(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2010-509662
(P2010-509662A)
(43)公表日　平成22年3月25日(2010.3.25)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	540P	5B017
		G06F	12/14	540A	

審査請求 有　予備審査請求 未請求　（全 24 頁）

(21)出願番号	特願2009-535501 (P2009-535501)
(86)(22)出願日	平成19年11月6日 (2007.11.6)
(85)翻訳文提出日	平成21年6月23日 (2009.6.23)
(86)国際出願番号	PCT/US2007/083763
(87)国際公開番号	WO2008/127408
(87)国際公開日	平成20年10月23日 (2008.10.23)
(31)優先権主張番号	11/598,173
(32)優先日	平成18年11月8日 (2006.11.8)
(33)優先権主張国	米国 (US)

(71)出願人　595168543
マイクロン　テクノロジー，　インク．
アメリカ合衆国，アイダホ州　８３７１６－９６３２，　ボイズ，　サウス　フェデラル　ウェイ　８０００
(74)代理人　100106851
弁理士　野村　泰久
(74)代理人　100074099
弁理士　大菅　義之
(72)発明者　アスナアシャリ，メディー
アメリカ合衆国，カリフォルニア州　９４５２６，ダンビル，モンテゴ　ドライブ　２６８

Fターム(参考)　5B017 AA03　BA07　CA11　CA14

最終頁に続く

(54)【発明の名称】外部不揮発性メモリに記憶された情報の暗号化のための方法およびシステム

(57)【要約】
ホストと不揮発性メモリの間で情報をやり取りするための制御装置を含む不揮発性記憶システムが記載される。制御装置は、制御装置の外部に位置する、不揮発性メモリデバイスと情報をやり取りするための暗号化／復号エンジンを含む。エンジンは、不揮発性メモリデバイスに記憶される情報を、記憶前に暗号化するために第一キーを使用し、記憶された暗号化情報を検索後に復号するために第一キーをさらに使用する。あるいは、不揮発性メモリ内に記憶された情報の安全性をさらに強化するために、第二キーが第一キーと併用される。

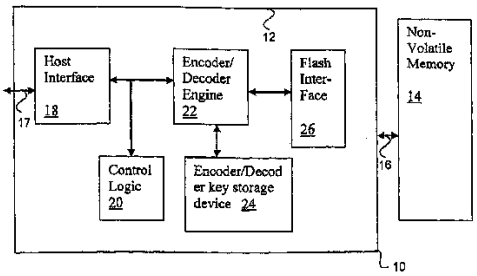


FIG. 1(a)

【特許請求の範囲】
【請求項１】
ホストと不揮発性メモリの間で情報をやり取りするための不揮発性記憶システムで利用される制御装置であり、
前記制御装置の外部に位置し、前記不揮発性メモリと情報をやり取りするための暗号化／復号エンジンを含み、前記エンジンは、前記不揮発性メモリに記憶される情報を記憶前に暗号化するためにキーを使用し、前記不揮発性メモリからの検索後に暗号化情報を復号するために前記キーを使用する、
ことを特徴とする制御装置。
【請求項２】
前記キーはマスターキーである、請求項１記載の制御装置。
【請求項３】
前記エンジンによって、前記不揮発性メモリ内の所定場所に暗号化データキーが記憶され、前記暗号化データキーは前記マスターキーを用いて前記エンジンによって作成されており、前記記憶された暗号化データキーは、前記所定場所から検索され、前記マスターキーを用いて前記エンジンによって復号され、前記所定場所以外に位置する前記不揮発性メモリから検索された情報を復号するために使用される、請求項２記載の制御装置。
【請求項４】
前記マスターキーと前記データキーを前記エンジンに選択的に提供するように構成されたマルチプレクサをさらに含む、請求項３記載の制御装置。
【請求項５】
前記所定場所は、前記システムのユーザーが記憶させようとするデータ以外の情報を記憶するためのプライベートエリアである、請求項３記載の制御装置。
【請求項６】
一つよりも多くのプライベートエリアが指定される、請求項５記載の制御装置。
【請求項７】
前記プライベートエリアの各々は、それに固有の暗号化データキーに関連する、請求項６記載の制御装置。
【請求項８】
前記暗号化データキーを作成するために前記エンジンによって受け取られるように構成された乱数を作成するための乱数発生器をさらに含む、請求項３記載の制御装置。
【請求項９】
前記マスターキーを作成するための乱数発生器をさらに含む、請求項２記載の制御装置。
【請求項１０】
前記データキーおよび／または前記マスターキーを記憶するためのエンコーダ／デコーダキー記憶デバイスをさらに含む、請求項９記載の制御装置。
【請求項１１】
前記乱数発生器によって作成された固有の乱数を記憶するための不揮発性メモリをさらに含む、請求項１０記載の制御装置。
【請求項１２】
前記暗号化データキーは前記プライベートエリアから検索され、前記データキーは前記エンジンによって復号され、前記プライベートエリア以外に位置する前記不揮発性メモリから検索された情報を復号するために使用される、請求項５記載の制御装置。
【請求項１３】
不揮発性メモリと、
ホストと前記不揮発性メモリの間に、その間で情報をやり取りするために接続され、前記不揮発性メモリの外部に位置する制御装置と、
を含み、
前記制御装置は、前記不揮発性メモリに暗号文で情報を転送するための暗号化／復号エ

ンジンを含み、前記エンジンは、記憶前に前記暗号文を作成することによって、前記不揮発性メモリに記憶される情報を暗号化するためにキーを使用し、前記記憶された情報の検索後に前記記憶された暗号文を復号するために前記キーを使用することによって平文を提供する、
ことを特徴とする、不揮発性メモリシステム。
【請求項１４】
前記キーはマスターキーである、請求項１３記載の不揮発性メモリシステム。
【請求項１５】
ユーザー情報以外の情報を記憶するための、前記不揮発性メモリ内で指定されたプライベートエリアから、暗号化データキーが検索され、前記データキーは前記エンジンによって復号され、前記プライベートエリア以外に位置する前記不揮発性メモリから検索された情報を復号するために使用される、請求項１３記載の不揮発性メモリシステム。
【請求項１６】
前記制御装置は、前記データキーおよび／または前記マスターキーの記憶のために、一度だけプログラム可能なメモリ、不揮発性メモリ、もしくは（複数の）ヒューズを含む、請求項１３記載の不揮発性メモリシステム。
【請求項１７】
前記不揮発性メモリは不揮発性半導体メモリもしくはハードディスクドライブを含む、請求項１３記載の不揮発性メモリシステム。
【請求項１８】
前記不揮発性半導体メモリは一つ以上の集積回路である、請求項１７記載の不揮発性メモリシステム。
【請求項１９】
前記制御装置は、通信リンクを通して前記不揮発性メモリに接続し、前記不揮発性メモリと同じユニット内にパッケージ化される、請求項１３記載の不揮発性メモリシステム。
【請求項２０】
前記制御装置は、前記デバイスに固有で、かつ一度だけ作成されるマスターキーを作成するための乱数発生器をさらに含む、請求項１９記載の不揮発性メモリシステム。
【請求項２１】
前記乱数発生器は、前記不揮発性メモリを行き来する情報の暗号化と復号のために、前記エンジンによって選択的に利用される第二キーを作成するために使用される、請求項１９記載の不揮発性メモリシステム。
【請求項２２】
前記エンジンは、暗号文データキーを作成し、前記不揮発性メモリの指定エリア内に記憶するために、前記第二キーを暗号化するように構成される、請求項２１記載の不揮発性メモリシステム。
【請求項２３】
前記指定エリアは、前記デバイスのユーザーが記憶させようとする情報以外の情報を記憶するために使用される、請求項２２記載の不揮発性メモリシステム。
【請求項２４】
平文を受け取るステップと、
暗号文を作成するために、第一キーで前記平文を暗号化するステップと、
前記暗号文が作成される場所の外部に位置する不揮発性メモリ内に、前記暗号文を記憶するステップと、
前記記憶された暗号文を検索するステップと、
前記第一キーを用いて前記検索された暗号文を復号するステップと、
を含む、不揮発性メモリに情報を記憶し、不揮発性メモリから情報にアクセスする方法。
【請求項２５】
前記不揮発性メモリ内の所定エリアに、第二キーの暗号化版を記憶するステップと、
前記暗号化された第二キーを検索するステップと、

