

(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2004-510367

(P2004-510367A)

(43) 公表日 平成16年4月2日(2004.4.2)

(51) Int. Cl.⁷

H04L 9/08

G06F 12/14

H04L 9/36

F I

H04L 9/00

G06F 12/14

H04L 9/00

G01A

320B

685

テーマコード (参考)

5B017

5J104

審査請求 未請求 予備審査請求 未請求 (全 29 頁)

(21) 出願番号 特願2002-529347 (P2002-529347)
 (86) (22) 出願日 平成13年8月31日 (2001.8.31)
 (85) 翻訳文提出日 平成14年5月13日 (2002.5.13)
 (86) 国際出願番号 PCT/EP2001/010162
 (87) 国際公開番号 W02002/025410
 (87) 国際公開日 平成14年3月28日 (2002.3.28)
 (31) 優先権主張番号 00203207.6
 (32) 優先日 平成12年9月15日 (2000.9.15)
 (33) 優先権主張国 欧州特許庁 (EP)
 (81) 指定国 EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), CN, JP

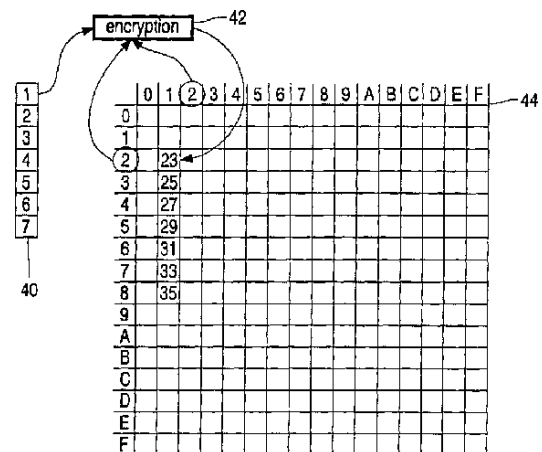
(71) 出願人 590000248
 コーニンクレッカ フィリップス エレクトロニクス エヌ ヴィ
 Koninklijke Philips Electronics N. V.
 オランダ国 5621 ペーアー アインドーフエン フルーネヴァウツウェeg 1
 Groenewoudseweg 1, 5621 BA Eindhoven, The Netherlands
 (74) 代理人 100087789
 弁理士 津軽 進
 (74) 代理人 100114753
 弁理士 宮崎 昭彦

最終頁に続く

(54) 【発明の名称】 暗号化キーとしてのデータ塊アドレスによる保護

(57) 【要約】

コンピュータが、有限サイズのデータ塊 (data chunk) に編成された秘密データに対して動作する。まず、上記各データ塊に一群の論理アドレスのうちの特定の論理アドレスが割り当てられる。次に、各データ塊は媒体上の対応する固有物理アドレスに記憶され、その際に、上記特定の論理アドレスと上記固有の物理アドレスとの間に所定の関係を維持する。次いで、コンピュータのソフトウェアプログラムは上記論理アドレスを介して上記データ塊にアクセスする。所定の関係の表示が読み出される。特に、記憶する前に、データ塊は、少なくとも当該データ塊に割り当てられたアドレスにも基づくような暗号化キーを介して暗号化される。読み取り後、データ塊は後者の暗号化キーの逆体としての解読キーを用いて解読される。上記データ塊は一樣なサイズであっても、なくてもよい。



【特許請求の範囲】

【請求項 1】

有限の大きさのデータ塊に編成された秘密データを処理するコンピュータ方法であって、

- 前記データ塊の各々に、一群の論理アドレスのうちの特定の論理アドレスを割り当てるステップと、
- 前記各データ塊を媒体上の各々の固有の物理アドレスに記憶するステップであって、その際に、前記特定の論理アドレスと前記固有の物理アドレスとの間に所定の関係を維持するような記憶するステップと、
- 前記データ塊に前記論理アドレスを介してアクセスするようなコンピュータソフトウェアプログラムを実行するステップと、

を有するコンピュータ方法において、該方法が、

- 前記記憶するステップの前に、前記データ塊を少なくとも該データ塊に割り当てられたアドレスにも基づくような暗号化キーを介して暗号化するステップと、
- 読み取りの後に、前記データ塊を前記暗号化キーの逆体としての解読キーを用いて解読するステップと、

を有していることを特徴とするコンピュータ方法。

10

【請求項 2】

請求項 1 に記載の方法において、前記アドレスが物理アドレスであることを特徴とする方法。

【請求項 3】

請求項 1 に記載の方法において、前記データ塊が複数の物理アドレスを組み合わせて使用することにより暗号化されることを特徴とする方法。

20

【請求項 4】

請求項 3 に記載の方法において、前記複数のアドレスが非連続であることを特徴とする方法。

【請求項 5】

請求項 1 に記載の方法において、前記暗号化キーが他のソース主体により提供される追加キーにも基づくものであることを特徴とする方法。

【請求項 6】

請求項 1 に記載の方法において、限られた数のコピーがライセンスされ、該限られた数だけ動作させると、前記秘密データの元のバージョンを読み取り不能にすることを特徴とする方法。

30

【請求項 7】

請求項 1 に記載の方法において、前記記憶するステップが 1 以上の物理的にアドレス指定されるロケーションをスキップし及び / 又は 1 以上の物理的にアドレス指定されるロケーションを順番的に入れ替えることにより前記データ塊の自然順序を変更することを特徴とする方法。

【請求項 8】

請求項 1 に記載の方法において、前記記憶するステップは予備処理方法を適用し、その間において、特定のデータ塊に代用物理ロケーションを割り当てる場合に適切な暗号化キーを自動的に関連付けることを特徴とする方法。

40

【請求項 9】

請求項 1 に記載の方法において、前記データ塊が一様な大きさであることを特徴とする方法。

【請求項 10】

請求項 1 に記載の方法において、更に、前記所定の関係の表現を読み取り、関連する論理アドレスと対にされた前記物理アドレスの発生を、読み取られる前記所定の関係に従うかに関してチェックし、該チェックの結果に基づいて当該媒体を認可されたものか又はそれ以外のものであるとして許容し又は拒絶することを特徴とする方法。

【請求項 11】

50

有限の大きさのデータ塊に編成された秘密データを処理する装置であって、

- 前記データ塊の各々に、一群の論理アドレスのうちの特定の論理アドレスを割り当てる割当手段と、

- 前記各データ塊を媒体上の各々の固有の物理アドレスに記憶する記憶手段であって、その際に、前記特定の論理アドレスと前記固有の物理アドレスとの間に所定の関係を維持するような記憶手段と、

