The method of claim 14, wherein said number generator is a random number generator residing within the host device.

18. An apparatus comprising:

a storage device to access a storage medium containing data and a key distribution data block, said storage device including a processing logic, a one-way function and an encryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said storage device to compute a media key, said one-way function combines said media key with a nonce generated by a number generator to produce a bus key and said encryption logic encrypts said data accessed from said storage medium using said bus key prior to transmitting the encrypted data via a data bus.

19. The apparatus of claim 18, further comprising a host device coupled to said storage device via said data bus, said host device including a processing

logic, a one-way function and a decryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said host device to compute a media key, said one-way function combines said media key with said nonce generated by said number generator to produce a bus key and said decryption logic decrypts said encrypted data received over the data bus using said bus key.

20. The apparatus of claim 18, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a host device that does not have access to the same nonce used by said storage device to encrypted said data transmitted over the data bus.

21. The apparatus of claim 19, wherein said media key computed by the said storage device will be the same as the media key computed by the host device provided that neither the device key assigned to the storage device nor the device key assigned to the host device have been compromised.

22. The apparatus of claim 19, wherein said number generator is a random number generator residing within said host device.

23. The apparatus of claim 19, wherein said storage device is embodied in the form of a DVD drive and said host device is embodied in the form of either a DVD player or a personal computer.

24. The apparatus of claim 19, wherein said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card.

25. The apparatus of claim 19, wherein said storage medium is embodied in the form of a DVD containing scrambled content.

26. The apparatus of claim 19, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

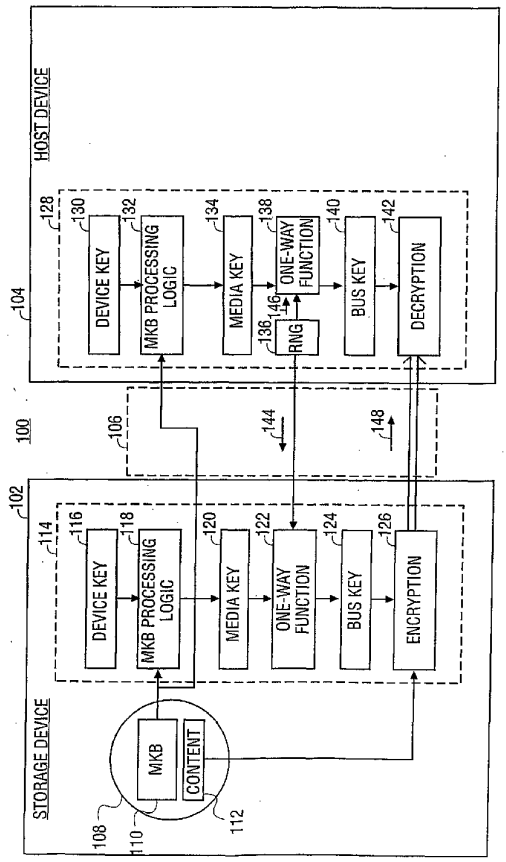

HOST DEVICE
104
128
130
DEVICE KEY
132
MKB PROCESSING LOGIC
134
MEDIA KEY
138
ONE-WAY FUNCTION
140
BUS KEY
142
DECRYPTION
136
146
RNG
100
106
144
148
102
114
116
DEVICE KEY
118
MKB PROCESSING LOGIC
120
MEDIA KEY
122
ONE-WAY FUNCTION
124
BUS KEY
126
ENCRYPTION
STORAGE DEVICE
MKB
CONTENT
108
110
112

