(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5662037号
(P5662037)

(45)発行日　平成27年1月28日(2015.1.28)　(24)登録日　平成26年12月12日(2014.12.12)

(51)Int.Cl.　F I
G06F 12/16 (2006.01)　G06F 12/16 320A
G06F 12/00 (2006.01)　G06F 12/00 537H
G06F 12/00 542A

請求項の数 9　外国語出願　(全 18 頁)

(21)出願番号　特願2010-46014(P2010-46014)
(22)出願日　平成22年3月3日(2010.3.3)
(65)公開番号　特開2010-231778(P2010-231778A)
(43)公開日　平成22年10月14日(2010.10.14)
審査請求日　平成25年2月4日(2013.2.4)
(31)優先権主張番号　12/398,090
(32)優先日　平成21年3月4日(2009.3.4)
(33)優先権主張国　米国(US)

(73)特許権者　503260918
アップル　インコーポレイテッド
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　インフィニット　ループ　1
(74)代理人　100092093
弁理士　辻居　幸一
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜

最終頁に続く

(54)【発明の名称】不揮発性メモリに対してデータの読み出しおよび書き込みを行うためのデータホワイトニング

(57)【特許請求の範囲】
【請求項１】
不揮発性メモリを管理するためのシステムであって、
不揮発性メモリと、
システム・オン・チップ（ＳｏＣ）と、
を備え、
前記システム・オン・チップは、
データをホワイトニングするよう構成された暗号化モジュールと、
前記暗号化モジュールに接続され、受け取ったデータが非秘密データまたは秘密データのいずれであるかを検出するように構成されたメモリインターフェースと、を備え、
前記受け取ったデータが非秘密データである場合、前記暗号化モジュールは前記受け取った非秘密データをホワイトニングし、前記メモリインターフェースは前記ホワイトニングされた非秘密データを前記不揮発性メモリ内に格納する、システム。
【請求項２】
請求項１に記載のシステムであって、前記暗号化モジュールは、次世代標準暗号化方式（ＡＥＳ）エンジンを備える、システム。
【請求項３】
請求項１に記載のシステムであって、
前記ＳｏＣは、前記秘密データおよび非秘密データを前記不揮発性メモリとやり取りするためのコマンドを前記メモリインターフェースに発行するよう構成されたファイルシス

テムをさらに含み、
前記メモリインターフェースは、前記不揮発性メモリ内の前記秘密データまたは前記非秘密データの格納を管理するためのメモリ管理データを生成するよう構成されたメモリトランスレーションレイヤを備える、システム。
【請求項４】
請求項３に記載のシステムであって、前記ファイルシステムは、さらに、
前記秘密データと共に暗号鍵を提供し、前記非秘密データと共に暗号鍵を提供しないよう構成されている、システム。
【請求項５】
メモリインターフェースを用いて不揮発性メモリを管理する方法であって、
前記不揮発性メモリに格納する情報を受信する工程と、
前記情報が、秘密情報であるか非秘密情報であるかを検出する工程と、
前記検出に基づいて、プライベート鍵およびホワイトニング鍵のいずれかを選択する工程と、前記ホワイトニング鍵は前記情報が非秘密情報である場合に選択され、
前記情報が非秘密情報である場合に、前記選択されたホワイトニング鍵を用いた前記情報のホワイトニングを有効にして、前記不揮発性メモリに格納する前記情報をホワイトニングする工程と、
を備える、方法。
【請求項６】
請求項５に記載の方法であって、前記検出する工程は、前記プライベート鍵が、前記不揮発性メモリに前記情報を書き込むためのコマンドと共に受信されたか否かを判定する工程を備える、方法。
【請求項７】
請求項５に記載の方法であって、前記ホワイトニング鍵の値は、前記情報および前記情報に関連づけられたアドレスに依存しない、方法。
【請求項８】
請求項５に記載の方法であって、さらに、
前記情報が秘密情報であると検出された場合に、第１の初期化ベクトルを受信する工程と、
前記情報が非秘密情報であると検出された場合に、第２の初期化ベクトルを生成する工程と、
前記情報が秘密情報であるか非秘密情報であるかに基づいて、前記第１および第２の初期化ベクトルのいずれかを選択する工程と、
を備える、方法。
【請求項９】
請求項５に記載の方法であって、さらに、
前記受信した情報のメモリ管理データを生成する工程と、
前記不揮発性メモリに格納するために、前記ホワイトニング鍵を用いた前記メモリ管理データの暗号化を有効にする工程と、
を備える、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＮＡＮＤ型フラッシュメモリなどの不揮発性メモリに格納するためにデータをホワイトニングおよび管理するためのシステム、方法、および、装置に関する。
【背景技術】
【０００２】
ＮＡＮＤ型フラッシュメモリおよびその他の不揮発性メモリは、通例、大容量記憶装置として電子デバイス内で用いられる。例えば、携帯型メディアプレーヤは、しばしば、音楽、ビデオ、および、その他のメディアを格納するためにフラッシュメモリを備えている

。

【０００３】

記憶容量を維持または増大させつつ、これらの電子デバイスのサイズを減少させるために、フラッシュ型およびその他のタイプのメモリセルは、絶えず小型化および高密度化されている。これは、不揮発性メモリへの書き込みおよび不揮発性メモリからの読み出しの信頼性を低下させるプログラムディスターブなどの問題を引き起こしうる。特に、１または複数のページ（例えば、不揮発性メモリに一度に書き込むことのできるデータの単位）のプログラミングの際に、メモリセルに格納されるデータビットがほぼすべて同じ値（例えば、ほぼすべてが１または０）である場合、これらのメモリセルに印加されたプログラミング電圧が、近接するメモリセルに強い電界効果を及ぼしうる。この結果、影響を受けたメモリセルが不正確にプログラミングされたり部分的にプログラミングされたりする場合があり、それによって、次の読み出し動作中にデータが不正確に解釈される可能性が増大しうる。

【発明の概要】

【０００４】

ＮＡＮＤ型フラッシュメモリなどの不揮発性メモリへの格納に向けてデータに対してホワイトニングまたはその他の管理を行うためのシステム、装置、および、方法が提供されている。「ホワイトニング」とは、一般に、データシーケンスのランダム性を増大させることを意味し、データシーケンスの１および０の数が大きく偏る可能性を低減しうるものである。データのホワイトニングは、次世代標準暗号化方式（ＡＥＳ）に基づくブロック暗号などの暗号化モジュールを用いて実行できる。暗号化モジュールは、秘密情報（例えば、個人情報）のセキュリティを提供するために用いられてもよいため、ここに開示する実施形態は、ホワイトニング専用のハードウェアを必要とすることなくデータホワイトニングを提供できる。

【０００５】

一部の実施形態では、メディアプレーヤなどの電子デバイスが提供される。電子デバイスは、システム・オン・チップ（ＳｏＣ）と、フラッシュメモリなどの不揮発性メモリとを備えてよい。ＳｏＣは、暗号化モジュールとメモリインターフェースとを備えてよい。メモリインターフェースは、読み出しコマンドおよび書き込みコマンドに応答して、それぞれ、不揮発性メモリに対してデータの読み出しおよびプログラミングを行うために、不揮発性メモリと通信することができる。一部の実施形態において、メモリインターフェースは、不揮発性メモリと、読み出しおよび書き込みコマンドを発行しうるＳｏＣのファイルシステムとの間のインターフェースとして機能しうるトランスレーションレイヤを備えてよい。