- 前記データ塊に前記論理アドレスを介してアクセスするようなコンピュータソフトウェアプログラムを実行する処理手段と、

を有する装置において、該装置が、

- 前記の記憶を行う前に、前記データ塊を少なくとも該データ塊に割り当てられたアドレスにも基づくような暗号化キーを介して暗号化する暗号化手段と、

- 読み取りの後に、前記データ塊を前記暗号化キーの逆体としての解読キーを用いて解読する解読手段と、

を有していることを特徴とする装置。

【請求項 1 2】

請求項 1 1 に記載の装置において、前記アドレスが物理アドレスであることを特徴とする装置。

【請求項 1 3】

請求項 1 1 に記載の装置において、前記データ塊が複数の物理アドレスを用いて暗号化されることを特徴とする装置。

【請求項 1 4】

請求項 1 3 に記載の装置において、前記複数のアドレスが非連続であることを特徴とする装置。

【請求項 1 5】

請求項 1 1 に記載の装置において、前記暗号化キーが他のソース主体により提供される追加キーにも基づくものであることを特徴とする装置。

【請求項 1 6】

請求項 1 1 に記載の装置において、前記記憶手段が 1 以上の物理的にアドレス指定されるロケーションをスキップし及び / 又は 1 以上の物理的にアドレス指定されるロケーションを順番的に入れ替えることにより前記データ塊の自然順序を変更することを特徴とする装置。

【請求項 1 7】

請求項 1 1 に記載の装置において、前記記憶手段は予備処理方法を適用し、その間において、特定のデータ塊に代用物理ロケーションを割り当てる場合に適切な暗号化キーを自動的に関連付けることを特徴とする装置。

【請求項 1 8】

請求項 1 1 に記載の装置において、前記データ塊が一様な大きさであることを特徴とする装置。

【請求項 1 9】

請求項 1 に記載の方法を適用するように構成された暗号化装置。

【請求項 2 0】

請求項 1 に記載の方法を適用するように構成された解読装置。

【請求項 2 1】

請求項 1 に記載の方法に使用される保護された一連のデータ塊を担持するデータ担体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、有限サイズのデータ塊 (data chunk) に編成された秘密データを操作するコンピュータ方法に関する。

【0 0 0 2】

10

20

30

40

50

【従来の技術】

秘密データの多くのファイルは、限られた状況及び／又は特定の当事者のみに対して、アクセスされ及び／又は流布されねばならない。斯様な秘密性を維持するための種々の方法が提案され、しばしば、保護方法の強固さと、元の保護を与える間及び保護された情報が資格ある主体（エンティティ）により使用される際の両方において掛かるような、該方法を実施化することにより掛かる費用との間の取り引きが適用される。特別な保護方法が、富士通社に譲渡されたナカシマ他の米国特許第 5, 6 6 1, 8 0 0 号に提案されており、該方法は：

- 一様なサイズのデータ塊に編成された秘密情報を操作するコンピュータ方法であって、
 - 各データ塊に一群の論理アドレスのうちの特定の論理アドレスを割り当てるステップと、
 - 各データ塊を媒体上の対応する固有の物理アドレスに記憶し、その際に、その特定の論理アドレスと上記固有の物理アドレスとの間に所定の関係を維持するステップと、
 - 上記データ塊に上記論理アドレスを介してアクセスするようなコンピュータソフトウェアプログラムを実行するステップと、
 - 前記所定の関係の表示を読み取るステップと、
 - 関連する論理アドレスと対となる物理アドレスの発生を、読み取られる上記所定の関係に従うかについてチェックするステップと、
 - 該チェックの結果に基づいて、当該媒体を許可されたものか、それ以外ものであるとして受諾又は拒絶するステップと、
- を含む。

10

20

【0003】

今や、論理アドレスと物理アドレスとの間のストレートな変換が、しばしば、ユーザにとり過度に透明的となることがあるので、斯かる保護は、当該情報の悪意の受信者により容易に破られる可能性がある。対照的に、本発明者は、データ塊内の上記表示にも影響を与えるような手段として上記アドレスを使用することが、不変的に一層高い保護の度合いを提供し、それでいて、許可されたユーザに対しては復号の複雑さを費用及び遅延等の点で許容可能なレベルに維持することになることを認識した。

【0004】

30

【発明が解決しようとする課題】

従って、本発明の目的は、なかでも、保護されるデータの実際のアドレスを、許可されていないユーザに対する解読の複雑さに関する保護のレベルを十分なレベルにまで上昇させる手段として使用して、十分な程度のセキュリティをなし、その際に、解読キーが一旦利用可能になれば、許可されたユーザによる解読を比較的素直なものに維持することにある。

【0005】**【課題を解決するための手段】**

従って、本発明は一態様によれば請求項 1 に記載されたように特徴付けられる。特に、本発明の用途の一つは、純粹に消費者用電子機器型プラットフォーム上での（従って、明示的に如何なる汎用コンピュータシステムも使用しない）、及び／又は非専門家により主に使用されることを意図する環境におけるデジタルコンテンツの保障された記憶であり得る。更に、上記引用例に記載された物理及び論理セクタの正しい対合に関するチェックは、本発明の保障レベルの価値ある更なる上昇を示すかもしれない。しかしながら、全ての実施化が、このフィーチャの使用を期待するものではない。

40

【0006】

また、本発明は、請求項 1 に記載した方法を実施化するように構成された装置、請求項 1 に記載した方法に用いる一連の保護されたデータ塊を担持するデータ担体にも関し、それら自体は独立請求項 9、16、17 及び 18 に各々記載されている。本発明の他の有利な態様は、従属請求項に記載されている。

50

【 0 0 0 7 】

本発明の、これら及び他の態様及び利点を、以下、好ましい実施例の開示及び特に添付図面を参照して詳細に説明する。

【 0 0 0 8 】

【 発明の実施の形態 】

図 1 は、データを処理する一般的なコンピュータ型処理システムを示している。パーソナルコンピュータ 2 0 又は消費者用電子機器型装置内の専用の特殊用途プロセッサ等の中央処理装置の周りには、画像表示サブシステム 2 2、オプションとしてのプリンタサブシステム 2 4、光学的若しくは磁氣的に読み取り可能な物理的大容量媒体、即ちデータ担体 2 8 を導入するバース手段を有するようなデータ記憶サブシステム 2 6、及びキーボード又は他の手動入力サブシステム 3 0 が集中配置されている。上記光学的又は磁氣的な大容量記憶媒体は、図 1 に示すユーザ装置において復号される保護された情報を有することができ、斯かる媒体上の上記保護された情報又はデータには、該保護されたデータを使用するプログラム又は該プログラムの一部が伴っても、伴わなくてもよい。該プログラム自体は本発明の一部を構成する必要がない他の手段により保護することができ、従って、更なる工夫なしでは、該組合せは、完全にそのようにするよう許可されていない環境によっては完全に処理することはできない。

【 0 0 0 9 】

上記構成においては、簡略化のために種々の可能性のある他の設備は示されていないが、例えば音声制御、オーディオ出力、マウス、インターネット又は他の遠隔データ提示設備、及び当該データ処理システムによりアクチュエータ制御され且つ動作に関してセンサ又は他の帰還情報を提供することができる外部ハードウェアを、機能を高めるために追加することもできる。