FIG. 1

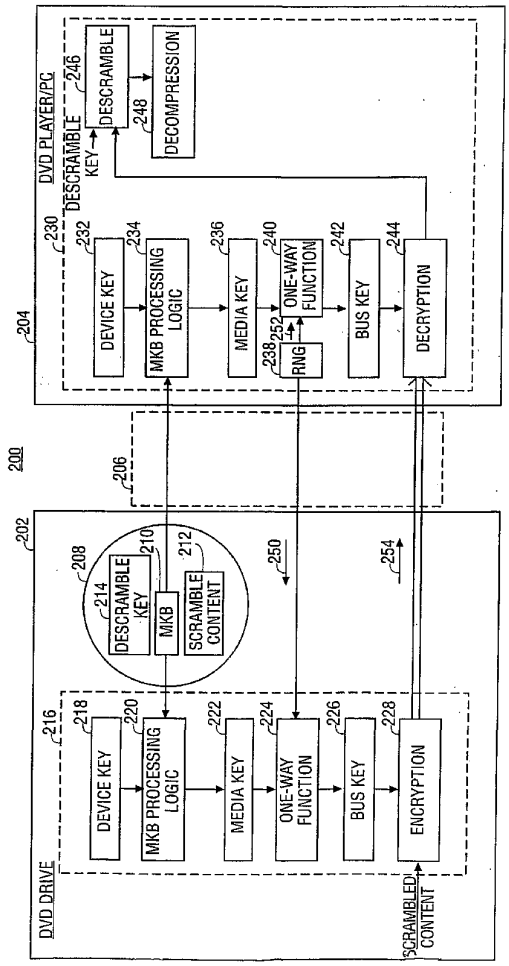

200
DVD PLAYER/PC
204
DESCRAMBLE KEY
246
DESCRAMBLE
248
DECOMPRESSION
230
232
DEVICE KEY
234
MKB PROCESSING LOGIC
236
MEDIA KEY
240
ONE-WAY FUNCTION
242
BUS KEY
244
DECRYPTION
238
252
RNG
206
202
208
210
212
214
DESCRAMBLE KEY
MKB
SCRAMBLE CONTENT
250
254
DVD DRIVE
216
218
DEVICE KEY
220
MKB PROCESSING LOGIC
222
MEDIA KEY
224
ONE-WAY FUNCTION
226
BUS KEY
228
ENCRYPTION
SCRAMBLED CONTENT

FIG. 2

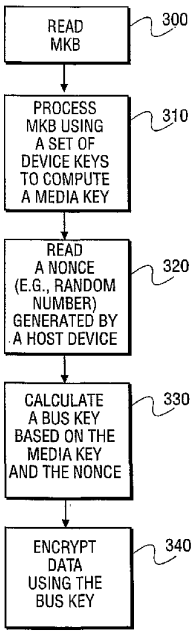

READ MKB
300
PROCESS MKB USING A SET OF DEVICE KEYS TO COMPUTE A MEDIA KEY
310
READ A NONCE (E.G., RANDOM NUMBER) GENERATED BY A HOST DEVICE
320
CALCULATE A BUS KEY BASED ON THE MEDIA KEY AND THE NONCE
330
ENCRYPT DATA USING THE BUS KEY
340

FIG. 3

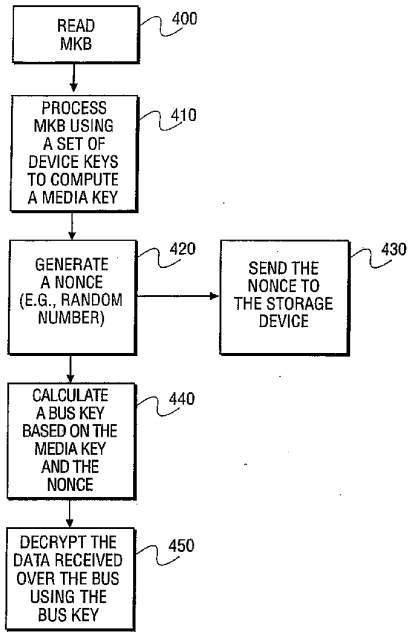

READ MKB
400
PROCESS MKB USING A SET OF DEVICE KEYS TO COMPUTE A MEDIA KEY
410
GENERATE A NONCE (E.G., RANDOM NUMBER)
420
SEND THE NONCE TO THE STORAGE DEVICE
430
CALCULATE A BUS KEY BASED ON THE MEDIA KEY AND THE NONCE
440
DECRYPT THE DATA RECEIVED OVER THE BUS USING THE BUS KEY
450

FIG. 4

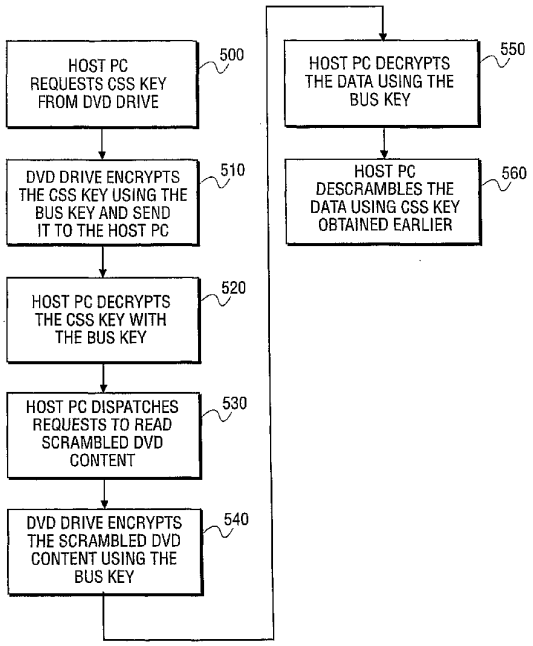

HOST PC REQUESTS CSS KEY FROM DVD DRIVE
500
DVD DRIVE ENCRYPTS THE CSS KEY USING THE BUS KEY AND SEND IT TO THE HOST PC
510
HOST PC DECRYPTS THE CSS KEY WITH THE BUS KEY
520
HOST PC DISPATCHES REQUESTS TO READ SCRAMBLED DVD CONTENT
530
DVD DRIVE ENCRYPTS THE SCRAMBLED DVD CONTENT USING THE BUS KEY
540
HOST PC DECRYPTS THE DATA USING THE BUS KEY
550
HOST PC DESCRAMBLES THE DATA USING CSS KEY OBTAINED EARLIER
560