前記第二キーを復号するために前記第一キーを使用するステップと、
前記第二キーを用いて、前記不揮発性メモリの前記所定エリア以外のエリアから情報を検索するステップと、
をさらに含む、請求項２４記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は概して不揮発性メモリシステムに関連し、特に、外部不揮発性記憶デバイスに情報を安全に記憶し、外部不揮発性記憶デバイスから情報に安全にアクセスするための制御装置を持つ不揮発性メモリシステムに関連する。
【背景技術】
【０００２】
近年、不揮発性メモリは、電力供給されていない時でも記憶情報を保持するといった多数の特徴を持つため、好ましい記憶媒体として際立った評判を得ている。他方で、またその結果と言ってもよいが、認証されていないアクセス元からは発見できないように安全な方法で情報を記憶することが、インターネットに支配された世界や電子商取引では極めて重要になっており、機密情報の電子記憶装置にとっては重大な必要条件となっている。
【０００３】
例えば、情報の電子アクセスを許可するパスワード、ユーザーID、および電子証明書は、財務データやその他の極秘情報へのアクセスを許可することを主な理由として、機密情報となっている。そのため、不揮発性メモリへの情報の記憶と、不揮発性メモリからの情報の検索は、特に安全に行われる場合には好ましい。これは1メガバイトを超えるような大きなサイズの不揮発性メモリについてはなおさら顕著なことである。
【０００４】
一部の用途では、スマートカードやTrusted Platform Module（TPM）などのデバイスは、特殊な型の不揮発性メモリである、組み込みフラッシュや電気的にプログラム可能なリードオンリーメモリ（EPROM）を含む。こうした用途やその他の用途では大きな不揮発性メモリを利用することが好ましい。不揮発性メモリは機密事項を記憶するために利用されることが多い。しかしながら現在、不揮発性メモリやフラッシュデバイスへ記憶されるために電子集積回路やデバイスから出る情報は、厳重警備下にないため、侵入に対する脆弱性を有する。
【０００５】
現在、不揮発性メモリに記憶される情報のアクセスとプログラミングのために暗号化／復号技術を利用するシステムが存在するが、こうしたシステムは制御装置もしくは集積回路の内部に不揮発性メモリを包含するため、大量の情報の記憶や、大容量の情報の記憶にはあまり適していない。
【０００６】
加えて、不揮発性メモリの製造コストは、集積化が原因で、標準的なCMOS論理技術でデバイスやチップを製造するよりも著しく高いので、集積回路、デバイス、もしくはチップの内部に大きな不揮発性メモリを包含することは非常にコストがかかる。一例として、制御装置やデバイスを含む同じ集積回路内に大きなフラッシュメモリを包含すると、25～30％コストを増加することが知られている。数バイト程度などの比較的小さなサイズの不揮発性メモリは、CMOS論理技術を用いて包含することができる。CMOS論理技術で実装された不揮発性メモリセルは、電気的に消去可能でプログラム可能なROM（EEPROM）技術で実装された同等のセルよりも著しく大きい。しかしながら、CMOSでのデバイスやチップの製造コストは、EEPROMでの製造コストよりも著しく低い。より大きなCMOS不揮発性メモリセルが不揮発性メモリのために必要であるため、CMOS論理技術を用いて製造される小さな不揮発性メモリを持つデバイスやチップのコスト増加はわずかである。これはデバイスやチップを少々大きくすることになるが、EEPROM技術を用いてデバイスやチップを実装しなければならない場合よりも、コストが著しく低くなる。サイズの増加が極めてわずかである場

合は、ダイのサイズが大きくなっても許容できるが、大容量のメモリが必要となる際には、ダイのサイズの増加は全く実用的ではなく、EEPROM技術を利用する必要がある。

【０００７】

不揮発性メモリが、制御装置の外部、すなわち異なるダイ、集積回路やチップ、もしくは異なるパッケージ上に位置する用途においては、外部不揮発性メモリに情報を記憶し、外部不揮発性メモリから情報を検索する安全なシステムは事実上存在しない。

【発明の概要】

【０００８】

上記を踏まえて、制御装置の外部にある安全な情報記憶媒体を達成するための制御装置を含む不揮発性記憶システムが必要となっている。

【図面の簡単な説明】

【０００９】

【図１（ａ）】本発明の一実施形態に従う不揮発性メモリシステムを示す。

【図１（ｂ）】図１（ａ）のシステムの制御装置の詳細をさらに示す。

【図１（ｃ）】図１（ａ）の制御装置の試験／製造の実施形態例を示す。

【図１（ｄ）】本発明の別の実施形態に従う不揮発性システム79の実施形態例を示す。

【図１（ｅ）】図１（ａ）の不揮発性システムなどの、前述の不揮発性メモリシステムのいずれかの応用例を示す。

【図２】不揮発性メモリに記憶された情報を検索する際に図１（ａ）のシステムによって利用されるステップ例を示す。

【図３】本発明の別の実施形態に従う不揮発性メモリシステムを示す。

【図４】情報が不揮発性メモリに記憶される際に一実施形態で処理されるステップ例のフローチャートを示す。

【図５】情報が不揮発性メモリから検索される際に一実施形態で処理されるステップ例のフローチャートを示す。

【発明を実施するための形態】

【００１０】

ここで図１（ａ）を参照すると、本発明の一実施形態に従う不揮発性メモリシステム10が、インターフェース（もしくは通信リンク）16を通して不揮発性メモリ14に接続する制御装置12を含むように示される。リンク16は、フラッシュインターフェース、SPI、I2C、NORおよびNANDフラッシュバス、業界標準規格に準拠するように定められたバスなど、業界で周知の様々な形式をとることができる。本明細書で使用される“不揮発性メモリ”とは、電力供給されていない時に情報を保持することができるメモリをあらわす。本明細書で使用される“不揮発性半導体メモリ”とは、電力供給されていない時に情報を保持することができる、基板上に作られた半導体メモリをあらわす。半導体は基板上に作られ、不揮発性半導体メモリは一つ以上のダイ、チップ、もしくは集積回路内に作ることができる。

【００１１】

制御装置12は、ホストインターフェース18、制御論理20、エンコーダ／デコーダエンジン22、エンコーダ／デコーダキー記憶デバイス24、およびフラッシュインターフェース26を含むように示される。本明細書で使用される“キー”とは、情報の暗号化および／または復号の目的で開発される電子価値をあらわす。

【００１２】

ホストインターフェース18は、ホストリンク17を通してホスト（不図示）から情報を受け取るために接続して示される。ホストリンク17は、一例ではユニバーサルシリアルバス（USB）接続であり、他の実施形態ではその他の既知の接続形式であってもよい。ホストとなるデバイスの例としては、コンピュータの中央処理装置（CPU）、デジタルカメラの処理装置、携帯電話などの移動体通信デバイス、および不揮発性メモリと情報をやり取りする多くのその他のものがある。ホストインターフェース18はさらに、ホストから受け取った情報を提供するために制御論理20に接続して示される。

【００１３】
加えて、ホストインターフェース18はホストから受け取った情報を提供するためにエンジン22に接続して示される。制御論理20は、不揮発性メモリシステムに固有のキーであるマスターキーを記憶デバイス24から検索し、情報の暗号化および／または復号で使用するためにエンジン22へマスターキーをロードする。これについては間もなくさらに明らかにする。
【００１４】
制御論理20はさらに、マスターキーを保持するために記憶デバイス24に接続して示される。記憶デバイス24は、本発明の一実施形態では不揮発性メモリである。別の実施形態では、マスターキーはハードワイヤード（hard-wired）であるか、恒久的にプログラムされているか、もしくはリードオンリーメモリ（ROM）内にある。マスターキーのハードワイヤリングの方法例としては、電気的にプログラム可能なヒューズ、アンチヒューズ、レーザーブロー（laser blown）、および不揮発性メモリセルの使用を含むが、これらに限定はされない。あるいはマスターキーは、ファームウェアもしくはソフトウェアのコードによって、制御装置のROM内にプログラムされるか、もしくは記憶されてもよい。マスターキーは制御論理20内に随意に記憶されてもよく、この場合、記憶デバイス24は不要である。別の実施形態では、マスターキーはエンジン22内に記憶される。マスターキーの作成とプログラミングは、制御装置12もしくはシステム10の製造時に行われる。
【００１５】
記憶デバイス24が不揮発性メモリである場合は、CMOSプロセスを使用するため、制御装置12のサイズはやや大きくなるが、サイズの増加はわずかである。これは記憶デバイス24のサイズが数バイト程度であり、サイズの増加がわずかである、もしくは無視できるためである。しかしながら、不揮発性メモリ14のサイズは重要であり、不揮発性メモリ14が制御装置12内に位置する場合は、制御装置12に関連するサイズとコストを著しく増加する。しかしながら、本発明の実施形態に従って、大きなサイズの不揮発性メモリ14に関連する負荷は、不揮発性メモリ14を制御装置12の外部に位置するようにすることで除去され、その結果制御装置12の製造のためのCMOSプロセスの実用化が可能となる。
【００１６】
ホストリンク17の例としては、業界標準規格のUSB、マルチメディアカード（MMC）、セキュアデータ（SD）、コンパクトフラッシュ（CF）、メモリースティック（MS）、IDE、シリアルATA（SATA）、PCI Express（PCIe）、SCSI、IS07816、およびlow pin count（LPC）を含むが、これらに限定はされない。
【００１７】
情報の暗号化および／または復号に使用されるエンジン22は、暗号学的に強力でなければならない。すなわち、解読されていない暗号化アルゴリズムを使用しなければならない。次世代標準暗号化方式（Advanced Encryption Standard：AES）128/196/256など、現在強力であると知られているアルゴリズムが、エンジン22によってプログラム可能なように実行される。本発明の実施形態から逸脱することなく、いかなる暗号化／復号アルゴリズムが利用されてもよいことが理解されるべきである。一実施形態では、暗号化／復号アルゴリズムは解読不可能であることが知られているため、より安全である。
【００１８】
暗号化／復号アルゴリズムを異なるアルゴリズムに変える必要がある場合には、そうしたアルゴリズムの変更に適合するように、エンジン22を修正するかもしくは交換する必要がある。エンジン22は一般的に、不揮発性メモリに記憶される情報のリアルタイムの暗号化を実現するために、既知の解読不能なアルゴリズムを実装するようにハードウェアを用いて設計される。あるいは、エンジン22はアルゴリズムを実装するようにファームウェアやソフトウェアを用いてプログラムされる。しかしながら、エンジン22のファームウェアやソフトウェアによる実装は、暗号化／復号の速度を低下させることが理解される。従って、リアルタイムでの暗号化／復号を実現するために、エンジン22はハードウェアで設計され、既知の暗号化／復号アルゴリズムを実装する。