【 0 0 1 0 】

図 2 の (a) 及び (b) は本発明による暗号化ロックの基本的な処理的使用を図示している。データセクタ 1 ~ 7 からなるデータファイル 4 0 は記憶アレイ 4 4 に記憶されるべきものであり、該アレイは例示的に共に h e x 0 から h e x F までの二次元物理アドレス範囲を有している。ここでは個々のデータの塊を表すような特定のセクタを暗号化するために、該セクタの物理アドレスが取り出され、暗号化サブシステム 4 2 に供給されるが、該サブシステムは当該アドレスを使用して、該アドレスを、暗号化処理を実行するために暗号化キーに含める。暗号化の後、上記セクタは記憶データセクタ 2 3 ないし 3 5 の 1 つとして記憶される。後者の符号は元のファイル 4 0 のものに対して変更されており、かくして、暗号化されたデータ塊の内容に対する当該暗号化の影響を表している。暗号化処理自体は、例えば R S A 又は D E S アルゴリズムに基づくもののよう、科学的及び商業的の両面で広く使用されているので、斯かる処理のこれ以上の詳細な説明は簡略化のために省略されている。上記データを読み取る際に、元の物理アドレスが、暗号化されたデータセクタと共に取り出され、次いで、後者は元の暗号化処理の逆を用いることにより解読サブシステム 4 6 において解読され、元のデータファイル 4 0 として使用するために提供される。セクタの全体、又はむしろセクタの重要な部分のみ、及び / 又はファイルを有する全セクタのうちの限られた選択のみを暗号化することもできることに注意されたい。暗号化されるデータ塊は、相互に一樣なサイズを有することもできるが、これは本発明の全ての実施例の明示的な要件ではないことにも注意されたい。

【 0 0 1 1 】

上記に対する種々の変更が可能である。第 1 に、当該データ塊が関連するコンピュータプログラムは、符号化キーに関して即座に適用するために、物理アドレスに代えて当該データ塊の論理アドレスを供給することもできる。事実、データ塊の物理アドレスは、通常、素直な論理 / 物理アドレス変換を介して見付けることができる。第 2 に、単一の複合暗号化キーの一部を集合的に構成又は生じさせるために、種々の、特に非連続的な物理アドレスの組合せを使用することもできる。第 3 に、他の、多分秘密の暗号化キー及び / 又は方法を上記のものと組み合わせて、単一の複合暗号化演算にすることもできる。更に、上記

物理アドレス自体よりは、増加される若しくは減少される物理アドレス、又は因果的及び予測的態様で実際の物理若しくは論理アドレスに関係する別のアドレスのような他のアドレスを使用することもできる。

【0012】

暗号化されたデータにアクセスするために、アプリケーション又はコンピュータプログラムは当該アドレスに基づく暗号化ロックを知らなければならない。斯様なアプリケーションは、保護されたデータの合法的なコピー又は移動のみがなされるのを保証するために信頼されるアプリケーションであろう。従って、当該アプリケーションは斯様なコピー又は移動を実行する、例えば複写生成管理組織等による認可が確かに付与されており、従って解読キー又は複数のキーを取り出すことができるかをチェックしなければならない。これに関して、図3の(a)及び(b)は、保障された及び保障されていないロックされたファイルの再配置を各々示している。図3(a)において、図2(b)に示したファイルはサブシステム46において再び解読され、続いて、暗号化サブシステム42において、変更された物理アドレスの組に基づいて更に暗号化される。これが、再配置されたデータが、関連する符号を更に変更することにより異なる情報内容を有するものとして表すことにより象徴化されている。対照的に、図3(b)は保障されない再配置を示し、該再配置により、たとえ解読が解読サブシステム45により実施されたとしても、該記憶情報は内容の重大な部分を失ってしまう。勿論、暗号化キーが論理アドレスであったなら、上記の変更された物理アドレスは論理/物理アドレス変換の変更に基づくのみのもとなり、最終的な情報は同一のままである。

10

20

【0013】

図4の(a)及び(b)は、再生の攻撃、及びこれに対する種々の救済策を示している。ここで、権限のない主体による再生攻撃は下記のように進行し得る。先ず、該主体は図3(b)に示したような暗号化されたファイルを図4(a)に示すように、何らかの可能な複写又は転写手段により他の場所にコピーし、その際に元の暗号化された情報を維持する。次に、上記主体は該元の暗号化された情報を図3(a)に示すように保障された形で移動する。最後に、該主体は前記の転写されたものを元の位置に複写し戻す。このようにして、ここでは、元の情報の2つの正しく暗号化されたものが利用可能となる。図2の元の実施例は、それ自体によっては、この方法に対しては保護せず、従って、追加の対策が必要であると思われる。

30

【0014】

充分な解決策が図4(b)により提案されている。ここでは、データセクタを書き込む信頼されるアプリケーションが、どの物理セクタが使用されるか及び/又はどの様な順番で使用されるかを制御する。ケース(1)はセクタを跳ばし、ケース(2)は2つのセクタを入れ替える。ファイルの素直なコピーを行うことは、これら変更を元に戻すことになるが、暗号化は元の物理アドレスに基づくままとなるので、後の解読は一部又は完全に使用不能な結果をもたらす。創作された媒体の場合、物理上への論理アドレスのマッピング順序をケース(3)のように変更することができる。最初のセクタアドレスを秘密キーと共に記憶する、これを秘密キーと組み合わせる、及び最初のセクタアドレスの暗号化されたテーブルを維持する等の、種々の他の斯様な対策が、当業者には添付請求項の範囲を逸脱することなしに明らかであろう。

40

【0015】

他の提案される方法は予備処理(sparring)のものであり、該予備処理は、何らかの理由で特定のセクタが読み取り不能になった場合、駆動装置が、該読み取り不能になったセクタに対してそれまで使用されていた論理セクタアドレスに他の物理アドレスを透明的に割り当てることを意味する。本発明の原理の下でデータ塊の論理アドレスが該データを暗号化するのに使用される場合は、本当のブレイクダウンは発生しない。一方、物理アドレスが使用される場合、暗号化されたファイルを読み取り可能に維持するためには、追加の対策が取られなければならない。他方、上述した予備処理方法が信頼されるアプリケーション自体で利用可能な場合、この機能は、論理セクタの物理セクタへのマッピングに

50

影響させることにより保護の程度を更に上昇させることができる。

【0016】

上記提案した方法自体はビットコピー攻撃に対しては保護を行わず、これは適用の主分野を大容量記憶装置にさせる。しかしながら、着脱式記憶媒体に関しては、これら自体はビットコピー攻撃に対しては脆弱であり、結果として、十分なデータの保護を達成するには、固有の媒体識別子の使用等の追加の対策が必要となる。後者のフィーチャは、本発明の教示内容と容易に組み合わせることができる。

【0017】

結論として、本発明は各セクタに自身の解読キーの組を持たせ、これにより特に総体的な使用可能なキーが存在しないようにすることを提案する。特に、キーからキーへの即座の変化が、試行錯誤により動作する如何なる解読方法にも高度に負担を負わせる一方、信頼されたソフトウェアは非常に容易に利用可能なキーを有することになる。外部解読キーへアクセスしても内容を自由に利用可能にすることにはならないことにも注意されたい。何故なら、外部キー自体と、該外部キーを暗号化／解読アルゴリズム内でセクタアドレスと組み合わせなければならない方法との両者が再現されねばならず、これは、事実上、煎じ詰めれば完全な信頼されたアプリケーションを再構築しなければならないこととなるからである。