FIG. 5

【国際公開パンフレット（コレクトバージョン）】

(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 02/080170 A3

(51) International Patent Classification⁷: G11B 20/00, H04N 7/167

(21) International Application Number: PCT/US02/07085

(22) International Filing Date: 7 March 2002 (07.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/823,423 29 March 2001 (29.03.2001) 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.; Blakely, Sokoloff, Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 et al. (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.

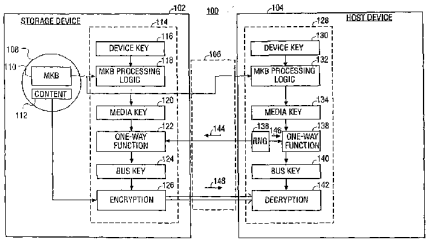
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,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

Published:
— with international search report

(88) Date of publication of the international search report:
5 June 2003

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: METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE



(57) Abstract: A system is described for protecting digital content stored (112) on a storage medium (108) from unauthorized copying. The system includes a number generator to generate a nonce, an encryption subsystem (114) and a decryption subsystem (128). The encryption subsystem encrypts data accessed from a storage medium containing a key distribution data block (MKB,110) using an encryption bus key (124) prior to transmitting the encrypted data via a data bus (106). The encryption bus key is derived based on at least a portion of the key distribution data block (110), at least one device key (116) assigned to the encryption subsystem and the nonce generated by the number generator. The decryption subsystem is coupled to the data bus to decrypt the encrypted data received over the data bus using a decryption bus key (140) derived based on at least a portion of the key distribution data block, at least one device key (130) assigned to the decryption subsystem and the nonce generated by the number generator.

WO 02/080170 A3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int al Application No
PCT/US 02/07085

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 H04N7/167

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 H04N 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, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 081 616 A (MATSUSHITA ELECTRIC IND CO LTD) 7 March 2001 (2001-03-07) page 2, line 32 - line 39 page 3, line 15 - line 19 page 7, line 14 - line 50 page 19, line 15 - line 24	1-26
A	WO 00 57636 A (MICROSOFT CORP) 28 September 2000 (2000-09-28) page 15, line 22 -page 16, line 21 page 20, line 6 - line 18 page 22, line 16 -page 23, line 9	1-26

-/--

[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
6 January 2003	13/01/2003

Name and mailing address of the ISA	Authorized officer
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	Fantini, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/07085

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 984 346 A (HITACHI EUROP LTD) 8 March 2000 (2000-03-08) abstract column 6, line 15 -column 7, line 12 column 7, line 29 - line 39 column 8, line 47 -column 9, line 46	1-26
A	INTEL CORPORATION ET AL: "Content Protection for Recordable Media Specification: DVD Book, Revision 0.94" CONTENT PROTECTION FOR RECORDABLE MEDIA SPECIFICATION: DVD BOOK, REVISION 0.94, 18 October 2000 (2000-10-18), XP002167964 the whole document	1-26

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte nal Application No
PCT/US 02/07085

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1081616	A	07-03-2001	AU	6864500 A	26-03-2001
			EP	1081616 A2	07-03-2001
			WO	0116821 A2	08-03-2001
			JP	2002015147 A	18-01-2002
			BR	0007050 A	31-07-2001
			CN	1321265 T	07-11-2001
			EP	1089241 A2	04-04-2001
			WO	0116671 A1	08-03-2001
			JP	2001155425 A	08-06-2001
			NO	20012129 A	29-06-2001
WO 0057636	A	28-09-2000	AU	3771900 A	09-10-2000
			AU	4025900 A	09-10-2000
			EP	1163794 A1	19-12-2001
			EP	1161828 A1	12-12-2001
			WO	0057636 A1	28-09-2000
			WO	0057637 A1	28-09-2000
EP 0984346	A	08-03-2000	EP	0984346 A1	08-03-2000
			JP	2000076141 A	14-03-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51)Int.Cl.[7]	FI	テーマコード（参考）
	H04L 9/00 601E	

(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) 5B017 AA03 AA06 BA07 CA09 CA16
5D044 BC04 CC04 DE17 DE50 GK17 HL08 HL11
5J104 AA13 EA23 NA42