【００１９】
制御論理20は基本的に情報の流れを制御し、様々な形式をとってもよく、その内の一つは前述の通り中央処理装置（CPU）である。エンジン22はさらに記憶ユニット24とフラッシュインターフェース26に接続して示される。不揮発性メモリ14は、一つ以上の不揮発性メモリデバイスもしくは集積回路（もしくはチップ）に包含されてもよい。
【００２０】
一実施形態例では、間もなく論じるように、不揮発性メモリ14は一つ以上の集積回路の中にあってもよく、その回路は制御装置12と同じパッケージに含まれるか、もしくは物理的に外部に位置するパッケージに含まれる。
【００２１】
本発明の一実施形態では、システム10は、次の図面に関連してさらに論じるように、動作のためにホストに接続可能な、携帯用の取り外し可能な消費者デバイスである。システム10がホストに接続する際、システム10もしくは携帯用の取り外し可能な消費者デバイスのユーザーは、認証もしくは認可され、この時マスターキーがエンジン22に提供される。
【００２２】
前述の通り、システム10は、情報や電子データ、もしくは他の種類の電子情報を安全な方法で記憶するために、不揮発性メモリ14などの大きなサイズの適切な不揮発性メモリを必要とする。大きなサイズ、とは、不揮発性メモリ以外のものがその上に製造されているダイの内部には、包含させることが経済的にも実用的にも不可能であるような不揮発性メモリをあらわすことを意図する。記憶される情報は、標準規格の接続を通してデバイスに接続するホスト、あるいは、デバイスもしくは制御装置の内部に含まれるファームウェアのいずれかによって提供される。そのようなデバイスの多くの応用例が予想され、その内の一つを図１（ｅ）に関連して示し、論じる。
【００２３】
本明細書の記載と図面のほとんどは、暗号文、もしくは暗号化された情報として、本発明の実施形態に従う（図１（ａ）の）不揮発性メモリ14もしくは他の不揮発性メモリに記憶される情報について論じるが、暗号化されていない情報、もしくは平文もまた、不揮発性メモリ内に記憶されてもよいことが理解される。後者の場合、記憶された平文の復号は全く必要ないことが明らかである。本明細書で使用される“暗号文”（cipher text：CT）とは、暗号化版の情報をあらわす。本明細書で使用される“平文”（plain text：PT）とは、いかなる種類の暗号化も行っていない、生の形式の情報をあらわす。“平文データキー”とは、暗号化されていない、もしくは復号されたデータキーである。“暗号文データキー”とは暗号化されたデータキーである。
【００２４】
動作中、ホストはホストリンク17を通して、不揮発性メモリ14に記憶される情報をホストインターフェース18に提供する。そしてホストインターフェース18は、ホスト提供情報を制御論理20とエンジン22に接続する。制御論理20の制御の下、エンジン22は記憶デバイス24からマスターキーを受け取り、それを用いてホスト提供情報を暗号化し、その暗号化情報をフラッシュインターフェース26を通して不揮発性メモリ14に渡す。
【００２５】
不揮発性メモリ14から情報が読み出される時、情報はフラッシュインターフェース26を通してエンジン22に転送され、エンジン22はマスターキーを用いて、不揮発性メモリ14から転送された情報を復号する。本発明の一実施形態では、記憶デバイス24がマスターキーをエンジン22に提供する。エンジン22によるマスターキーの使用は、制御論理20の指示の下に行われる。復号情報はその後エンジン22によってホストインターフェース18に提供され、そしてホストインターフェース18はその復号情報をホストに提供する。
【００２６】
一実施形態では、マスターキーはランダムであり、エンジン22は安全性を確保するために比較的強力な暗号化／復号アルゴリズムを使用する。実際には、制御装置12の製造中に乱数発生器がマスターキーを作成する。これについては次の図面に関連して論じる。マス

ターキーのランダム性および／または暗号化／復号コードの強度が低いほど、不揮発性メモリ14に記憶された、もしくは記憶される情報の安全性は低くなり、脆弱性を増すことになることが理解される。

【００２７】

このように、各システムが異なるマスターキーを用いてプログラムされ、マスターキーは他者にわからないままであるという点で、制御装置12（もしくはシステム10）は独自の特徴を持つ。実際には、マスターキーが何らかの方法で消去（purge）、削除（delete）、もしくは破棄（destroy）される場合、不揮発性メモリに記憶された情報は復号できないので無用となる。間もなく論じるように、データキーなどの第二キーを使用する場合には、データキーが削除されるかもしくはわからなくなる場合、不揮発性メモリに記憶された情報は無用となるが、システムは次の情報を記憶するために再利用され得る。しかしながら、失われたデータキーを用いて記憶された以前の全記憶情報は永遠に失われる。これは、システム、もしくはシステムで動作する不揮発性メモリが失われる場合に、記憶情報への不正アクセスを防ぐ上で非常に有用である。

【００２８】

マスターキーが不正な手段によって回復される場合、各システムは固有のマスターキーを持つため、システム10などの他のシステム（もしくは制御装置12）のインテグリティは損なわれない。様々なマスターキーが製造中に試験装置によって作成され、作成された各マスターキーは異なるシステム10（もしくは制御装置12）にプログラムされる。従って、マスターキーは全ての人に（システム10の設計者にすら）わからないままである。マスターキーのプログラマビリティのために、他のデバイスの中でもとりわけ、一度だけプログラム可能なメモリ、不揮発性メモリ、もしくはヒューズが記憶デバイス24で利用され得る。これは、マスターキーは一度だけプログラムされる必要があり、その後はシステム10（もしくは制御装置12）によってのみ使用されるからである。マスターキーはシステム10（もしくは制御装置12）の寿命を通して使用される。

【００２９】

乱数発生器（不図示）は、システム10（もしくは制御装置12）の製造中、リアルタイムもしくはオンザフライで乱数を作成し、その乱数はマスターキーとなってシステム10（もしくは制御装置12）にプログラムされる。従って、製造完了時にマスターキーは記憶デバイス24に記憶され、その記憶デバイス24は、不揮発性メモリ、ヒューズ、一度だけプログラム可能なメモリ、もしくは電力が加えられていない時に情報を保持できる任意の他の種類のメモリであることが好ましい。マスターキーは、いかなる方法でも決して変更もしくは改変されることがない。

【００３０】

追加の随意的な安全手段として、製造中にマスターキーを読まれないように守るため、記憶デバイス24のトランジスタを隠すキャップとして機能する層が、マスターキーがプログラムされる層の上に挿入される。このように、システム10（もしくは制御装置12）を分解することによってマスターキーを明らかにしようとするには、かなりの精巧さが必要となり、それ程の精巧さがなければ明らかにすることができず、さらに特殊な装置と高いコストを必要とする。いくつかの実施形態はプログラミング手段の難読化を必要としないことが理解される。つまり、いくつかの実施形態では、マスターキーがシステムにプログラムされる方法は物理的に読み取り不可能であり、マスターキーの不正認証を防ぐための特別な製造ステップを必要としない。