【0018】

次に、図5は例示的实施例として保護されたオーディオデータのインターネット設備上での保障された伝送を示している。先ず、当該制御のサーバ側50は、音符により示すオーディオコンテンツをインターネットを介して配信するために使用される、レコードレーベルのインターネットポータルとすることができる。ここでサーバ側として示されるものは、符号化設備58、大容量記憶設備60及び伝送用暗号化設備56である。インターネット設備プロパ52は最終的にクライアント54による受信を許可し、該クライアントは続いて保障記憶設備64に記憶するための再暗号化設備62、及びここでも音符として示す上記オーディオコンテンツを再生するための解読復号設備66を有している。上記サーバ側及びクライアント側は、共に、保障されており、それらの間に保障された接続を確立するものと仮定する。上記クライアントは、該クライアントに存する又は外部世界から到来する如何なる情報も保障されるという点において保障されていると仮定する。

【0019】

図5の状況において、図6はインターネット70から取り込まれた保護されたデータの保障された記憶による、本発明の更なる有利な特徴を図示している。保障されたローカルな記憶のために、信頼されるアプリケーションTA74は、実際に必要とされる以上の媒体スペース76をファイルシステムFSに要求し、斯様にして要求したスペースのセクタアドレス78を取り込む。次いで、これらセクタはクラスタ化され、各クラスタのアドレスは上記コンテンツ提供者から受信されたキー72と組み合わせられて、関連するクラスタのデータ80を暗号化する。クラスタ内で利用可能な全てのスペースよりも少ないものしか実際には使用されず、余ったスペースは上記ファイルシステムに返却されることに注意されたい。図6は、元の内容(図2(a)の“40”参照)による7個のセクタ1ないし7、形成されたクラスタ、及び全体として要求されたスペースを示している。

【0020】

かくして、コンテンツの操作は信頼されるアプリケーションが許可するであろうものに制限され、該アプリケーションは当該ユーザ主体が有するライセンスに依存するであろう。限られた回数再生することしかライセンスされていないコンテンツは、着脱可能な媒体には書き込まれないであろう。無制限に再生するライセンスは有するが、限られたコピーのライセンスしか有さないコンテンツは、当該媒体の識別子が設けられた媒体にしか書き込まれず、該識別子が暗号化処理に使用されるであろう。コピーのライセンスの特定の型式に応じて、当該コンテンツは何れかの特定の時点において、単一の媒体上、又は単一の装置上のみ、又は限られた組の媒体及び／又は装置のうちの幾つかのもの上に存在し得る。コピーはローカルソース、即ち信頼されるアプリケーションにおいてのみ発生することが

10

20

30

40

50

できる。この信頼されるアプリケーションは上記の保護されたデータと同一のシステムパーティションに存在し、両者は同一の論理アドレス空間に縛られることに注意されたい。当該コンテンツを或る他の媒体で1回再生するライセンスは、元の媒体から1回のみ抽出することができるが、該元の媒体が、例えばレーザを十分に高い出力率で動作させることによりT O Cが破壊されるようなC D - R上の“T O C消却”手順によるように、後のアクセスに対して読み取り不能にされ得ることのみを前提とする。

【図面の簡単な説明】

【図 1】

図 1 は、データを処理する通常のコンピュータ型処理システムである。

【図 2】

図 2 の (a) 及び (b) は、暗号化ロックの基本的処理使用を図示する。

【図 3】

図 3 の (a) 及び (b) は、ロックされたファイルの保障された及び保障されていない再配置を図示する。

【図 4】

図 4 の (a) 及び (b) は、再生攻撃及び該攻撃に対する種々の救済策を図示する。

【図 5】

図 5 は、インターネット設備上での保護されたデータの保障された伝送を図示する。

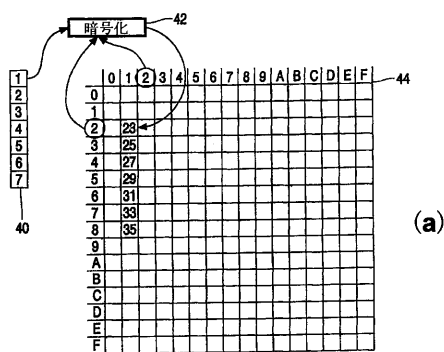
【図 6】

図 6 は、インターネット設備から取り出された保護されたデータの安全な記憶を図示する

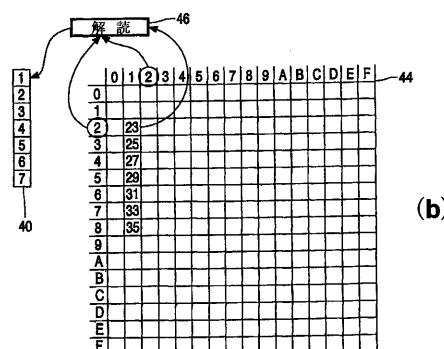
10

20

【図 2】

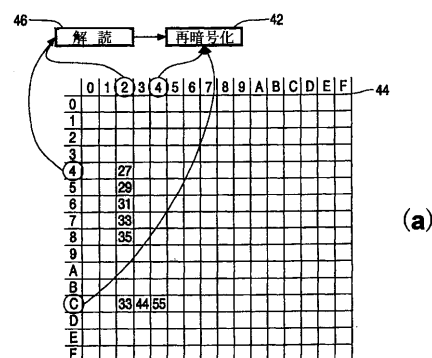


(a)

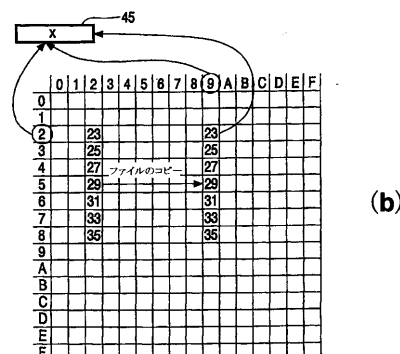


(b)

【図 3】



(a)



(b)

【図 4】

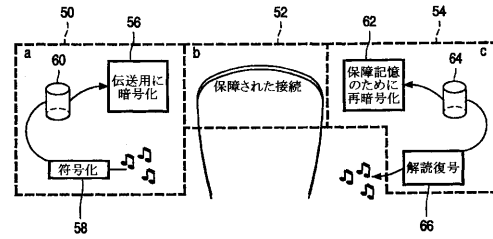
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2			23									23				
3			25									25				
4			27									27				
5			29									29				
6			31									31				
7			33									33				
8			35									35				
9																
A																
B																
C			33	44	55	66	77	88	99							
D																
E																
F																

(a)