【０００６】

プログラムディスターブまたはその他の信頼性の問題を防止するために、メモリインターフェースは、ファイルシステムが暗号化を要求する秘密データだけでなく、不揮発性メモリに書き込まれるすべてのデータを暗号化するよう、暗号化モジュールに指示することができる。メモリインターフェースは、暗号化を要求されていない非秘密データ、および、不揮発性メモリに格納される任意のメモリ管理データを暗号化することができる。メモリ管理データは、メタデータとも呼ばれ、秘密または非秘密データの格納を管理するためにメモリインターフェースによって生成される任意のデータを含みうる。一部の実施形態において、メタデータは、ファイルシステムがデータのために提供するアドレス（すなわち、「論理アドレス」）と、不揮発性メモリにおいてデータが格納されるまたは格納されたアドレス（すなわち、「物理アドレス」）との間のマッピングの追跡記録を保持しうるメモリマップ情報を含んでよい。

【０００７】

ＳｏＣの暗号化モジュールは、１または複数の初期値を用いてデータを暗号化および復号することが可能であり、かかる初期値は、「暗号化シード」とも呼ばれる。ＡＥＳエンジンについては、暗号化シードは、鍵および初期化ベクトル（「ＩＶ」）を含みうる。メ

モリインターフェースは、読み出しまたはプログラミングされるデータのタイプ（秘密データ、非秘密データ、または、メタデータ）に基づいて、暗号化シードを生成または選択することができる。一部の実施形態において、メモリインターフェースは、データを書き込みまたは読み出しするためのコマンドをファイルシステムから受信することができると共に、情報が秘密であるか非秘密であるかを検出することができる。データが秘密である場合には、メモリモジュールは、ファイルシステムによって提供された安全なプライベート鍵および初期化ベクトルを用いてデータを暗号化することができる。一方、非秘密データについては、メモリインターフェースは、所定のホワイトニング鍵と、データの論理アドレスに基づいて生成されうるＩＶとを用いることができる。

【０００８】

この技術によると、メモリインターフェースは、データの物理アドレスに依存しうる暗号化シードを用いることなく、秘密および非秘密データをホワイトニングすることができる。したがって、秘密および非秘密データは、前の物理アドレスに基づいてデータを復号し、新しい物理アドレスに基づいてデータを再暗号化する必要なく、（例えば、有効な情報および空きブロックを整理するためにデータが移動されるガベージコレクションまたはウェアレベリングの際に）不揮発性メモリの異なる物理ロケーション間で移動されることができる。

【０００９】

一部の実施形態では、メモリインターフェースによって生成されたメタデータは、不揮発性メモリ内に維持されてよい。これらの実施形態において、メモリインターフェースは、メタデータが不揮発性メモリに格納される前にホワイトニングするために、メタデータを暗号化することができる。ＡＥＳエンジンについては、メモリインターフェースは、所定のホワイトニング鍵と、メタデータが格納される物理アドレスに基づいて生成されうるＩＶとをＡＥＳエンジンに供給することができる。ＩＶは、物理アドレスに基づく場合があるため、秘密データまたは非秘密データの場合と異なり、メモリインターフェースは、（例えば、ガベージコレクション中に）異なる物理ロケーションの間でメタデータを移動させる際に、メタデータの各ページに対して復号および再暗号化を実行してよい。

【図面の簡単な説明】

【００１０】

本発明の上述およびその他の態様および利点については、添付の図面を参照しつつ行う以下の詳細な説明で詳述する。なお、図面において、同じ符号は同じ構成要素を指すものとする。

【００１１】

【図１】本発明の一実施形態に従って構成された電子デバイスを示す概略図。

【００１２】

【図２】本発明の一実施形態に従って構成され、電子デバイスに実装されたシステム・オン・チップを示す概略図。

【００１３】

【図３】本発明の一実施形態に従って不揮発性メモリにデータを書き込むための処理の一例を示すフローチャート。

【００１４】

【図４】本発明の一実施形態に従って不揮発性メモリからデータを読み出すための処理の一例を示すフローチャート。

【００１５】

【図５】本発明の一実施形態に従って不揮発性メモリの物理ページ間でデータを移動させるための処理の一例を示すフローチャート。

【発明を実施するための形態】

【００１６】

図１は、電子デバイス１００の概略図である。いくつかの実施形態において、電子デバイス１００は、携帯型メディアプレーヤ（例えば、カリフォルニア州クパチーノのアップ

ル社が提供するｉＰｏｄ（登録商標））、携帯電話（例えば、アップル社が提供するｉＰｈｏｎｅ（登録商標））、ポケットサイズのパーソナルコンピュータ、携帯情報端末（ＰＤＡ）、デスクトップコンピュータ、ラップトップコンピュータ、および、任意の他の適切なタイプの電子デバイスであってもよいし、それらを含むものであってもよい。

【００１７】

電子デバイス１００は、システム・オン・チップ（ＳｏＣ）１１０および不揮発性メモリ１６０を備えてよい。不揮発性メモリ１６０は、フローティングゲート技術に基づくＮＡＮＤ型フラッシュメモリであってよく、それぞれ一度に消去可能である複数の「ブロック」に分けられ、さらに、それぞれ一度にプログラム可能かつ読み出し可能である複数の「ページ」に分けられてよい。不揮発性メモリ１６０の各ページは、物理ページアドレスを用いてアドレス指定できる。図１（および、それ以降の図）と、開示されている様々な実施形態は、フラッシュ技術を用いるものについて説明しているが、任意のその他のタイプの不揮発性メモリを実装することも可能である。例えば、不揮発性メモリ１６０は、ＮＡＮＤ型フラッシュメモリ、ＮＯＲ型フラッシュメモリ、任意の次世代不揮発性メモリ、または、それらの組み合わせを含みうる。また、一部の実施形態において、不揮発性メモリ１６０は、オフチップではなくシステム・オン・チップ１１０上に実装されてよく、電子デバイス１００は、図の簡単のために図１では図示していないが、電源または任意のユーザ入出力デバイスなど、他の構成要素を備えうる。

【００１８】

システム・オン・チップ１１０は、ＳｏＣ制御回路１２０、暗号化モジュール１３０、メモリ１４０、および、不揮発性メモリインターフェース１５０を備えてよい。ＳｏＣ制御回路１２０は、ＳｏＣ１１０の全体的な動作および機能と、その他の構成要素を制御しうる。例えば、ユーザ入力またはアプリケーションの指示に応答して、ＳｏＣ制御回路１２０は、不揮発性メモリ１６０からデータを取得または不揮発性メモリ１６０にデータを格納するために、不揮発性メモリインターフェース１５０に読み出しまたは書き込みコマンドを発行してよい。ＳｏＣ制御回路１２０は、電子デバイス１００の機能を実現するよう動作する、任意の組み合わせのハードウェア、ソフトウェア、および、ファームウェア、並びに、任意のコンポーネント、回路、または、ロジックを備えてよい。

【００１９】

メモリ１４０は、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、シンクロナスダイナミックランダムクセスメモリ（ＳＤＲＡＭ）、ダブルデータレート（ＤＤＲ）ＲＡＭ、キャッシュメモリ、または、読み出し専用メモリ（ＲＯＭ）などの、任意の適切なタイプの揮発性または不揮発性メモリを備えていてよい。メモリ１４０は、不揮発性メモリ１６０に対するプログラムまたは読み出しのためのデータを一時的に格納できるデータソースを備えてよい。一部の実施形態において、メモリ１４０は、ＳｏＣ制御回路１２０またはメモリインターフェース１５０によって実行できるファームウェアまたはソフトウェアアプリケーションを格納する、ファームウェアまたはソフトウェアに一次記憶を提供する、または、それらの両方を行うことが可能である。

【００２０】

不揮発性メモリインターフェース１５０は、任意の適切な組み合わせのハードウェアおよびソフトウェアを備えてよく、ＳｏＣ制御回路１２０および不揮発性メモリ１６０の間のドライバまたはインターフェース（例えば、フラッシュインターフェース）として機能しうる。例えば、メモリインターフェース１５０は、ＳｏＣ制御回路１２０からの読み出しまたは書き込みコマンドを解釈して、不揮発性メモリ１６０のバスプロトコルに適合する読み出しまたはプログラミングの命令を生成できる。メモリインターフェース１５０は、不揮発性メモリ１６０のページおよびブロックを管理するために、これらの機能と、後述するように、不揮発性メモリ１６０に格納されるデータをホワイトニングするよう暗号化モジュール１３０に指示すること、および、ウェアレベリングまたはガベージコレクション中に不揮発性メモリ１６０の物理ロケーション間でデータページを移動することなど、その他の任意の適切な機能とを実行できる。メモリインターフェース１５０は、ＳｏＣ