【００３１】

本発明の一実施形態では、不揮発性メモリ14は、システムのユーザーが記憶させようとする情報以外の情報である、（複数の）証明書やパスワードなどの個人情報もしくは機密情報の記憶のために、（複数の）プライベートエリアと呼ばれる所定の（複数の）記憶場所を含む。プライベートエリアは、システム10のユーザーが記憶させようとするデータ以外のデータを保存するための、不揮発性メモリ内の所定場所である。つまり、証明書、パスワードなどは、ユーザーが記憶させようとする情報以外の情報であるが、システムが正

常に機能するために記憶に必要なものである。

【００３２】

本発明のさらに別の実施形態では、情報にアクセスするためにデータキーもしくは第二キーが使用され、情報のさらなる安全性を提供する。マスターキーは、プライベートエリアの中、およびプライベートエリアの範囲内に記憶された情報のみにアクセスするために使用され、データキーは暗号化された形式で記憶され、不揮発性メモリ内の残りの情報にアクセスするために検索される。

【００３３】

情報を検索するために二つのキーを使用する実施形態の動作方法をさらに明らかにするため、マスターキーとデータキーを用いて情報にアクセスするためにシステム10によって処理されるステップ例のフローチャートを図２に示す。一つ以上のデータキーがあってもよく、各データキーは不揮発性メモリの特定場所にアクセスするためのものである。（複数の）データキーは、暗号化された形式で記憶デバイス24もしくは不揮発性メモリ14に記憶される。あるいはデータキーは、エンジン22、例えばレジスタファイル、もしくは制御装置12内の任意の他の場所に記憶される。

【００３４】

図１（ｂ）は図１（ａ）の制御装置12の詳細をさらに示す。図１（ｂ）では、エンジン22はマルチプレクサ（mux）25を通して乱数発生器23に接続して示され、mux 25は、マスターキーもしくはデータキーをエンジン22に接続するリンク27を受ける。mux 25は、エンジン22の入力が、リンク27を通してキーを、もしくはデータリンク29を通して他の情報を、選択的に受け取ることを可能にする。キーがエンジン22内に記憶される場合は、mux 25は同様にエンジン22内に位置することが理解される。

【００３５】

図１（ｂ）にさらに示されるように、図１（ａ）の制御論理20は、マスターキー、データキー、もしくは他の種類のキーを選択的に受け取るmux 31へ、選択信号を提供するために接続して示される。動作中、データキーもしくは第二キーが作成される場合、制御論理20は、選択信号33を通して、mux 31にその入力としてマスターキーを選択するように信号を送り、エンジン22は、乱数発生器によって作成された乱数をリンク27を通して受け取る。エンジン22はマスターキーを用いて、受け取った乱数を暗号化し、暗号化（もしくは暗号文）データキーを作成する。この時点から、ユーザーが不揮発性メモリに記憶させようとするデータを暗号化し、復号するために、データキーがシステム10によって利用される。プライベートエリアが指定される実施形態例では、データキーは暗号化されプライベートエリアに記憶され、マスターキーを用いてアクセスされる。

【００３６】

一実施形態例では、製造中に、乱数発生器23が、マスターキーの作成においてエンジン22に使用される乱数を作成する。このように、マスターキーは制御装置12から決して出ることがなく、完全に制御装置内で作成されるため、安全性を強化する。一般的に、試験ツールや刺激デバイスを使用するために、データや情報がチップ、ダイ、もしくはパッケージから出る時には、安全性は少なくともある程度危険に晒される。情報が決してチップから出ない時とは対照的に、情報がチップから出た後に妨害するのは実に簡単である。

【００３７】

図１（ｃ）は、図１（ｂ）に関連する前述の記載のものとは異なる、図１（ａ）の制御装置12を試験／製造するための制御装置試験装置77を示す。図１（ｃ）では、試験装置41は、マスターキーを制御装置にプログラムすることによって、制御装置12を試験するか、もしくは製造を補助するように示される。試験装置41は制御装置12の外部にあり、物理的に外側に位置するため、マスターキーはより妨害を受けやすい。従って、図１（ｃ）の実施形態の安全性は、マスターキーの作成とプログラミングに関しては図１（ｂ）の実施形態の安全性よりも低いため、安全な試験／製造環境が必要となる。図１（ｃ）では、試験装置41内に位置する乱数発生器43が、マスターキーとして機能する乱数を作成し、試験装置ケーブル45を通して制御装置のエンジン22に転送する。受け取られたマスターキーは、

その後上述の方法で制御装置に記憶される。実施形態１（ｂ）および１（ｃ）の両方において、マスターキーは各制御装置12に対して一度だけ作成されることに留意すべきである。これもやはり、図１（ａ）のシステム10など、その中で制御装置12が使用されるシステムの安全レベルをさらに強化するためである。

【００３８】

図１（ｄ）は、制御装置81と、通信リンク91を通して接続する不揮発性メモリ85とを含む、不揮発性システム79の実施形態例を示し、制御装置81とメモリ85は物理的に別々のユニットにパッケージ化される。例えば、制御装置81は、不揮発性メモリ85を含まないパッケージ83に位置するように示される。通信リンク91は、制御装置81と不揮発性メモリ85を物理的に接続する。不揮発性メモリ85は、不揮発性半導体メモリである場合、一つ以上の集積回路もしくはダイを含むように示される。図１（ｄ）のシステム79は、図１（ａ）のシステム10および図３のシステム40よりも比較的安全性が低い。これは、関連キーの知識がないために、情報の解読は前述のシステムと同程度に困難ではあるが、暗号化情報が制御装置パッケージ83の外側を移動しなければならず、妨害しやすいためである。

【００３９】

図１（ｅ）は、システム10などの前述の不揮発性メモリシステムのいずれかの応用例を示す。図１（ｅ）では、ノートブックコンピュータ101が携帯用の取り外し可能な消費者デバイス105を受けるように示され、そのポート103にはデバイス105のコネクタ107が取り外し可能なように接続する。デバイス105は不揮発性メモリ111に接続する制御装置109を含むように示される。

【００４０】

制御装置109は、デバイス105がそのコネクタ107を通してコンピュータ101に接続する時、コンピュータ101のホストと通信する。制御装置109は、本明細書で上述の通り、ホストと不揮発性メモリとの間で情報をやり取りする。例えば、コンピュータ101のユーザーは、ファイルなどの情報をデバイス105に保存したいかもしれない。情報はポート103とコネクタ107を通して制御装置109に転送され、ここで情報は、前述の方法でキーを用いて暗号化される。暗号化情報（もしくは暗号文）は不揮発性メモリ111に記憶される。同様に、コンピュータ101のユーザーがデバイス105に以前に記憶した情報を読み出したい時は、記憶された暗号化情報は制御装置によって不揮発性メモリ111から読み出され、平文に復号され、コネクタ107とポート103を通してコンピュータ101に提供される。

【００４１】

一例では、デバイス105は図１（ａ）のシステム10である。あるいは、デバイス105は、図１（ｄ）に関連して論じたように、別々にパッケージ化される不揮発性メモリを含まない。一実施形態例では、ポート103とコネクタ107はUSB規格に準拠するが、他の種類の通信方法が本発明の様々な実施形態で利用されてもよい。