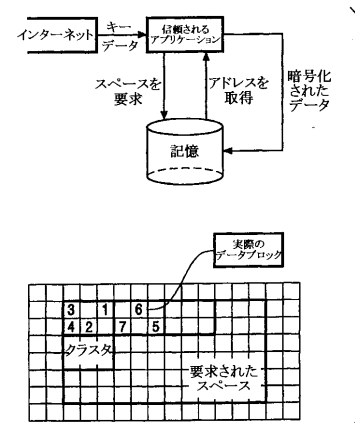
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2			23													
3			25													
4			(1)													
5			28													
6			30													
7			33													
8			33													
9			36													
A																
B																
C																
D																
E																
F																

(b)

【図 5】



【図 6】



【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
28 March 2002 (28.03.2002)

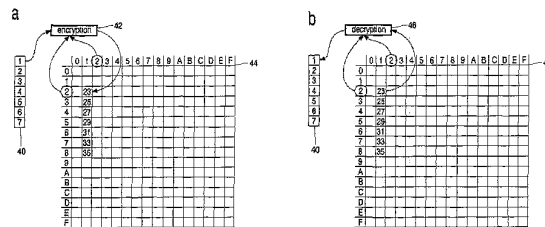
PCT

(10) International Publication Number
WO 02/25410 A2

- (51) International Patent Classification: G06F 1/00 (74) Agent: HOEKSTRA, Jelle; INTERNATIONAAL OC-
TROOIBUREAU B.V., Prof Holstlaan 6, NL-5656 AA
Eindhoven (NL).
- (21) International Application Number: PCT/EP01/10162
- (22) International Filing Date: 31 August 2001 (31.08.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 00203207.6 15 September 2000 (15.09.2000) EP
- (71) Applicant: KONINKLIJKE PHILIPS ELECTRON-
ICS N.V. (NL/NL); Groenewoudseweg 1, NL-5621 BA
Eindhoven (NL).
- (72) Inventor: FONTIJN, Wilhelmus, F. J.; Prof. Holstlaan
6, NL-5656 AA Eindhoven (NL).
- (81) Designated States (national): CN, JP.
- (84) Designated States (regional): European patent (AT, BE,
CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE, TR).
- Published:
— without international search report and to be republished
upon receipt of that report

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

(54) Title: PROTECT BY DATA CHUNK ADDRESS AS ENCRYPTION KEY



(57) Abstract: A computer operates on confidential data that are organized in finite-sized data chunks. First, each said data chunk is assigned a particular logical address of a set of logical addresses. Next, each data chunk is stored at a respective unique physical address on a medium, whilst maintaining a predetermined relationship between the particular logical address and the unique physical address. Next, a computer software program accesses the chunks through the logical addresses. A representation of predetermined relationship is read. In particular, before storing, a data chunk is encrypted through an encryption key that is at least co-based on an address assigned to the data chunk. After reading, a data chunk is decrypted through usage of a decryption key as an inverse of the latter encryption key. The chunks may or may not be uniform-sized.

WO 02/25410 A2

WO 02/25410

PCT/EP01/10162

1

Protect by data chunk address as encryption key

BACKGROUND OF THE INVENTION

- The invention relates to a computer method for operating confidential data that are organized in finite-sized data chunks. Many files of confidential data should have access thereto and/or dissemination thereof limited to restricted situations and/or particular parties only. Various schemes for conserving such confidentiality have been proposed, and often a trade-off will be applied between the robustness of the protection scheme and the cost incurred through implementation thereof, such as incurred both during the providing of the original protection, and also at the time when the protected information is being used by an entity entitled to do so. A particular protective policy has been proposed in US Patent 5,661,800 to Nakashima et al, and assigned to Fujitsu Limited, such encompassing:
- a computer method for operating confidential data that are organized in uniform-sized data chunks, and comprising the steps of:
 - assigning to each data chunk a particular logical address of a set of logical addresses;
 - 15 - storing each data chunk at a respective unique physical address on a medium, whilst maintaining a predetermined relationship between its particular logical address and the unique physical address;
 - executing a computer software program that accesses the chunks through the logical addresses;
 - 20 - reading a representation of the predetermined relationship;
 - checking occurrence of the physical addresses as being paired to associated logical addresses for conformance to the predetermined relationship as being read; and
 - on the basis of an outcome of the checking, accepting or rejecting the instant medium as an authorized version or otherwise.
- 25 Now often, the straight translating between logical address and physical address is overly transparent to a user, so that the protection may be broken easily by a malevolent receiver of the information. In contradistinction, the present inventor has recognized that using the address as a means for also influencing the *representation* inside the data chunk will offer a degree of protection that is invariably much higher, while

WO 02/25410

PCT/EP01/10162

2

nevertheless keeping the decoding complexity for an authorized user at an acceptable level as regarding costs, delay, and the like.

SUMMARY TO THE INVENTION

5 In consequence, amongst other things, it is an object of the present invention to use the actual address of protected data as a means for raising the level of protection regarding decoding complexity to an *unauthorized* user to an adequate level for so effecting a sufficient degree of security, while keeping decoding by an *authorized* user relatively straightforward, once the decoding key has become available.

10 Now therefore, according to one of its aspects the invention is characterized according to the recitation presented in Claim 1. In particular, one of the applications of the present invention can be the secure storage of digital content on a purely consumer electronics based platform, thus explicitly without the use of any general computer system, and/or in an environment that is principally intended for use by non-professional persons.

15 Furthermore, the check on the correct pairing of physical and logical sectors as recited in the reference could represent a valuable further raising of the security level of the present invention. However, not every implementation is expected to use this feature.

The invention also relates to apparatus arranged for implementing the method according to Claim 1, and to a data carrier carrying a set of protected data chunks for being
20 used in the method as claimed in Claim 1, and by themselves being claimed in independent Claims 9, 16, 17 and 18, respectively. Further advantageous aspects of the invention are recited in dependent Claims.

BRIEF DESCRIPTION OF THE DRAWING

25 These and further aspects and advantages of the invention will be discussed more in detail hereinafter with reference to the disclosure of preferred embodiments, and in particular with reference to the appended Figures that show:

Figure 1, a general computer-based processing system for operating data;
Figures 2a, 2b illustrate the basic process use of the encryption lock;
30 Figures 3a, 3b illustrate secured and unsecured relocation of a locked file;
Figures 4a, 4b illustrate a replay attack and various remedies thereagainst;
Figure 5 illustrates secured transport of the protected data on an internet facility;

WO 02/25410

PCT/EP01/10162

3

Figure 6 illustrates secure storage of protected data retrieved from an internet facility.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

5 Figure 1 illustrates a general computer-based processing system for operating data. Centered around a central processing unit such as a personal computer 20 or a dedicated special purpose processor in a consumer-electronics oriented device are an image display subsystem 22, an optional printer subsystem 24, a data storage subsystem 26, such as having
10 berth means for introducing an optically or magnetically readable physical mass medium or data carrier 28, and a keyboard or other manual entry subsystem 30. The optical or magnetical mass storage medium may in fact carry the protected information for being decoded in the user apparatus shown in Figure 1, and the protected information or data thereon may or may not be accompanied by the program or by a part thereof that will use the protected data. In its turn, the program itself may be protected by other means that need not
15 form part of the invention, so that without further measures, the combination cannot fully be operated by an environment that is not fully entitled to do so.

