【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成25年3月21日(2013.3.21)

【公開番号】特開2010-231778(P2010-231778A)
【公開日】平成22年10月14日(2010.10.14)
【年通号数】公開・登録公報2010-041
【出願番号】特願2010-46014(P2010-46014)
【国際特許分類】
Ｇ０６Ｆ　12/16　(2006.01)
Ｇ０６Ｆ　12/00　(2006.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　12/16　３２０Ａ
Ｇ０６Ｆ　12/00　５３７Ｈ
Ｇ０６Ｆ　12/00　５４２Ａ
Ｇ０６Ｆ　12/14　５４０Ａ

【手続補正書】
【提出日】平成25年2月4日(2013.2.4)
【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】
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。
【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。
【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】
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。
【請求項６】
請求項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暗号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。
【請求項７】
請求項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。
【請求項８】
請求項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。
【請求項９】
請求項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。
【請求項１０】
請求項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。
【請求項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。

【請求項１２】
請求項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。
【請求項１３】
請求項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。
【請求項１４】
請求項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。
【請求項１５】
請求項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。
【請求項１６】
請求項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の物理アドレスを決定し、
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。
【請求項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。
【請求項１８】
請求項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。
【請求項１９】
請求項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。
【請求項２０】
請求項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。
【請求項２１】
請求項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。
【請求項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。
【請求項２３】
請求項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。
【請求項２４】
請求項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。
【請求項２５】
請求項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ＮＡＮＤ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。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００５３
【補正方法】変更
【補正の内容】
【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。