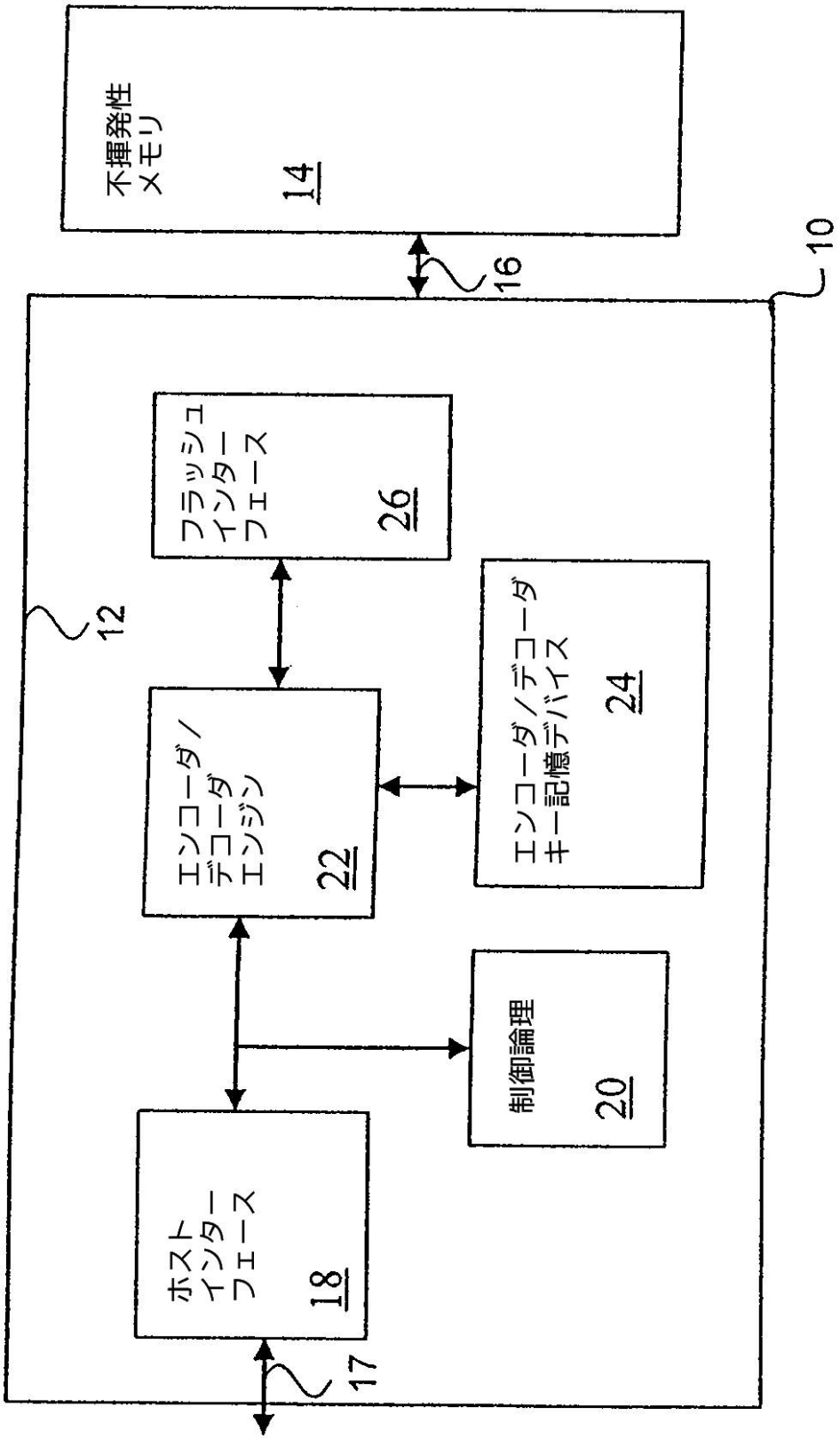
【００４２】

図２は、不揮発性メモリ14に記憶された情報を検索する際に図１（ａ）のシステム10によって利用されるステップ例を示す。図２ではステップ30において、暗号化データキーもしくは暗号文データキーが不揮発性メモリ14から読み出される。暗号化データキーは不揮発性メモリのプライベートエリアに記憶されることが好ましく、プライベートエリアは、マスターキー、もしくはマスターキーを用いて作成されるさらなる第三キーのいずれかを用いてアクセスされる。次にステップ32では、検索された暗号文データキーが、記憶デバイス24に記憶されたマスターキーを用いてエンジン22によって復号される。次にステップ34では、検索された復号データキーもしくは平文データキーがエンジン22にロードされ、不揮発性メモリ14のプライベートエリア以外のあらゆる場所から検索された任意のデータもしくは情報を復号するために使用される。マスターキーとデータキーを使用する前述の例のように、二つのキーが利用される場合は、ステップ34で一旦データキーが検索されると、パスワードもしくは証明書などの他の機密情報が不揮発性メモリ14からアクセスされるか、もしくは不揮発性メモリ14に記憶されない限り、マスターキーはもはや使用する必要がない。

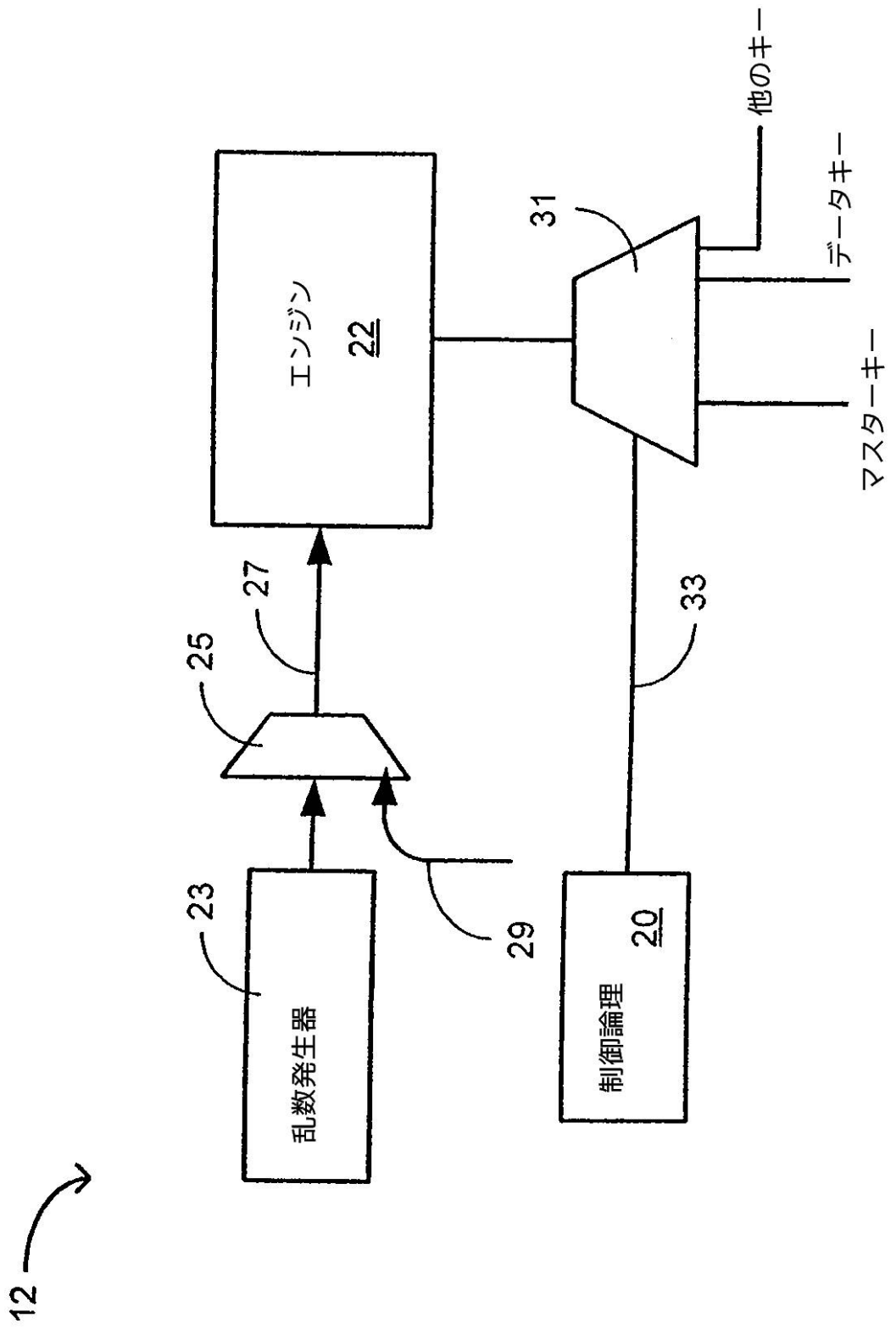
【００４３】
本発明の別の実施形態では、一つよりも多くのプライベートエリアが不揮発性メモリ14内で指定されてもよく、さらに、各プライベートエリアは異なるデータキーを使用することによってアクセスされてもよいことに留意すべきである。キーが安全に記憶され得る限り、利用されるデータキーの数に制限はない。
【００４４】
図３は本発明の別の実施形態に従う不揮発性メモリシステム40を示す。図１（ａ）の不揮発性メモリ14が、図１（ａ）のエンジン22とフラッシュインターフェース26とを含む制御装置42に接続して示されるが、エンジンはマスターキーとデータキーを受け取るように示される。制御装置42は、一時記憶のためにレジスタ44に接続する平文を受け取るように示される。レジスタ44はエンジン22に接続して示され、エンジン22は図１（ａ）と同様の方法でフラッシュインターフェース26に接続して示される。図３の実施形態と図１（ａ）の実施形態の違いは、平文もしくは暗号文のいずれかがフラッシュインターフェース26に選択的に提供され得ることである。PTがCTに変換される場合は、随意に二つのキー（マスターキーとデータキー）を用いてそれを暗号化するために、レジスタ44からエンジン22に転送される。つまり、前述の通り、PTがパスワード、証明書、キーなどを含む機密情報である場合は、それを暗号化するためにマスターキーが使用され、そうでなければ、PTがデータ、もしくは時にユーザーデータと呼ばれるもの、パスワードや証明書やキーなど以外のデータである場合は、データキーを用いて暗号化される。
【００４５】
図３に示すように、エンジン22はバイパスされてもよいが、不揮発性メモリ14に記憶される、もしくは不揮発性メモリ14から検索される情報に提供される安全性は、わずかなものとなるだろう。
【００４６】
不揮発性メモリ14は、大きな記憶容量、すなわち1メガバイトより大きな記憶容量を持ってもよい。大容量の情報を記憶するための不揮発性メモリを制御装置の外部に位置付けることで、フラッシュや他の種類の不揮発性メモリの製造で使用されるプロセスよりも安価な、CMOS技術を使用する制御装置の製造が可能になる。
【００４７】
図４は、図３の不揮発性メモリ14に情報が記憶される際に処理される一実施形態のステップ例のフローチャートを示す。まず、PTが制御装置によって受け取られ、キーがエンジン22にロードされる。次に、PTのCT版を作成するために、PTはロードされたキーで暗号化され、不揮発性メモリに保存もしくは記憶される。使用されるキーの種類は、プライベートエリアが不揮発性メモリ内で指定されているかどうか、およびCTの記憶先がプライベートエリアであるかどうかによって決まる。後者の場合、マスターキーがキーとして使用される。二つのキーが利用され、プライベートエリア以外のエリアがアクセスされる場合には、データキーが使用される。プライベートエリアが指定されていない場合は、明らかにマスターキーが使用される。
【００４８】
図５は、図３の不揮発性メモリ14から情報が検索される際に別の実施形態で処理されるステップ例のフローチャートを示す。まず、CTが制御装置によって受け取られ、キーがエンジン22にロードされる。次に、CTを復号するためにロードされたキーが使用され、その結果PTを検索する。暗号化と復号の際には、同じ場所を行き来する情報に対して同じキーが使用されることに留意されたい。そうでなければ、復号は正確なPTをもたらさないだろう。どのキーが図５で使用されるかについては、図４に関連して論じたものと同じ状況が図５に当てはまる。
【００４９】
本発明は特定の実施形態に関して説明されているが、当業者にはその変更および変形が本開示により明らかとなるだろうということが予想される。したがって以降の請求項は、本発明の趣旨と範囲内に含まれる、そうした変形および変更の全てを包含するものと解釈