 In the arrangement, various possible further facilities have not been shown for brevity but may be added for enhancing functionality, such as speech control, audio output, mouse, internet or other remote data presentation facilities, and external hardware that is
20 actuator-controlled by the data processing system and which can present sensor or other feedback information as regarding its operation. The prime functionality of the system may be consumer audio/video rendering, data processing of a more general character, games, and other.

 Figures 2a, 2b illustrate the basic process use of the encryption lock according
25 to the present invention. A data file 40, consisting of data sectors 1 through 7, is to be stored in a storage array 44 that by way of example has bidimensional physical address ranges both running from hex0 through hexF. For encrypting of a particular sector, that here represents an individual chunk of data, its physical address is retrieved, fed to an encryption subsystem 42 that uses the address in question for including it into an encryption key for therewith
30 executing an encryption process, and after encryption, the sector is stored as one of stored data sectors 23 through 35. The latter numerals have been changed with respect to those of the original file 40, for so symbolizing the influence of the encrypting on the content of the encrypted data chunk. By itself, encryption processes have been in wide use, both scientifically and commercially, such as being based for example on the RSA and DES

WO 02/25410

PCT/EP01/10162

4

algorithms, and further detailing of such processes has been left out for brevity. Upon reading the data, the original physical address is retrieved, as well as the encrypted data sectors, the latter are then decrypted by using the inverse of the original encryption process in decrypting subsystem 46 and presented for use as original data file 40. Note that the whole sector, or rather only a critical part thereof, and/or only a limited selection amongst all of the sectors comprising a file may be encrypted. Note that the encrypted data chunks may have mutually uniform sizes, but this is not an explicit requirement of all embodiments of the present invention.

Various amendments to the above are feasible. In the first place, the computer program to which the data chunks are associated, may present the logical addresses of the data chunks instead of their physical addresses for immediate application for the encoding key. In fact, the physical address of the data chunk is generally found through a straightforward logical-to-physical address translation. Next, a combination of various, and in particular, non-contiguous physical addresses may be used for collectively constituting or causing part of a single composite encryption key. Third, other and possibly secret encryption keys and/or methods may be combined with the above into a single composite encryption operation. Further, another address than the physical address itself may be used, such as an incremented or decremented physical address, or another address that in a causal and predictable manner relates to the actual physical or logical address.

To access the encrypted data, the application or computer program must be aware of the address-based encryption lock. Such application would be a trusted application for ensuring that only legitimate copying and/or moving of the protected data can take place. Therefore, the application must check that it has indeed been given authority to execute such copying or moving, such as by a copy generation management organization, so that it will be able to retrieve the decryption key or keys. In this ambit, Figures 3a, 3b illustrate secured and unsecured locked file relocation, respectively. In Figure 3a, the file as shown in Figure 2b is again decrypted in subsystem 46, followed by a further encryption in encryption subsystem 42, be it on the basis of an amended set of physical addresses. Such is symbolized by representing the relocated data sectors as having a different information content by further changing the associated numerals. Figure 3b in contrast illustrates unsecured relocation, by which the stored information, even if decryption will be undertaken by decryption subsystem 45, may have lost a significant part of its content. Of course, if the encryption key was the *logical address*, the amended physical address is only based on amending the logical-to-physical address translation, and the eventual information remains the same.

WO 02/25410

PCT/EP01/10162

5

Figures 4a, 4b illustrate a replay attack and various remedies thereagainst. Now, a replay attack by an unauthorized entity can proceed as follows. First it will copy, as in Figure 4a, the encrypted file shown in Figure 3b, to another location, according to some feasible copying or transfer mechanism, while also retaining the original encrypted information. Next, it will move the original encrypted information *securely* as shown in Figure 3a. Finally, it will copy the transferred version back to the original location. In this manner, there will now be two correctly encrypted versions available of the original information. The original embodiment of Figure 2 by itself does not protect against this scheme, so that additional measures would appear desirable.

An adequate solution is proposed by Figure 4b. Herein, the trusted application that writes the data sectors, will control which physical sectors will be used and/or in what sequence. Case (1) will skip a sector, whereas case (2) interchanges two sectors. The making of a straightforward copy of the file will undo these amendments, but the encryption remains based on the original physical addresses, so that subsequent decrypting will present results that are partly or fully unusable. In the case of authored media, the sequencing of mapping the logical addresses on the physical can be changed such as in case (3). Various further such measures would appear to the skilled art person while not exceeding the scope of the appended Claims, such as storing the first sector address with the secret key, combining it with the secret key, and keeping an encrypted table of first sector addresses.

Another proposed mechanism is that of *sparing*, which means that if for some reason a particular sector becomes unreadable, the drive apparatus will transparently assign another physical sector to the logical sector address that was used up to then for the now unreadable sector. If the logical address of the chunk is used to encrypt the data under the principles of the present invention, no real breakdown occurs. If on the other hand, the *physical* address is used, additional measures must be taken to maintain the encrypted file readable. On the other hand, if the above recited *sparing* mechanism is available to the trusted application itself, this feature may further raise the degree of protection by influencing the mapping of the logical sectors on the physical sectors.

Note that the above proposed scheme by itself does not protect against bit-copy attacks, which would make its prime field of application mass storage devices. As regarding removable storage media however, these would by themselves vulnerable to a bit-copy attack, and in consequence, additional measures, such as the use of a unique medium identifier, would be required to achieve adequate data protection. The latter feature could readily be combined with the teachings of the present invention.

WO 02/25410

PCT/EP01/10162

6

Concluding, the present invention proposes to let each sector have its own set of decryption keys, so that in particular, there is no overall useable key. Notably, the rapid changes from key to key will highly tax any decryption methods that operate by trial and error, whereas trusted software will have the keys extremely readily available. Note also that access to an external decryption key will still not make the content freely available, because both the external key itself and also the manner in which it must be combined with the sector address in the encryption/decryption algorithm must be reproduced, which in fact boils down to having to rebuild the entire trusted application.

Now, by way of an exemplary embodiment, Figure 5 illustrates secured transport of the protected audio data on an Internet facility. First, the server side 50 of control may be an Internet Portal of a Record Label, used to distribute audio content, which has been symbolized by musical notes, via the Internet. Shown here at the server side are encoding facility 58, mass storage facility 60, and encrypting for transport facility 56. The Internet facility proper 52 will eventually allow reception by client 54, that in its turn has re-encrypting facility 62 for subsequent storage in secure storage facility 64, and decrypting-decoding facility 66 for reproducing the audio content, that is again symbolized by musical notes. Both the server side and also the client side are assumed to be secure, for so establishing a secure connection therebetween. The client is assumed to be secure in the sense that any information residing therein or arriving from the outer world, is also secure.