制御回路１２０とは別個のモジュールとして図示されているが、一部の実施形態では、これらのモジュールは、ハードウェアまたはソフトウェア構成要素（または両方）を共有してよく、機能の一部に互換性があってもよい。

【００２１】

暗号化モジュール１３０は、適切な暗号に基づいて暗号化および復号を実行するよう構成された任意のハードウェアまたはソフトウェア、もしくは、それらの組み合わせであってもよいし、それらを含むものであってもよい。例えば、暗号化モジュール１３０は、次世代標準暗号化方式（ＡＥＳ）、データ暗号化規格（ＤＥＳ）、または、ＲＳＡに基づいてよい。暗号化モジュール１３０は、不揮発性メモリ１６０に格納された、または、（例えば、図１には示していないが、Ｗｉ－Ｆｉ（登録商標）回路などの通信回路を用いて）電子デバイス１００に対して送受信される、秘密データ（個人情報または課金情報など）にセキュリティを提供できる。セキュリティの提供に加えて、暗号化モジュール１３０が用いる暗号化アルゴリズムは、自身が暗号化するデータのホワイトニングまたはランダム化を行うさらなる機能を提供してもよい。したがって、暗号化モジュール１３０は、データが秘密でない場合でもデータの暗号化を指示されてよく、その結果、そのデータは、不揮発性メモリ１６０に書き込まれる前にホワイトニングされることができる。このように、プログラムディスターブおよびその他の信頼性の問題を、低減することができる。

【００２２】

暗号化モジュール１３０は、ＳｏＣ制御回路１２０または不揮発性メモリインターフェース１５０によって提供される１または複数の「暗号化シード」を用いて、データを暗号化および復号できる。なお、暗号化シードは、暗号化または復号を実行するために暗号化アルゴリズムによって必要とされうる。一部の実施形態において、特にＡＥＳに基づく暗号化モジュールについて、暗号化シードは、鍵および初期化ベクトル（「ＩＶ」）を含みうる。元の暗号化されていないデータを暗号化データから回復するために、復号に用いる暗号化シードは、もともと暗号化に用いたシードと同じである必要があってよい。したがって、電子デバイスがこれらの暗号化シードを管理および生成するために利用できる様々な技術を図示した図２ないし図５を参照しつつ、様々な特徴を以下で開示する。

【００２３】

ここで、図２によると、システム・オン・チップ（ＳｏＣ）２１０の概略図が示されている。ＳｏＣ２１０は、ＳｏＣ１１０のより詳細な図であってもよいし、完全に異なる実装のシステム・オン・チップであってもよい。ＳｏＣ２１０は、ＳｏＣ制御回路２２０、暗号化モジュール２３０、および、不揮発性メモリインターフェース２５０を備えてよく、これらの構成要素は、それぞれ、図１の同じ名称の構成要素について上述した特徴および機能のいずれかを有するものであり、その逆も成り立つ。例えば、一部の実施形態において、暗号化モジュール２３０は、次世代標準暗号化方式（ＡＥＳ）エンジンであってもよいし、それを備えるものであってもよい。ＡＥＳエンジンは、暗号化シードを取得するための鍵入力およびＩＶ入力と、データ入力（図示せず）から受信したデータの暗号化を有効または無効にするためのイネーブル入力とを有してよい。

【００２４】

図２にはメモリモジュールが図示されていないが、１または複数の適切なバッファまたはその他の一時記憶モジュールを、図２に示した任意の様々な構成要素の間に提供できることを理解されたい。これらのメモリモジュールは、ＳｏＣ制御回路２２０の内部、ＳｏＣ制御回路２２０の外部（例えば、図１のメモリ１４０）、もしくは、不揮発性メモリインターフェース２５０の内部または外部など、ＳｏＣ２１０の任意の適切な位置に配置されてよい。

【００２５】

ＳｏＣ制御回路２２０は、電子デバイス（例えば、図１の電子デバイス１００）の一般的な機能を提供できる。例えば、ＳｏＣ制御回路２２０は、ユーザが起動した任意のアプリケーション（例えば、音楽またはその他のメディアアプリケーション）を実行することが可能であり、電子デバイスのオペレーティングシステムを備えることができる。動作中

、アプリケーションおよびその他のプログラムまたはファームウェアは、大容量記憶装置（例えば、図１の不揮発性メモリ１６０）にデータを格納したり、そこからデータを取り出したりすることが必要になる場合がある。ＳｏＣ制御回路２２０は、情報のタイプ、実行されているアプリケーション、または、電子デバイスを操作している特定のユーザなど、様々な要素に基づいて、データを「秘密」または「非秘密」情報として割り振ってよい。「秘密データ」は、一般に、データを暗号化する指示と共に（例えば、後述のファイルシステム２２２から）保存に向けて提供される任意の情報のことを指しうる。秘密データとしては、例えば、個人情報およびクレジットカード情報が挙げられる。

【００２６】

ＳｏＣ制御回路２２０は、アプリケーションまたはオペレーティングシステムによって指示された読み出しおよび書き込みコマンドを発行するために、ファイルシステム２２２を備えてよい。ファイルシステム２２２は、ファイルアロケーションテーブル（ＦＡＴ）ファイルシステムなど、任意の適切なタイプのファイルシステムを含みうる。各読み出しまたは書き込みコマンドと共に、ファイルシステム２２２は、データが読み出しまたは書き込みされる場所を示す論理アドレスを提供することができる。ファイルシステム２２２は、さらに、オペレーティングシステムまたはアプリケーションが、データが秘密であると判定したか否かについての情報を提供できる。秘密データについては、ファイルシステム２２２は、読み出しまたは書き込みコマンドと共にプライベート鍵および初期化ベクトルを提供できる。データが秘密でない場合、ファイルシステム２２２は、有効な暗号化シードを提供しなくてよい。例えば、ファイルシステム２２２は、有効な暗号化シードの代わりにＮＵＬＬ値を提供してよい。

【００２７】

ファイルシステム２２２は、電子デバイス（例えば、ＮＡＮＤ型フラッシュ）に実装された不揮発性メモリに直接的には適合していないプロトコルを用いて、論理アドレスおよび暗号化シードと共に、読み出しおよび書き込み要求を提供してよい。例えば、ファイルシステム２２２によって提供される論理アドレスは、ハードドライブを用いたシステムに典型的な規則またはプロトコルを用いてよい。ハードドライブを用いたシステムは、フラッシュメモリと違って、ブロック消去を最初に実行することなくメモリロケーションに上書きすることができ、デバイスの寿命を延ばすために、ウェアレベリングを実行する必要がない。したがって、ＳｏＣ２１０は、不揮発性メモリインターフェース２５０を備えてよく、不揮発性メモリインターフェース２５０は、不揮発性メモリに適した方法でファイルシステム要求を処理するために、任意のメモリ固有（例えば、フラッシュ固有）またはベンダー固有（もしくは両方）の機能を実行できる。