されることが意図される。

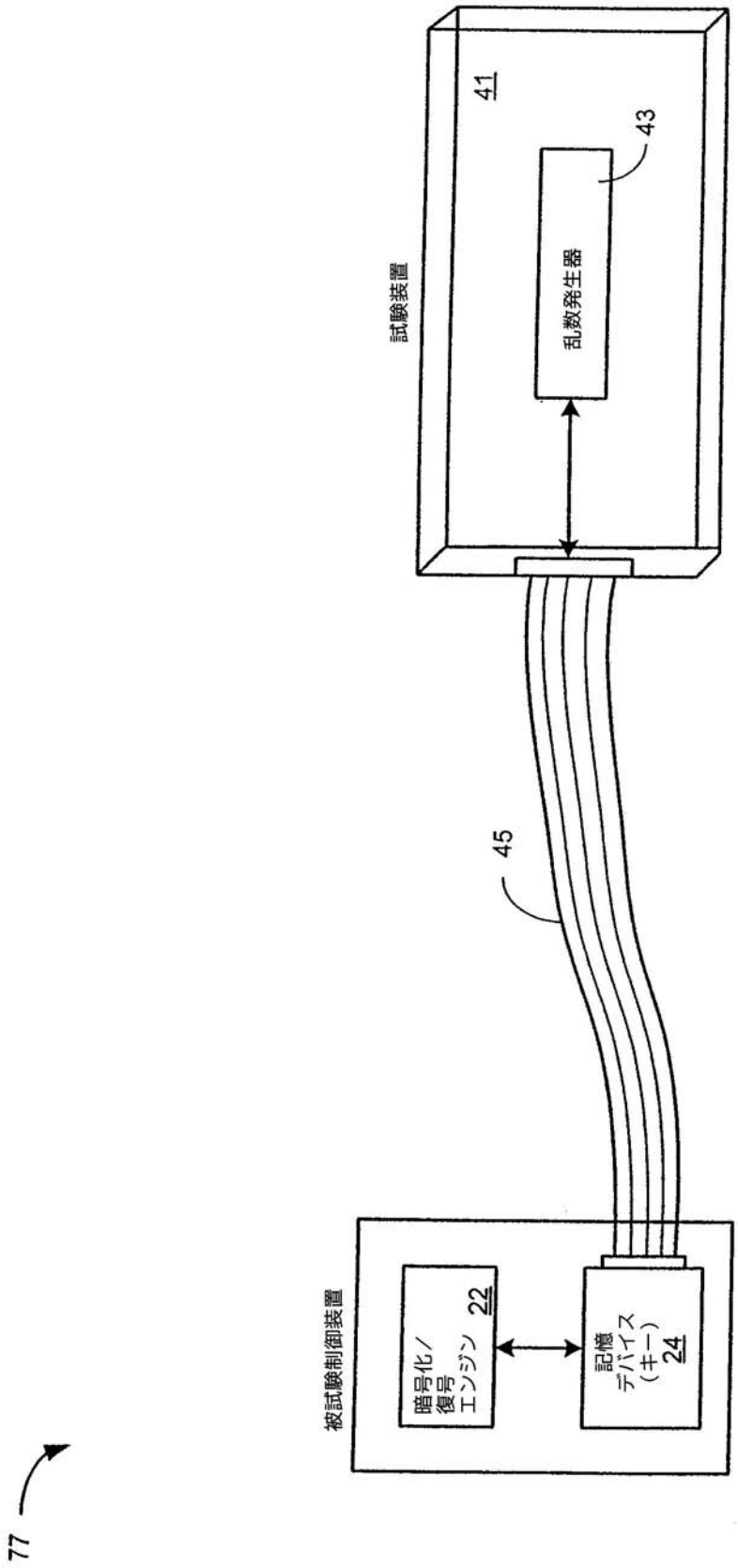
【図１（ａ）】


不揮発性
メモリ
14
16
10
12
フラッシュ
インター
フェース
26
エンコーダ／
デコーダ
エンジン
22
エンコーダ／デコーダ
キー記憶デバイス
24
制御論理
20
ホスト
インター
フェース
18
17