In the context of Figure 5, Figure 6 illustrates a further advantageous feature of the present invention through a secure storage of protected data retrieved from an Internet 70. For secure local storing, the Trusted Application TA 74 claims more medium space 76 from the File System FS than actually needed, and will retrieve the sector addresses 78 of the space so claimed. Then, the sectors are clustered and the addresses of each cluster are combined with the key 72 received from the content provider to encrypt the data 80 for the associated cluster. Note that less than all available space in a cluster will actually be used, and superfluous space may be returned to the File System. Figure 6 at right shows the seven sectors 1 through 7 through their original content (cf. Figure 2a "40"), the cluster formed, and the totally claimed space.

The manipulation of the content is now restricted to what the Trusted Application will allow, which in turn will depend on the license that the user entity in question has. Content licensed to be played only a limited number of times may not be written to removable media. Content with a license for unlimited replay, but with a restricted copy license may only be written to media that have been provided with an identifier of the

WO 02/25410

PCT/EP01/10162

7

medium in question, which identifier will then be used in the encryption process. Depending on the specific type of copy license, at any particular time the content may be present on a single medium, or on a single device only, or on several ones of a limited set of media and/or devices. A copy can only be generated at the local source, the Trusted Application. Note that
5 this Trusted Application will reside at the same system partition as the protected data, and both are bound to the same logical address space. A license to reproduce the content a single time on a certain other medium may be extracted only once from the original medium, but provided only that the original medium can be made unreadable for later access, such as by a
10 "Burning TOC" procedure on a CD-R, in which procedure the TOC will be destroyed by operating the laser at a sufficiently high power rating.

WO 02/25410

PCT/EP01/10162

8

CLAIMS:

1. A computer method for operating confidential data that are organized in finite-sized data chunks, said method comprising the steps of:
 - assigning to each said data chunk a particular logical address of a set of logical addresses;
 - 5 - storing each said data chunk at a respective unique physical address on a medium, whilst maintaining a predetermined relationship between said particular logical address and said unique physical address;
 - and executing a computer software program that accesses the chunks through said logical addresses;
 - 10 said method being characterized by the following steps:
 - before said storing, encrypting a said data chunk through an encryption key that is at least co-based on an address assigned to said data chunk,
 - and after said reading, decrypting a said data chunk through usage of a decryption key as an inverse of the latter encryption key.
 - 15
2. A method as claimed in Claim 1, wherein said address is a physical address.
3. A method as claimed in Claim 1, wherein said data chunk is encrypted through using a plurality of physical addresses in combination.
- 20 4. A method as claimed in Claim 3, wherein said plurality of addresses are non-contiguous.
5. A method as claimed in Claim 1, wherein said encryption key is co-based on an additional key provided by a further source entity.
- 25 6. A method as claimed in Claim 1, wherein a limited number of copyings has been licensed, and furthermore rendering upon actuating said limited number an original version of the confidential data unreadable.

WO 02/25410

PCT/EP01/10162

9

7. A method as claimed in Claim 1, wherein said storing amends a natural sequence of chunks through skipping one or more and/or sequentially interchanging of one or more physically addressed locations.

5

8. A method as claimed in Claim 1, wherein said storing applies a *sparing* mechanism whilst automatically associating an appropriate encryption key when assigning a substitute physical location to a particular data chunk.

10 9. A method as claimed in Claim 1, wherein said chunks are uniform-sized.

10. A method as claimed in Claim 1, and furthermore reading a representation of said predetermined relationship, checking occurrence of said physical addresses as being paired to associated logical addresses for conformance to said predetermined relationship as being read, and on the basis of an outcome of said checking, accepting or rejecting said instant medium as an authorized version or otherwise.

15

11. An apparatus for operating confidential data that are organized in finite-sized data chunks, said apparatus comprising:

20

- assigning means for assigning to each said data chunk a particular logical address of a set of logical addresses;

- storing means for storing each said data chunk at a respective unique physical address on a medium, whilst maintaining a predetermined relationship between said particular logical address and said unique physical address;

25

- processing means for executing a computer software program that accesses said chunks through said logical addresses;

said apparatus being characterized by comprising:

- encrypting means for before said storing, encrypting a said data chunk through an encryption key that is at least co-based on an address assigned to said data chunk,

30

- decrypting means for after said reading, decrypting a said data chunk through usage of a decryption key as an inverse of the latter encryption key.

12. An apparatus as claimed in Claim 11, wherein said address is a physical address.

WO 02/25410

PCT/EP01/10162

10

13. An apparatus as claimed in Claim 11, wherein said data chunk is encrypted through using a plurality of physical addresses.
- 5 14. An apparatus as claimed in Claim 13, wherein said plurality of addresses are non-contiguous.
15. An apparatus as claimed in Claim 11, wherein said encryption key is co-based on an additional key provided by a further source entity.
- 10 16. An apparatus as claimed in Claim 11, wherein said storing amends a natural sequence of chunks through skipping one or more and/or sequentially interchanging of one or more physically addressed locations.
- 15 17. An apparatus as claimed in Claim 11, wherein said storing applies a *sparing* mechanism whilst automatically associating an appropriate encryption key when assigning a substitute physical location to a particular data chunk.
18. An apparatus as claimed in Claim 11, wherein said chunks are uniform-sized.
- 20 19. An encrypting apparatus arranged for application in a method as claimed in Claim 1.
20. A decrypting apparatus arranged for application in a method as claimed in
- 25 Claim 1.
21. A data carrier carrying a protected set of data chunks for being used in a method as claimed in Claim 1.

WO 02/25410

PCT/EP01/10162

1/5

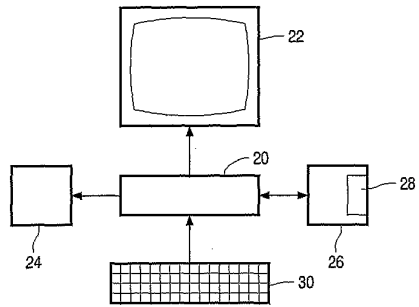


FIG. 1

WO 02/25410

PCT/EP01/10162

2/5

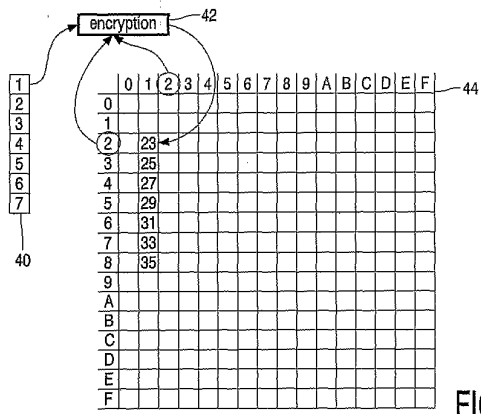


FIG. 2a

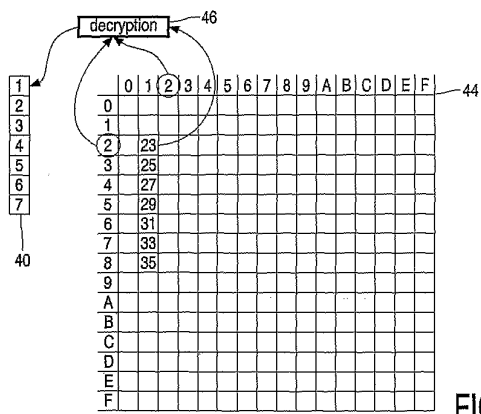
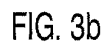
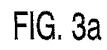