【００２８】

不揮発性メモリインターフェース２５０は、トランスレーションレイヤ２５２と、マルチプレクサ２５４および２５６と、バスコントローラ２５８とを備えていてよい。一部の実施形態において、トランスレーションレイヤ２５２は、フラッシュトランスレーションレイヤであってよい。トランスレーションレイヤ２５２は、ファイルシステム２２２からの読み出しまたは書き込みコマンドを解釈して、読み出しおよび書き込みコマンドを不揮発性メモリに適切な命令に翻訳することができる。より具体的には、書き込み／プログラム動作において、ファイルシステム２２２から受信した論理アドレスが、不揮発性メモリ上の消去済みの空き物理ロケーションに対応しないこともあるため、トランスレーションレイヤ２５２は、その論理アドレスに直接的にデータを書き込めないことがある。その代わり、トランスレーションレイヤ２５２は、ファイルシステム２２２から受信した論理アドレスを、不揮発性メモリ上の空き物理アドレスに変換できる。読み出し動作において、トランスレーションレイヤ２５２は、受信した論理アドレスに対応する格納データの実際の物理アドレスを決定できる。

【００２９】

トランスレーションレイヤ２５２は、論理および物理アドレス間のこのマッピングを維持するために、メモリ管理データ（すなわち「メタデータ」）を生成できる。メモリ「管

理データ」すなわち「メタデータ」は、ファイルシステムによって提供されない任意のデータを含んでよく、かかるデータは、インターフェース２５０の構成要素（例えば、トランスレーションレイヤ２５２）によって生成されてよい。トランスレーションレイヤ２５２は、さらに、後述するように、ガベージコレクションまたはウェアレベリングの実行など、不揮発性メモリのストレージを管理するための任意の他の適切なタスクを実行できる。

【００３０】

メモリ管理データ（例えば、決定された物理アドレス）を用いて、トランスレーションレイヤ２５２は、バスコントローラ２５８に読み出し要求および書き込み要求を提供することが可能であり、不揮発性メモリ上の記憶空間を解放するために、バスコントローラ２５８に消去要求を発行することが可能である。バスコントローラ２５８は、要求された読み出し、書き込み、および、消去動作を実行するために、不揮発性メモリが利用するバスプロトコルを用いて、不揮発性メモリと通信しうる。一部の実施形態において、バスコントローラ２５８は、ベンダー固有の不揮発性メモリと通信することができる「メモリテクノロジドライバ」を備えてよい。

【００３１】

不揮発性メモリインターフェース２５０は、バスコントローラ２５８に不揮発性メモリへのデータの書き込みを行わせる前に、暗号化モジュール２３０がデータをホワイトニングすることを可能にする。一部の実施形態において、トランスレーションレイヤ２５２は、暗号化モジュール２３０が、格納に先立って、あらゆるタイプのデータまたはメタデータ（例えば、秘密データ、非秘密データ、または、メモリ管理データ）を暗号化することを可能にし、その結果、ホワイトニングされたデータは、プログラム／読み出し／消去ディスターブの発生を低減または最小化することができる。データをホワイトニングするために、トランスレーションレイヤ２５２は、どちらの暗号化シード（ここでは、鍵および初期化ベクトル）を暗号化モジュール２３０に提供すべきかを決定しうる。暗号化シードは、復号が実行された時に回復可能であるように、かつ、利用可能な場合にはファイルシステム２２２によって提供された安全な暗号鍵が用いられるように選択されてよく、しばしば、そのように選択されることが好ましい。

【００３２】

トランスレーションレイヤ２５２は、暗号化モジュール２３０が用いる鍵を選択するよう、マルチプレクサ２５４を制御しうる。一部の実施形態において、トランスレーションレイヤ２５２は、暗号化／ホワイトニングされるデータのタイプに基づいて、プライベート鍵および所定のホワイトニング鍵のいずれかを選択してよい。トランスレーションレイヤ２５２は、秘密データのための読み出しまたは書き込みコマンドが受信されたことの検出に応答して、ファイルシステム２２２によって提供されうるプライベート鍵を選択してよい。他のタイプのデータ（例えば、非秘密データまたは非メタデータ）については、有効なプライベート鍵が提供されなくてもよいため、トランスレーションレイヤ２５２は、所定のホワイトニング鍵を選択してよい。ホワイトニング鍵は、様々な値の内の任意の値を取ってよく、一部の実施形態においては、ハードコード化されてもよいし、インターフェース２５０内にハードワイヤードされてもよい。ホワイトニング鍵は、セキュリティのためだけでなく、ホワイトニングに適した値を有していてよい。例えば、デバイスシミュレーションまたは数理モデルを用いて、様々なデータ値に対して（他のホワイトニング鍵の候補よりも）高度なホワイトニングを提供するように、ホワイトニング鍵の値を予め決定してよい。したがって、一部の実施形態において、ホワイトニング鍵の値は、読み出しまたは書き込みされるデータに依存しなくてよい。また、ホワイトニング鍵の値は、ロケーション非依存（例えば、データの対応する論理または物理アドレスに依存しない）であってよい。

【００３３】

トランスレーションレイヤ２５２は、暗号化モジュール２３０が用いる初期化ベクトルを選択するよう、マルチプレクサ２５６を制御しうる。プライベート鍵の場合と同様に、

ファイルシステム２２２は、秘密情報に対応する読み出しまたは書き込みコマンドと共に初期化ベクトルを提供できる。この初期化ベクトルは、読み出しまたは書き込みコマンドと共に受信した論理アドレスに基づいてよい。ファイルシステム２２２は、セキュリティを増すために論理アドレスに基づくＩＶを提供できる。特に、ファイルシステム２２２が、複数の論理アドレスに同じデータを格納するための書き込みコマンドを発行した場合、結果として生じる暗号化データは、同じにならない。

【００３４】

他のタイプのデータ（例えば、非秘密データまたはメタデータ）については、トランスレーションレイヤ２５２は、論理に基づいたＩＶを用いるか物理アドレスに基づいたＩＶを用いるかを選択することができる。さらに具体的には、インターフェース２５０は、格納または取り出される情報の物理アドレスまたは論理アドレスに基づいて初期化ベクトルを算出することが可能であり、トランスレーションレイヤ２５２は、これらのベクトルから選択するよう、マルチプレクサ２５６を制御しうる。上述のように、（論理または物理）アドレスに基づく初期化ベクトルを用いることにより、セキュリティを向上できる。また、トランスレーションレイヤ２５２は、有効な論理および物理アドレスと共にメタデータを維持することができるので、論理または物理アドレスに基づいてデータを暗号化することで、インターフェース２５０が後の復号のためにＩＶを再構築することを可能にできる。

【００３５】

メタデータは、論理アドレスと関連づけられていない場合があるため、トランスレーションレイヤ２５２は、メタデータの暗号化または復号のために、物理アドレスに基づくＩＶを選択することができる。すなわち、メタデータは、ファイルシステム２２２によって提供される代わりに、インターフェース２５０によって生成されてよいため、論理アドレスからは、有効なＩＶを生成できない。一部の実施形態において、不揮発性メモリに格納される、または、格納された任意の情報に対して、トランスレーションレイヤ２５２は、論理アドレスを利用できない場合（例えば、メタデータまたは任意のその他の適切な情報の場合）には物理アドレスに基づくＩＶを選択してよい。

【００３６】

トランスレーションレイヤ２５２は、論理アドレスに基づくＩＶを用いて非秘密データを暗号化または復号することを可能にすることができる。一部の実施形態において、不揮発性メモリに格納される、または、格納された任意の情報に対して、トランスレーションレイヤ２５２は、非秘密または秘密データなどについては、利用できる時はいつでも論理アドレスを用いて情報を暗号化することを可能にできる。特にガベージコレクションまたはウェアレベリングの際には、これにより、効果的なメモリ管理が可能になる。トランスレーションレイヤ２５２は、プログラミングおよび消去動作が不揮発性メモリ内で均一に分散されることを保証し、消去のためにブロックを解放するために、ウェアレベリングおよびガベージコレクションを実行できる。ウェアレベリングおよびガベージコレクションは、或る物理アドレスから新たな物理アドレスにページを移動させることを含みうる。物理アドレスの変化に影響されえない論理アドレスに基づくＩＶを用いることによって、トランスレーションレイヤ２５２は、データを復号および再暗号化する必要なしに、秘密および非秘密データを移動することができる。すなわち、（物理データに基づいて暗号化される）メタデータの移動で必要とされうるように、以前の物理アドレスに基づいて格納されたデータを復号し、新たな物理アドレスを用いてデータを再暗号化する動作は、トランスレーションレイヤ２５２では必要としなくてよい。不揮発性メモリ上の物理ロケーション間でのデータの移動については、図５を参照しつつ以下で詳述する。