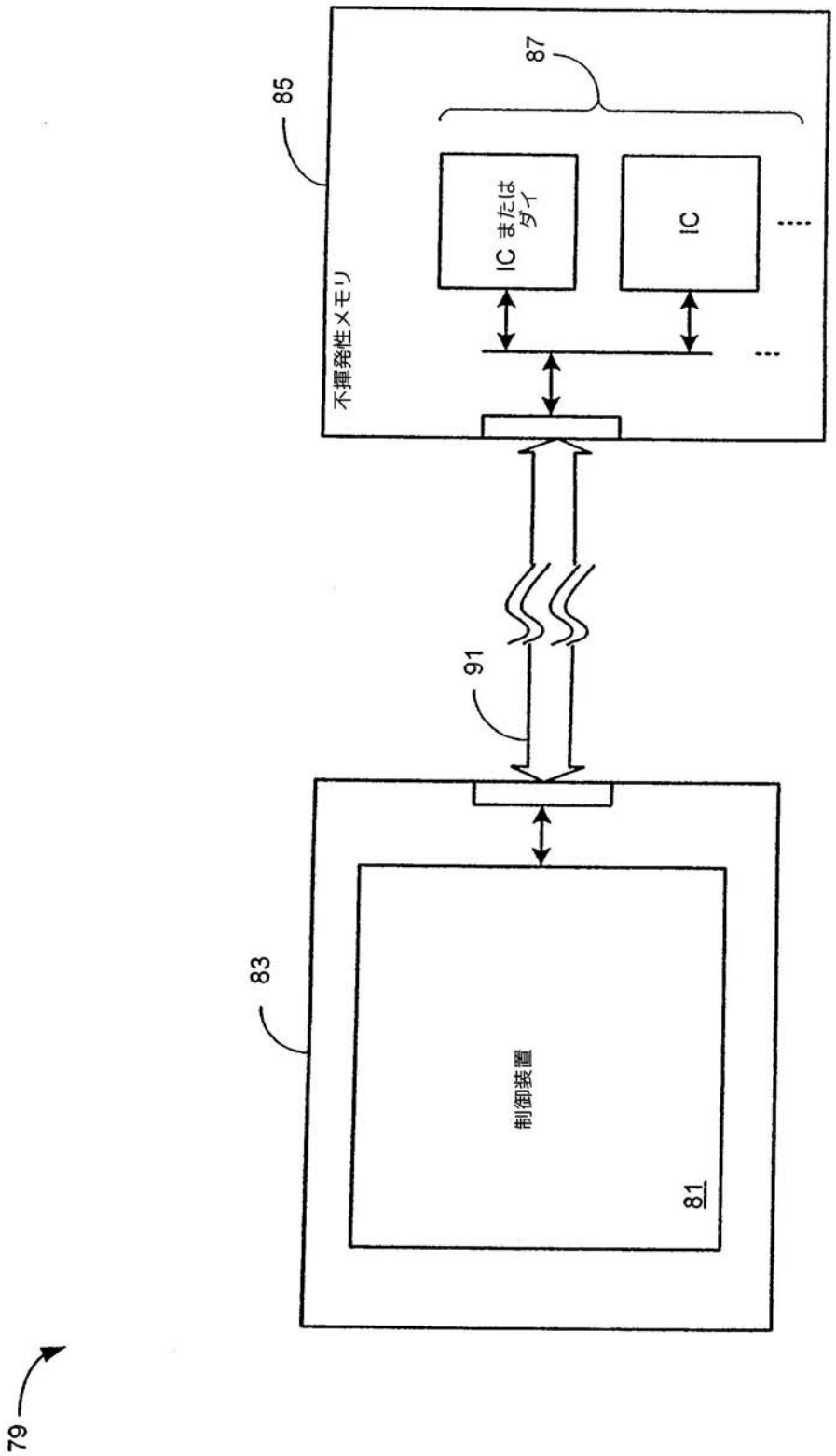
【図１（ｂ）】



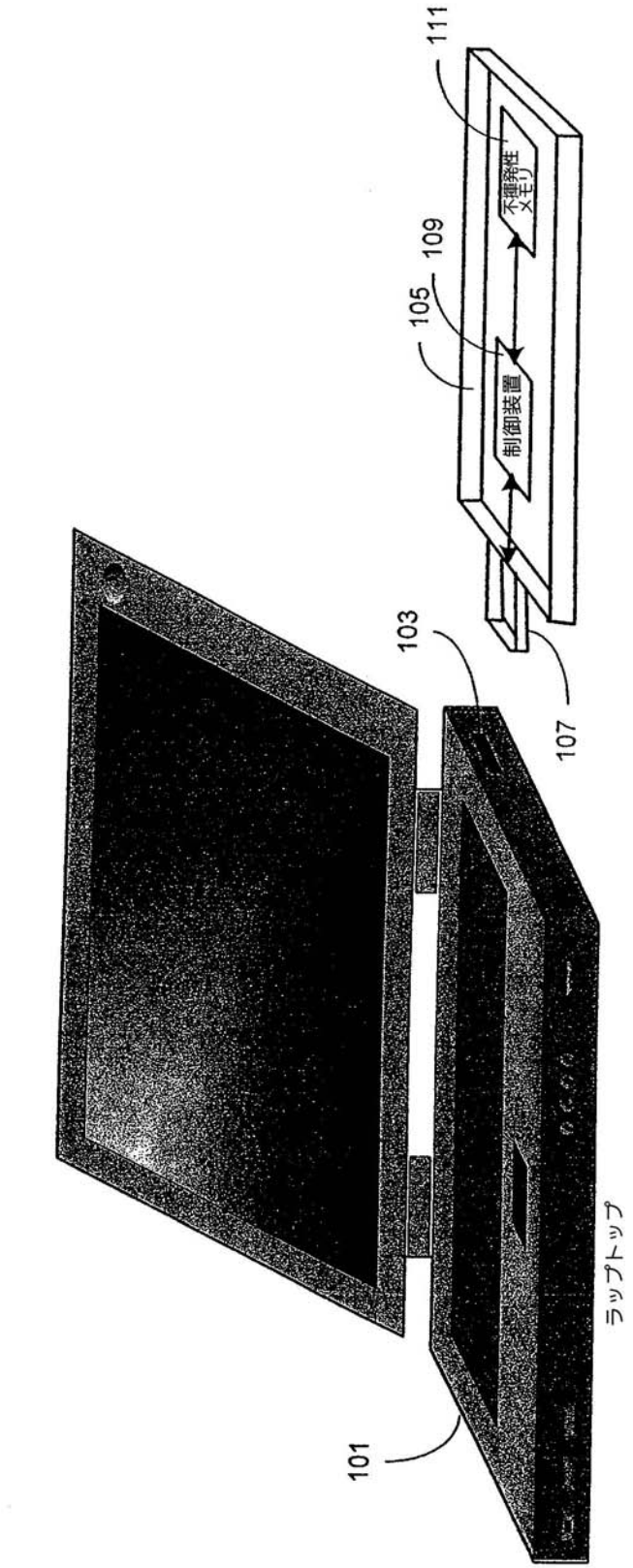
【図１（ｃ）】



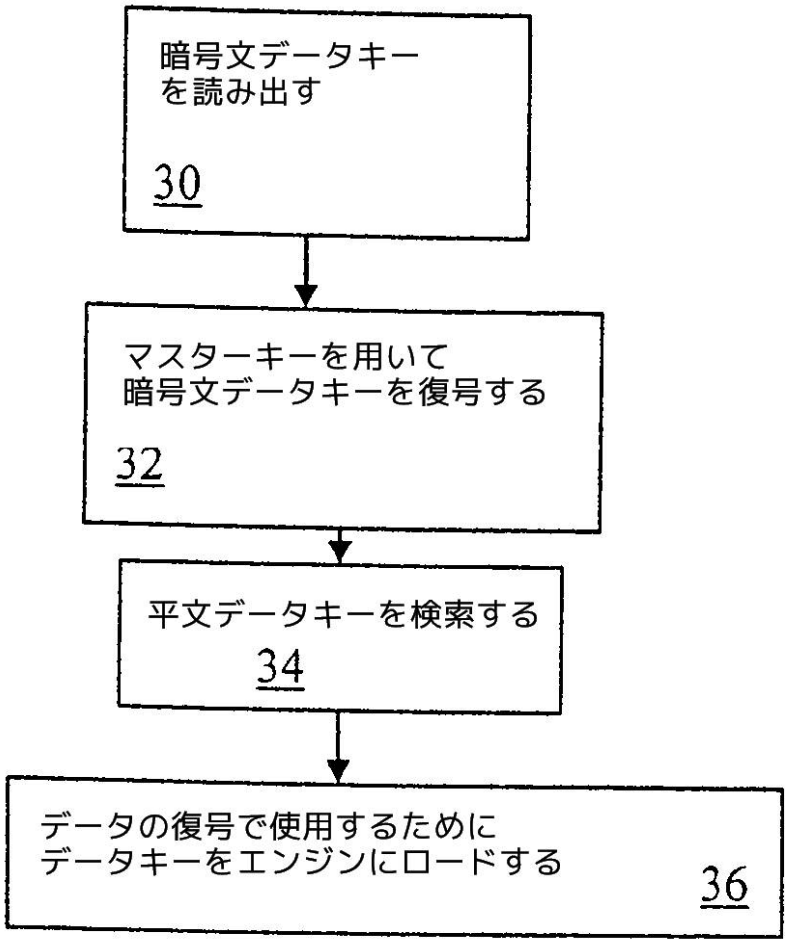
【図１（ｄ）】



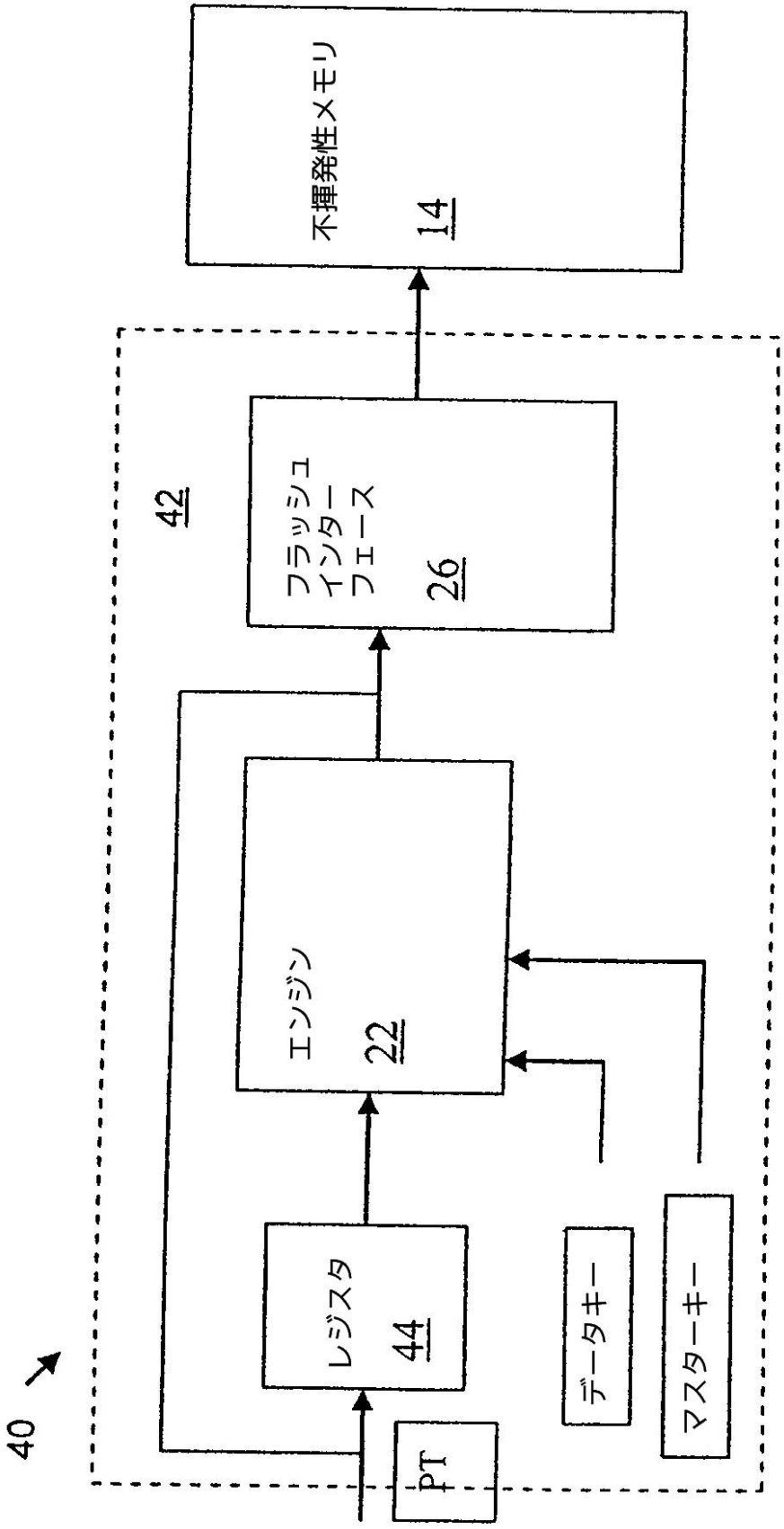
【図１（ｅ）】



【図２】


暗号文データキー
を読み出す
30
マスターキーを用いて
暗号文データキーを復号する
32
平文データキーを検索する
34
データの復号で使用するために
データキーをエンジンにロードする
36

【図３】



【図４】

PTを受け取る---キーをロードする---キーでPTを暗号化する---CTを記憶する

【図５】
CTを受け取る---キーをロードする---キーでCTを復号する---PTを記憶する
【手続補正書】
【提出日】平成21年6月23日(2009.6.23)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ホストと不揮発性メモリの間で情報をやり取りするための不揮発性記憶システムで利用される制御装置であり、
前記制御装置の外部に位置し、前記不揮発性メモリと情報をやり取りするための暗号化／復号エンジンを含み、前記エンジンは、前記不揮発性メモリに記憶される情報を記憶前に暗号化するためにマスターキーを使用し、前記不揮発性メモリからの検索後に暗号化情報を復号するために前記マスターキーを使用し、
前記エンジンによって、前記不揮発性メモリ内の所定場所に暗号化データキーが記憶され、前記暗号化データキーは前記マスターキーを用いて前記エンジンによって作成されており、前記記憶された暗号化データキーは、前記所定場所から検索され、前記マスターキーを用いて前記エンジンによって復号され、前記所定場所以外に位置する前記不揮発性メモリから検索された情報を復号するために使用される、
ことを特徴とする制御装置。
【請求項２】
前記マスターキーと前記データキーを前記エンジンに選択的に提供するように構成されたマルチプレクサをさらに含む、請求項１記載の制御装置。
【請求項３】
前記所定場所は、前記システムのユーザーが記憶させようとするデータ以外の情報を記憶するためのプライベートエリアである、請求項１記載の制御装置。
【請求項４】
一つよりも多くのプライベートエリアが指定される、請求項３記載の制御装置。
【請求項５】
前記プライベートエリアの各々は、それに固有の暗号化データキーを含む、請求項４記載の制御装置。
【請求項６】
前記暗号化データキーの非暗号化版であるデータキーを作成するための乱数発生器をさらに含む、請求項５記載の制御装置。
【請求項７】
前記暗号化データキーを作成するために前記エンジンによって受け取られるように構成された乱数を作成するための乱数発生器をさらに含む、請求項１記載の制御装置。
【請求項８】
前記データキーを記憶するためのエンコーダ／デコーダキー記憶デバイスをさらに含む、請求項７記載の制御装置。
【請求項９】
前記マスターキーを作成するための乱数発生器をさらに含む、請求項１記載の制御装置。
【請求項１０】
前記乱数発生器によって作成された固有の乱数を記憶するための不揮発性メモリをさらに含む、請求項９記載の制御装置。
【請求項１１】

前記乱数発生器は、前記制御装置の試験もしくは製造の補助のための試験装置の一部である、請求項９記載の制御装置。

【請求項１２】

前記マスターキーは、前記不揮発性記憶システムに固有であり、かつ一度だけ作成される、請求項９記載の制御装置。

【請求項１３】

前記マスターキーを記憶するためのエンコーダ／デコーダキー記憶デバイスをさらに含む、請求項１記載の制御装置。

【請求項１４】

前記制御装置は、前記データキーおよび／または前記マスターキーの記憶のために、一度だけプログラム可能なメモリ、不揮発性メモリ、もしくは（複数の）ヒューズを含む、請求項１記載の制御装置。

【請求項１５】

前記不揮発性メモリはフラッシュメモリもしくはハードディスクドライブである、請求項１記載の制御装置。

【請求項１６】

前記不揮発性メモリは不揮発性半導体メモリを含む、請求項１記載の制御装置。

【請求項１７】

前記不揮発性半導体メモリは一つ以上の集積回路である、請求項１６記載の制御装置。

【請求項１８】