FIG. 2b



WO 02/25410

PCT/EP01/10162

4/5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2			23								23					
3			25								25					
4			27								27					
5			29								29					
6			31								31					
7			33								33					
8			35								35					
9																
A																
B																
C			33	44	55	66	77	88	99							
D																
E																
F																

FIG. 4a

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2			23								23					
3			25								25					
4			(1) ↓								28					
5			28								30					
6			30								33					
7			33								33					
8			33								35					
9			36													
A																
B																
C																
D																
E																
F																

FIG. 4b

WO 02/25410

PCT/EP01/10162

5/5

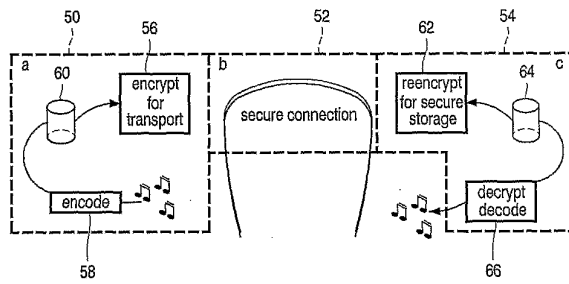


FIG. 5

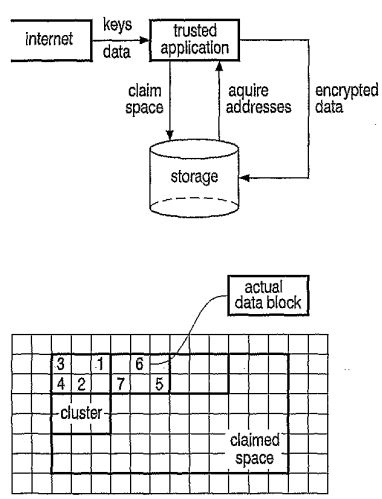


FIG. 6

【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
28 March 2002 (28.03.2002)

PCT

(10) International Publication Number
WO 02/025410 A3

(51) International Patent Classification: G06F 1/00, 12/14

(74) Agent: HOEKSTRA, Jelle; INTERNATIONAAL OC-
TROOIBUREAU B.V., Prof. Houtlaan 6, NL-5656 AA
Eindhoven (NL).

(21) International Application Number: PCT/JP01/10162

(22) International Filing Date: 31 August 2001 (31.08.2001)

(81) Designated States (national): CN, JP.

(25) Filing Language: English

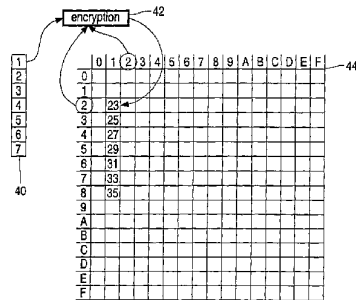
(84) Designated States (regional): European patent (AT, BE,
CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE, TR).

(26) Publication Language: English

(30) Priority Data: 00203207.6 15 September 2000 (15.09.2000) EP

Published:
with international search report(71) Applicant: KONINKLIJKE PHILIPS ELECTRON-
ICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA
Eindhoven (NL).(88) Date of publication of the international search report:
20 March 2003(72) Inventor: FONTIJN, Wilhelmus, F., J.; Prof. Houtlaan
6, NL-5656 AA Eindhoven (NL).For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: PROTECT BY DATA CHUNK ADDRESS AS ENCRYPTION KEY



(57) Abstract: A computer operates on confidential data that are organized in finite-sized data chunks. First, each said data chunk is assigned a particular logical address of a set of logical addresses. Next, each data chunk is stored at a respective unique physical address on a medium, whilst maintaining a predetermined relationship between the particular logical address and the unique physical address. Next, a computer software program accesses the chunks through the logical addresses. A representation of predetermined relationship is read. In particular, before storing, a data chunk is encrypted through an encryption key that is at least co-based on an address assigned to the data chunk. After reading, a data chunk is decrypted through usage of a decryption key as an inverse of the latter encryption key. The chunks may or may not be uniform-sized.

WO 02/025410 A3

【国際調査報告】

INTERNATIONAL SEARCH REPORT		Inventor's Name PCT/EP 01/10162
A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G06F1/00 G06F12/14		
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 G06F G11B		
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, INSPEC		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	WO 00 55736 A (KONINKL PHILIPS ELECTRONICS NV ; STARING ANTONIUS A M (NL)) 21 September 2000 (2000-09-21) the whole document	1-5, 7, 9, 11-16, 18-21
Y	US 5 661 800 A (NAITO KAZUNORI ET AL) 26 August 1997 (1997-08-26) column 1, line 41 -column 2, line 31 column 11, line 5 -column 13, line 32	1, 2, 8, 10-12, 17
Y	GB 2 264 373 A (EUROLOGIC RESEARCH LIMITED) 25 August 1993 (1993-08-25) page 2, line 26 -page 3, line 27	1, 2, 8, 10-12, 17
A	EP 0 899 733 A (SONY DADC AUSTRIA AG) 3 March 1999 (1999-03-03) page 3, paragraph 23 -page 4, paragraph 34	1-21
☐ Further documents are listed in the continuation of box C. ☒ 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 doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document relating 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 *Z* document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
27 November 2002		10/12/2002
Name and mailing address of the ISA European Patent Office, P.B. 5018 Patentkan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-5016		Authorized officer Nielsen, O

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.
PCT/EP 01/10162

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0055736	A	21-09-2000	WO 0055861 A1 21-09-2000 WO 0055736 A1 21-09-2000 EP 1076857 A1 21-02-2001 EP 1086467 A1 28-03-2001
US 5661800	A	26-08-1997	JP 7262001 A 13-10-1995 US 6199148 B1 06-03-2001 US 5930825 A 27-07-1999
GB 2264373	A	25-08-1993	NONE
EP 0899733	A	03-03-1999	EP 0899733 A1 03-03-1999 AT 199990 T 15-04-2001 AU 750499 B2 18-07-2002 AU 8194998 A 11-03-1999 BR 9806518 A 13-03-2001 CA 2245232 A1 28-02-1999 CN 1219728 A 16-06-1999 DE 69704352 D1 26-04-2001 DE 69704352 T2 12-07-2001 ES 2155230 T3 01-05-2001 JP 11250512 A 17-09-1999 SG 71803 A1 18-04-2000

フロントページの続き

(74)代理人 100121083

弁理士 青木 宏義

(72)発明者 フォンタイン ウィルヘルムス エフ ジェイ

オランダ国 5 6 5 6 アーアー アインドーフエン プロフ ホルストラーン 6

F ターム(参考) 5B017 AA03 BA07 CA16

5J104 AA12 AA16 EA04 EA15 NA02 NA27 PA14