【００３７】

ここで、図３ないし５によると、フラッシュメモリなどの不揮発性メモリに格納するためにデータのホワイトニングを行うための処理の例を示すフローチャートが示されている。これらの処理の工程は、図２のインターフェース２５０などのメモリインターフェースによってまたは、電子デバイスの任意の構成要素または構成要素の組み合わせによって実

行されてよい。ただし、簡単のため、メモリインターフェースによって実行されるものとして、処理を説明しているが、それに限定されない。

【００３８】

最初に図３によると、書き込みコマンドに応答して、不揮発性メモリ（例えば、ＮＡＮＤ型フラッシュメモリ）に格納するためにデータをホワイトニングするための処理３００のフローチャートが図示されている。処理３００は工程３０２から開始しうる。工程３０４で、メモリインターフェースは、論理アドレスにデータを書き込むためのコマンドを受信することができる。一部の実施形態において、書き込みコマンドは、ファイルシステム（例えば、ＦＡＴファイルシステム）から受信されてよく、データは、オンチップメモリ（例えば、図１のメモリ１４０）に格納されてよい。データをホワイトニングするのにどちらの暗号化シードを用いるかを決定するために、メモリインターフェースは、工程３０６で、データが秘密情報であるか非秘密情報であるかを判定することができる。メモリインターフェースは、有効な暗号化シード（例えば、プライベート鍵およびＩＶ）が書き込みコマンドの一部として受信された場合には、データが秘密であると検出してよい。データが秘密であると、メモリインターフェースが判定した場合、工程３０８で、メモリインターフェースは、受信したプライベート鍵およびＩＶを選択することができる。一方、これらの暗号化シードの値は、ファイルシステムによって提供されない場合もあり、その際、処理３００は、工程３１０に進んでよい。工程３１０で、メモリインターフェースは、所定のホワイトニング鍵を選択することができ、工程３１２で、データの論理アドレスに基づいて、初期化ベクトルを生成することができる。

【００３９】

工程３０８または工程３１２から、処理３００は、工程３１４に進みうる。工程３１４で、メモリインターフェースは、選択された鍵と、選択または生成された初期化ベクトルとを用いて、データを暗号化することができる。これは、暗号化モジュール（図２の暗号化モジュール２３０など）のイネーブル信号をアサートすると共に、選択／生成された鍵およびＩＶを暗号化モジュールに提供することを含みうる。このように、秘密データに対して、データはファイルシステムによって指定された方法で保護されることが可能であり、同様にホワイトニングされることが可能である。非秘密データは、暗号化される必要はないのだが、プログラムディスターブまたはその他の読み出し／書き込み／消去の問題を防ぐために、ホワイトニング用に設計された鍵を用いて暗号化されてよい。

【００４０】

工程３１６に進んで、メモリインターフェースは、不揮発性メモリ上にプログラミングされるべきデータのためのメタデータを算出することができる。例えば、フラッシュメモリについて、メモリインターフェースは、（工程３０４で受信した）論理アドレスとフラッシュメモリの物理アドレスとの間のマッピングの形態のメタデータを生成することができるフラッシュトランスレーションレイヤを備えてよい。マッピングおよび任意のその他の適切なメタデータを用いて、メモリインターフェースは、（例えば、バスコントローラを介して）、算出された物理アドレスで不揮発性メモリ上に暗号化／ホワイトニングされたデータをプログラミングすることができる。したがって、工程３０６ないし工程３１８（図３において点線で囲まれたサブ処理３０５）は、ファイルシステムによって指示されたようにデータを格納するためにメモリインターフェースが実行する工程であってよい。

【００４１】

メモリインターフェースは、例えば、後にデータを読み出すためのコマンドが受信された時に、格納されたデータの物理アドレスを呼び出すことができるように、工程３１６で算出されたメタデータを維持する必要がありうる。したがって、処理３００は、不揮発性メモリにメタデータを格納するために、サブ処理３１９の工程に進みうる。まず、工程３２０で、メモリインターフェースは、ホワイトニング鍵を選択できる。そのホワイトニング鍵は、（例えば、工程３１０で）非秘密データのために選択されたホワイトニング鍵と同じであってもよいし、同じでなくてもよい。次いで、工程３２２で、メモリインターフェースは、不揮発性メモリの物理アドレスに基づいて、初期化ベクトルを生成できる。こ

の工程は、メモリインターフェースが、不揮発性メモリ内でメタデータを格納する場所を決定し、決定された物理アドレスを用いて初期化ベクトルを算出することを含みうる。一部の実施形態において、メモリインターフェースは、後の取り出しに向けてメタデータの格納場所を示すために、（例えば、メモリインターフェースの内部のメモリに）不揮発性メモリに対するポインタを維持してもよいし、各ブロック内の特定のページをメタデータの格納用に割り当ててもよい。

【００４２】

工程３２４に進んで、メモリモジュールは、選択された鍵および生成された初期化ベクトルを用いて、メタデータを暗号化できる。このように、工程３２６で不揮発性メモリに格納される前に、メタデータは、潜在的なプログラムディスターブまたはその他の読み出し／書き込み／消去の問題を回避するために、暗号化モジュールによってホワイトニングされることもできる。次いで、処理３００は、工程３２８で終了してよく、これで、（ファイルシステムによって指示されたように）ホワイトニング済みの秘密または非秘密データと、格納データに関連づけられたホワイトニング済みメモリ管理データとの不揮発性メモリへの格納が完了する。

【００４３】

図４は、例えば、ファイルシステムから受信した読み出しコマンドを処理するために、メモリインターフェースが実行できる処理４００を示すフローチャートである。処理４００は、処理３００の逆の動作と見なすことができる。したがって、上述の図３の工程の記載を、図４の対応する工程にも適用できることから、図４については簡潔な説明にとどめている。

【００４４】

処理４００は工程４０２から開始しうる。次いで、工程４０４で、メモリインターフェースは、論理アドレスからデータを読み出すためのコマンドを受信しうる。要求されたデータが格納されている不揮発性メモリの物理アドレスを特定するために、メモリインターフェースは、サブ処理４０５の工程を実行することができる。サブ処理４０５は、格納されたメタデータを取得および処理するための工程を含みうる。特に、メモリインターフェースは、工程４０６で、不揮発性メモリの特定の物理ロケーションから、格納されたメタデータを読み出し、工程４０８でホワイトニング鍵を選択し、工程４１０で特定の物理ロケーションに基づいて初期化ベクトルを生成し、ホワイトニング鍵と生成された初期化ベクトルとを用いてメタデータを復号することができる。次いで、メタデータの復号が完了すると、メモリインターフェースは、読み出しコマンドによって要求されたデータの物理アドレスを決定するために、工程４１２でメタデータを解釈することができる。

【００４５】

次に、処理４００は、要求されたデータを読み出して、処理し、ファイルシステムに提供するための工程を含むサブ処理４１３に進んでよい。まず、工程４１４において、メモリインターフェースは、メタデータから予め決定した物理アドレスから、格納されたデータを読み出すことができる。次いで、メモリインターフェースは、（秘密データのために）工程４１８でファイルシステムから受信したプライベート鍵およびＩＶを選択するか、もしくは、（非秘密データのために）工程４２０でホワイトニング鍵を選択し工程４２２で論理アドレスに基づいてＩＶを生成することができる。工程４１８または工程４２２に続いて、メモリインターフェースは、選択／生成された鍵および初期化ベクトルを用いて、秘密または非秘密データを復号することができる。これで、ファイルシステムによって要求された、元々のホワイトニングされていないデータを生成でき、メモリインターフェースは、工程４２６でファイルシステムにこのデータを提供できる。処理４００は、工程４２８で終了してよい。