前記暗号化／復号エンジンは、平文を受け取り、前記不揮発性記憶システムへ記憶するために、前記マスターキーを用いて前記受け取った平文の暗号文版を作成し、情報の検索時には、前記平文を再生するために前記マスターキーを用いて前記暗号文を復号するように構成される、請求項１記載の制御装置。

【請求項１９】

前記不揮発性記憶システムは、前記ホストに取り外し可能なように接続可能な、携帯用の取り外し可能な消費者デバイスの一部である、請求項１記載の制御装置。

【請求項２０】

平文を受け取るステップと、

暗号文を作成するために、第一キーで前記平文を暗号化するステップと、

前記暗号文が作成される場所の外部に位置する不揮発性メモリ内に、前記暗号文を記憶するステップと、

前記記憶された暗号文を検索するステップと、

前記第一キーを用いて前記検索された暗号文を復号するステップと、

前記不揮発性メモリ内の所定エリアに、第二キーの暗号化版を記憶するステップと、

前記暗号化された第二キーを検索するステップと、

前記第二キーを復号するために前記第一キーを使用するステップと、

前記第二キーを用いて、前記不揮発性メモリの前記所定エリア以外のエリアから情報を検索するステップと、

を含む、不揮発性メモリに情報を記憶し、不揮発性メモリから情報にアクセスする方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/083763

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/02

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)
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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 264 373 A (EUROLOGIC RESEARCH LIMITED [IE]) 25 August 1993 (1993-08-25) abstract; figure 1 page 3, line 1 - line 27 page 4, line 13 - page 6, line 4 page 7, line 27 - page 8, line 20	1-25
A	WO 2006/071725 A (SANDISK CORP [US]; DISCRETIX TECHNOLOGIES LTD [IL]; HOLTZMAN MICHAEL [) 6 July 2006 (2006-07-06) the whole document	1-25
A	US 2006/195704 A1 (COCHRAN ROBERT A [US] ET AL) 31 August 2006 (2006-08-31) abstract; figures 1B,3 paragraph [0005] - paragraph [0014] paragraph [0018] - paragraph [0024] paragraph [0049] - paragraph [0050]	1-25

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 November 2008	25/11/2008

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, Fax (+31-70) 340-3016	Powell, David

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/083763

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2264373 A	25-08-1993	NONE	
WO 2006071725 A	06-07-2006	EP 1828948 A2	05-09-2007
		JP 2008524969 T	10-07-2008
		KR 20070103741 A	24-10-2007
US 2006195704 A1	31-08-2006	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,PL,PT,RO,SE,SI,SK,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,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．コンパクトフラッシュ