【００４６】

次に図５によると、不揮発性メモリ（例えば、フラッシュメモリ）の物理ページおよび／またはブロックの間でデータを移動させるためにメモリインターフェースが実行できる処理５００のフローチャートが図示されている。データは、様々な理由で、或る物理ロケ

ーションから別の物理ロケーションに移動されうる。例えば、メモリインターフェースは、不揮発性メモリ上で消去および再書き込みの分布を一様にするためにウェアレベリングを実行する際に、データまたはメタデータを移動しうる。あるいは、メモリインターフェースは、メモリセルのブロックの信頼性が実質的に低下した場合に、消去のためにブロックを解放するため、または、ブロックの使用を中止するために、そのブロックからデータまたはメタデータを移動しうる。メモリインターフェース（特に、トランスレーションレイヤ）は、様々な理由で、ページの再マッピングを開始しうるため、処理５００の工程は、移動時にデータが暗号化／復号される（またはされない）方法に主に焦点を置き、実行される特定の管理動作には焦点を置いていない。これは、単に図を必要以上に複雑にすることを防ぐためのものであり、処理５００の一般的な特徴は、不揮発性メモリの異なる物理アドレス間でのデータ移動を含む任意のメモリ管理動作に組み込まれてもよいし適合されてもよいことを理解されたい。

【００４７】

処理５００は工程５０２から開始しうる。次いで、工程５０４で、メモリインターフェースは、不揮発性メモリの物理アドレスからページを読み出すことができる。工程５０６で、メモリインターフェースは、ページが含むデータのタイプを決定することができる。例えば、メモリインターフェースは、ブロック内でのページの場所に基づいて、または、任意のその他の適切な方法を用いて、ページがデータ（例えば、秘密または非秘密データ）とメタデータのいずれを含むかを決定できる。ページがデータを含む場合、メモリインターフェースは、工程５０８で新たな物理アドレスにデータを格納できる。メモリインターフェースは、暗号化モジュールを用いてデータの復号および再暗号化を行う必要なく、新たな物理ページアドレスにデータを格納できる。すなわち、メモリインターフェースは、データを移動させる際に、暗号化モジュールを無効化または迂回することができる。これは、データが、秘密であろうとなかろうと、データの物理アドレスにもとより依存しない暗号化シードを用いて暗号化されていてよいからである。したがって、データの物理アドレスの変更は、データの暗号化／ホワイトニング方法に影響することがない。

【００４８】

工程５０８に続いて、メモリインターフェースは、工程５１０で、格納されたデータに対応するメタデータを更新することができる。これにより、メモリインターフェースは、（変更されない）データの論理アドレスと、データが実際に書き込まれる場所との間の適切なマッピングを維持することができる。メタデータ自体が不揮発性メモリに格納されてよいため、工程５１０は、データに対応するメタデータの読み出し、更新、および、書き込みを行うことを含んでよい。これらの工程は、図が必要以上に複雑になるのを避けるために、図５には示されていないが、図３および４に関連して上述したメタデータの書き込みおよび読み出しの工程と同様の工程を含みうる。

【００４９】

工程５０６において、工程５０４で読み出したページがメタデータを含むと、メモリインターフェースが決定した場合、処理５００は工程５１２に移動しうる。秘密または非秘密データと違って、メタデータは、或る物理ロケーションから別の物理ロケーションに移動される時に、復号および再暗号化される必要がありうる。これは、上述のように、メタデータの復号は、（論理アドレスではなく）メタデータが格納されている場所の物理アドレスを用いることを含むため、物理アドレスの変更により、メタデータの管理を最新に保つために、暗号化の変更が必要となりうるからである。したがって、工程５１２で、メモリインターフェースは、メタデータが格納された物理アドレスに基づいて、初期化ベクトルを生成できる。次いで、工程５１４で、メタデータは、生成した初期化ベクトルとホワイトニング鍵とを用いて復号されてよい。次に、工程５１６で、メモリインターフェースは、メタデータが格納される新たな物理アドレスに基づいて、新たな初期化ベクトルを生成してよく、工程５１８で、新たな初期化ベクトルとホワイトニング鍵とを用いてメタデータを再暗号化することができる。次いで、再暗号化されたメタデータは、工程５２０で、新たな物理アドレスに格納されてよい。

【００５０】
工程５１０または工程５２０に続いて、処理５００は、工程５２２に進むことができる。工程５２２で、メモリインターフェースは、さらなるページを移動させるか否かを決定できる。移動させる場合、処理５００は、工程５０４に戻ることができ、メモリインターフェースは、別の物理アドレスからデータを読み出すことができる。移動させない場合、処理５００は、工程５２４に進んで終了してよい。
【００５１】
図３ないし５の処理は例示にすぎないことを理解されたい。本発明の範囲から逸脱することなく、任意の工程を追加、修正、結合、または、再構成することが可能であり、任意のさらなる工程をすることができる。例えば、暗号化モジュールが鍵およびＩＶ以外の暗号化シードを用いる場合、図３ないし５の工程を修正して、異なる暗号化シードを生成することも可能であり、メタデータの暗号化シードは、物理アドレスに基づいてよく、秘密および非秘密データのシードは、論理アドレスに基づいてよい。
【００５２】
また、不揮発性メモリに情報を格納するための本開示のさまざまな実施形態は、秘密データ、非秘密データ、および、メモリ管理データ（すなわち「メタデータ」）の格納に関連して説明されている。これは例示にすぎず、本開示の特徴は、格納された情報がこれら３つのカテゴリに分類されないデバイス実装でも利用可能であることを理解されたい。特に、他のデバイス実装について、デバイスは、（データの移動を効率化できるように）可能であればいつでも論理アドレスに基づいた暗号化シードを用いることが可能であり、論理アドレスが提供されない場合には物理アドレスを用いることができる。アドレスに基づかない暗号化シードについて、デバイスは、プライベート鍵が提供されない場合に、ホワイトニング鍵またはその他の所定の鍵を用いることが可能であり、ホワイトニング鍵は、高度なホワイトニングを提供する能力ゆえに選択されてもよい。
【００５３】
上述の本発明の実施形態は、限定ではなく例示を目的としたものであり、本発明は、以下の特許請求の範囲によってのみ限定される。
適用例１：システムであって、不揮発性メモリと、システム・オン・チップ（ＳｏＣ）と、を備え、
前記システム・オン・チップは、非秘密データおよびメモリ管理データの内の少なくとも一方を含むデータをホワイトニングするよう構成された暗号化モジュールと、前記暗号化モジュールに接続され、前記ホワイトニングされたデータを前記不揮発性メモリに格納するよう構成されたメモリインターフェースと、を備える、システム。
適用例２：適用例１に記載のシステムであって、前記暗号化モジュールは、次世代標準暗号化方式（ＡＥＳ）エンジンを備える、システム。
適用例３：適用例１に記載のシステムであって、前記データは、秘密データをさらに含み、前記ＳｏＣは、前記秘密データおよび非秘密データを前記不揮発性メモリとやり取りするためのコマンドを前記メモリインターフェースに発行するよう構成されたファイルシステムをさらに含み、前記メモリインターフェースは、前記不揮発性メモリ内の前記秘密データまたは前記非秘密データの格納を管理するための前記メモリ管理データを生成するよう構成されたメモリトランスレーションレイヤを備える、システム。
適用例４：適用例３に記載のシステムであって、前記ファイルシステムは、さらに、前記秘密データと共に暗号鍵を提供し、前記非秘密データと共に暗号鍵を提供しないよう構成されている、システム。
適用例５：不揮発性メモリ内のユーザデータの格納を管理するための装置であって、前記ユーザデータのためのメモリ管理データを生成する手段と、前記メモリ管理データを格納する前記不揮発性メモリの第１の物理アドレスを選択する手段と、前記選択された第１の物理アドレスに基づいて、第１の暗号化シードを算出する手段と、前記選択された第１の物理アドレスに格納するために、前記第１の暗号化シードを用いて前記メモリ管理データを暗号化する手段と、を備える、装置。

適用例６：適用例５に記載の装置であって、さらに、前記不揮発性メモリに前記ランダム化されたメモリ管理データをプログラミングする手段を備える、装置。
適用例７：適用例５に記載の装置であって、前記暗号化する手段は、次世代標準暗号化方式（ＡＥＳ）エンジンを備え、前記第１の暗号化シードは、初期ベクトルを含む、装置。
適用例８：適用例７に記載の装置であって、さらに、前記ＡＥＳエンジンのための秘密鍵として所定の鍵を選択する手段を備え、前記所定の鍵は、前記選択された第１の物理アドレスの値に依存しない、装置。
適用例９：適用例５に記載の装置であって、前記メモリ管理データは、前記ユーザデータの論理アドレスを前記ユーザデータの物理アドレスと関連づけるメモリマップ情報を含む、装置。
適用例１０：適用例５に記載の装置であって、さらに、第１の物理アドレスから第２の物理アドレスに前記メモリ管理データを移動させる手段を備え、前記移動させる手段は、前記第１の暗号化シードを用いて前記メモリ管理データを復号するよう前記暗号化モジュールに指示する手段と、前記第２の物理アドレスに基づいて第２の暗号化シードを算出する手段と、前記不揮発性メモリの前記第２の物理アドレスに格納するために、前記第２の暗号化シードを用いて前記メモリ管理データを暗号化するよう、前記暗号化する手段に指示する手段と、を備える、装置。
適用例１１：システムであって、暗号化モジュールと、不揮発性メモリを管理するためのメモリインターフェースであって、前記暗号化モジュールと通信するよう動作可能であるメモリインターフェースと、を備え、
前記インターフェースは、非秘密データを含む情報を論理アドレスに格納するためのコマンドを受信し、前記論理アドレスに基づいて暗号化シードを生成し、前記不揮発性メモリの第１の物理アドレスに格納するために、前記暗号化シードを用いて前記情報を暗号化するよう、前記暗号化モジュールに指示し、前記第１の物理アドレスから前記不揮発性メモリの第２の物理アドレスに前記暗号化された情報を移動させる時に、前記情報の復号を迂回するよう構成されている、システム。
適用例１２：適用例１または１１に記載のシステムであって、前記不揮発性メモリはＮＡＮＤ型フラッシュメモリを含む、システム。
適用例１３：適用例１１に記載のシステムであって、前記メモリインターフェースは、さらに、前記コマンドが少なくとも１つの暗号化シードを欠いていることに基づいて、前記情報が非秘密データを含むことを検出するよう構成されている、システム。
適用例１４：適用例１１に記載のシステムであって、前記メモリインターフェースは、前記不揮発性メモリのガベージコレクションを開始するよう構成されており、前記暗号化された情報は、前記ガベージコレクション中に、前記第１の物理アドレスから前記第２の物理アドレスに移動される、システム。
適用例１５：適用例１１に記載のシステムであって、前記メモリインターフェースは、ファイルシステムと通信するよう動作可能であり、前記コマンドは、前記ファイルシステムから受信される、システム。
適用例１６：適用例１１に記載のシステムであって、前記メモリインターフェースは、さらに、前記論理アドレスを前記第２の物理アドレスに関連づけるように、メモリ管理データを更新し、前記論理アドレスから前記情報を取り出すための読み出しコマンドを受信し、前記メモリ管理データを用いて、前記第２の物理ロケーションを決定し、前記論理アドレスに基づいて前記暗号化シードを再生成し、前記再生成された暗号化シードを用いて前記情報を復号するよう、前記暗号化モジュールに指示するように構成されている、システム。
適用例１７：メモリインターフェースを用いて不揮発性メモリを管理する方法であって、前記不揮発性メモリに格納する情報を受信する工程と、前記情報が、秘密情報であるか非秘密情報であるかを検出する工程と、前記検出に基づいて、プライベート鍵およびホワイトニング鍵のいずれかを選択する工程と、前記選択された鍵を用いた前記情報の暗号化

を有効にして、前記不揮発性メモリに格納する前記情報を暗号化する工程と、を備える、方法。

適用例１８：適用例１７に記載の方法であって、前記検出する工程は、前記プライベート鍵が、前記不揮発性メモリに前記情報を書き込むためのコマンドと共に受信されたか否かを判定する工程を備える、方法。

適用例１９：適用例１７に記載の方法であって、前記ホワイトニング鍵の値は、前記情報および前記情報に関連づけられたアドレスに依存しない、方法。

適用例２０：適用例１７に記載の方法であって、さらに、前記情報が秘密情報であると検出された場合に、第１の初期化ベクトルを受信する工程と、前記情報が非秘密情報であると検出された場合に、第２の初期化ベクトルを生成する工程と、前記情報が秘密情報であるか非秘密情報であるかに基づいて、前記第１および第２の初期化ベクトルのいずれかを選択する工程と、を備える、方法。

適用例２１：適用例１７に記載の方法であって、さらに、前記受信した情報のメモリ管理データを生成する工程と、前記不揮発性メモリに格納するために、前記ホワイトニング鍵を用いた前記メモリ管理データの暗号化を有効にする工程と、を備える、方法。

適用例２２：メモリインターフェースを用いて不揮発性メモリに格納する情報を準備する方法であって、前記情報は論理アドレスに関連づけられており、前記方法は、前記論理アドレスに基づいて前記情報を暗号化する工程と、前記論理アドレスを前記不揮発性メモリの第１の物理アドレスと対応づけるメモリ管理データを生成する工程と、前記不揮発性メモリの第２の物理アドレスに基づいて前記メモリ管理データを暗号化する工程と、前記第１の物理アドレスに前記暗号化された情報を格納する工程と、前記不揮発性メモリの前記第２の物理アドレスに前記暗号化されたメモリ管理データを格納する工程と、を備える、方法。

適用例２３：適用例２２に記載の方法であって、さらに、前記第１の物理アドレスから前記不揮発性メモリの第３の物理アドレスに前記暗号化された情報を移動させる工程を備え、前記暗号化された情報は、前記移動させる工程の間、暗号化されたままである、方法。

適用例２４：適用例１７または２２に記載の方法であって、前記不揮発性メモリはＮＡＮＤ型フラッシュメモリを含む、方法。

適用例２５：適用例２２に記載の方法であって、前記不揮発性メモリは、複数のページを有するＮＡＮ型フラッシュメモリを含み、前記第１および第２の物理アドレスの各々は、前記複数のページの内の１つに関連づけられる、方法。

【図１】

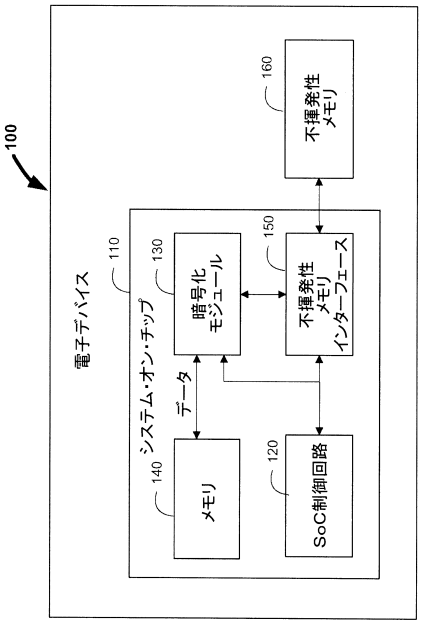

FIG. 1

【図２】

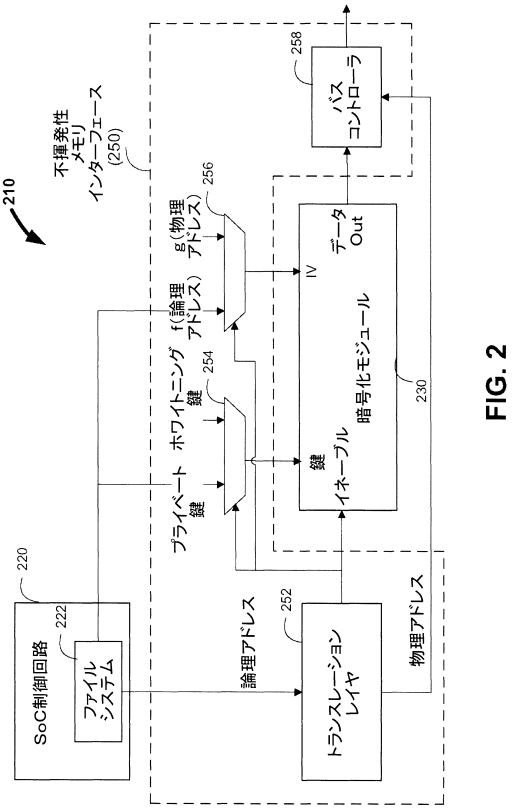

FIG. 2

【図３】

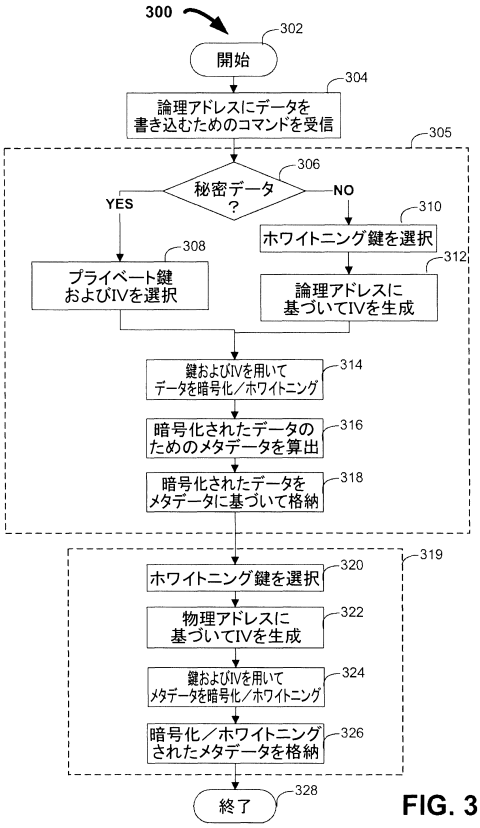

FIG. 3

【図４】

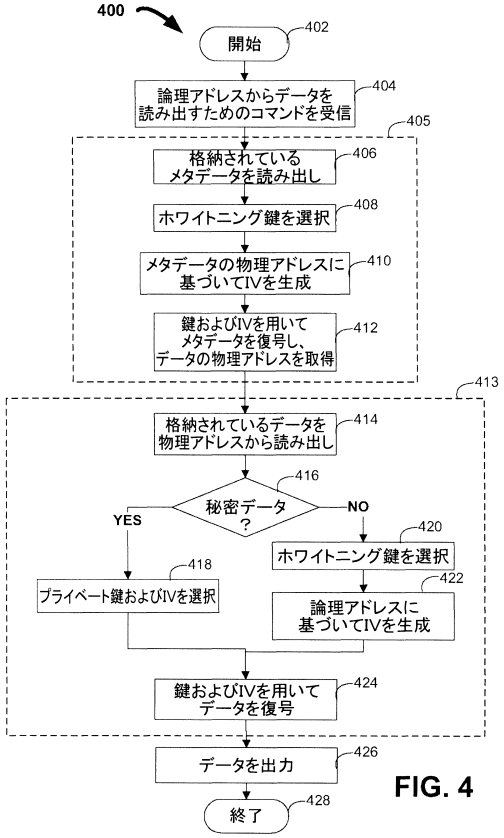

FIG. 4

【図５】

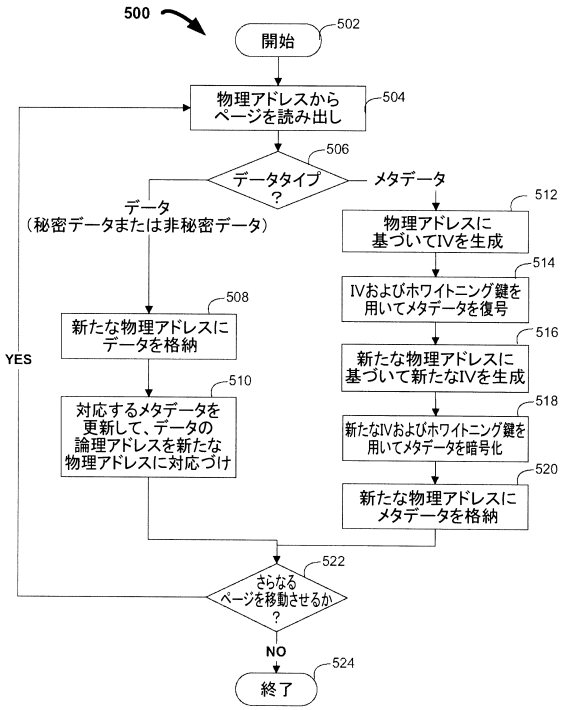
500
開始
502
物理アドレスから
ページを読み出し
504
データタイプ
？
506
メタデータ
データ
（秘密データまたは非秘密データ）
512
物理アドレスに
基づいてIVを生成
514
IVおよびホワイトニング鍵を
用いてメタデータを復号
516
新たな物理アドレスに
基づいて新たなIVを生成
518
新たなIVおよびホワイトニング鍵を
用いてメタデータを暗号化
520
新たな物理アドレスに
メタデータを格納
508
新たな物理アドレスに
データを格納
510
対応するメタデータを
更新して、データの
論理アドレスを新たな
物理アドレスに対応づけ
YES
522
さらなる
ページを移動させるか
？
NO
524
終了

FIG. 5

フロントページの続き

(72)発明者 ケニス・ハーマン
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ, インフィニット・ループ, １
(72)発明者 マシュー・バイオム
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ, インフィニット・ループ, １
(72)発明者 マイケル・ジェイ. ・スミス
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ, インフィニット・ループ, １
(72)発明者 トーマス・エム. ・トエルケス
アメリカ合衆国 カリフォルニア州９５０１４ クパチーノ, インフィニット・ループ, １

審査官 野田 佳邦

(56)参考文献 特開２００３－２４２０３０（ＪＰ, Ａ）
特開２００８－１９８２９９（ＪＰ, Ａ）
国際公開第２００８／１２７４０８（WO, Ａ１）
特開２００８－２０４５２８（ＪＰ, Ａ）
特開２００８－０９０４５１（ＪＰ, Ａ）
特表２０１１－５０８３６３（ＪＰ, Ａ）
特開２０１０－１０８０２９（ＪＰ, Ａ）
特表２０１１－５３０７７７（ＪＰ, Ａ）
特開２００９－１５７８４１（ＪＰ, Ａ）
特開２００９－１５７８３６（ＪＰ, Ａ）
川島 潤 Jun KAWASHIMA, メモリカードのためのセキュアファイルシステムＳＡＳの提案 A Proposal of Secure Filesystem for Memorycard SAS, 電子情報通信学会技術研究報告 Ｖｏｌ．１０５ Ｎｏ．４１ IEICE Technical Report, 日本, 社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers, ２００５年 5月 6日, 第105巻, p.19-24

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ １２／００－１２／０６
Ｇ０６Ｆ １２／１４
Ｇ０６Ｆ １２／１６