【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７部門第３区分
【発行日】平成20年10月30日(2008.10.30)

【公表番号】特表2008-524969(P2008-524969A)
【公表日】平成20年7月10日(2008.7.10)
【年通号数】公開・登録公報2008-027
【出願番号】特願2007-548469(P2007-548469)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｈ０４Ｌ　9/14　(2006.01)
Ｇ０６Ｆ　21/24　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ｚ
Ｈ０４Ｌ　9/00　６４１
Ｇ０６Ｆ　12/14　５４０Ａ

【手続補正書】
【提出日】平成20年9月10日(2008.9.10)
【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】
暗号化されたデータを保存するメモリシステムにおいて、
不揮発性のフラッシュメモリセルと、
前記セルからの、又は前記セルへのデータストリーム中のデータに対して暗号化処理を実行する回路と、
コントローラであって、暗号化アルゴリズムを用いて、暗号化処理するために、前記回路を設定すると共に前記セルと前記回路を制御し、前記回路が設定された後、前記コントローラの関与なしで、前記データストリーム中のデータが前記回路によって暗号化処理されるようにするコントローラと、
を備えることを特徴とするシステム。
【請求項２】
データがページの前記セルに書き込まれ、または前記セルから読取られ、前記回路が各々１ページ未満のデータユニットに暗号化処理を実行し、前記コントローラが前記回路を設定し、前記回路が設定された後に、前記回路が、前記コントローラの関与なしにデータの複数のページに暗号化処理を実行することを特徴とする請求項１に記載のシステム。
【請求項３】
前記コントローラが前記回路を設定し、前記データストリームが複数のソースの中から選択されたデータソースと、複数の行き先の中から選択された行き先を有することを特徴とする請求項１に記載のシステム。
【請求項４】
前記コントローラが前記回路を設定し、前記データストリーム中のデータが前記セルから生じ、前記コントローラ又はホスト装置に仕向けられることを特徴とする請求項３に記載のシステム。
【請求項５】
前記コントローラが前記回路を設定し、前記データストリーム中のデータが前記セルに

仕向けられ、前記コントローラ又はホスト装置から生じることを特徴とする請求項３に記載のシステム。
【請求項６】
前記コントローラが前記回路を設定し、前記データストリームが前記セルからホスト装置まで、又は前記ホスト装置から前記セルまでであり、前記回路をバイパスすることを特徴とする請求項３に記載のシステム。
【請求項７】
前記コントローラが前記回路を設定し、選択された暗号化アルゴリズムが前記暗号化処理で使用されることを特徴とする請求項１に記載のシステム。
【請求項８】
前記コントローラが前記回路を設定し、前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを複数の連続する段階で暗号化処理することを特徴とする請求項１に記載のシステム。
【請求項９】
前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを、２つ以上の鍵を使用して、複数の連続する段階で暗号化処理することを特徴とする請求項８に記載のシステム。
【請求項１０】
前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを２つ以上の暗号化処理によって、複数の連続する段階で暗号化処理することを特徴とする請求項８に記載のシステム。
【請求項１１】
暗号化されたデータを保存するメモリカードにおいて、
不揮発性のフラッシュメモリセルと、
前記セルからの、又は前記セルへのデータストリーム中のデータに対して暗号化処理を実行する回路と、
コントローラであって、暗号化アルゴリズムを用いて、暗号化処理するために、前記回路を設定すると共に前記セルと前記回路を制御し、前記回路が設定された後、前記コントローラの関与なしで、前記データストリーム中のデータが前記回路によって暗号化処理されるようするコントローラと、
を備え、
前記メモリセル、前記回路および前記コントローラは、カード中にカプセル化されていることを特徴とするカード。
【請求項１２】
データがページで前記セルに書き込まれ、または前記セルから読取られ、前記回路が各々１ページ未満のデータユニットに暗号化処理を実行し、前記コントローラが前記回路を設定し、前記回路が設定された後、前記回路が、前記コントローラの関与なしにデータの複数ページに暗号化処理を実行することを特徴とする請求項１１に記載のカード。
【請求項１３】
前記コントローラが前記回路を設定し、前記データストリームが複数のソースの中から選択されたデータソースと、複数の行き先の中から選択された行き先を有することを特徴とする請求項１１に記載のカード。
【請求項１４】
前記コントローラが前記回路を設定し、前記データストリーム中のデータが前記セルから生じ、前記コントローラ又はホスト装置に仕向けられることを特徴とする請求項１３に記載のカード。
【請求項１５】
前記コントローラが前記回路を設定し、前記データストリーム中のデータが前記セルに仕向けられ、前記コントローラ又はホスト装置から生じることを特徴とする請求項１３に記載のカード。

【請求項１６】
前記コントローラが前記回路を設定し、前記データストリームが前記セルからホスト装置まで、又は前記ホスト装置から前記セルまでであり、前記回路をバイパスすることを特徴とする請求項１３に記載のカード。
【請求項１７】
前記コントローラが前記回路を設定し、選択された暗号化アルゴリズムが暗号化および／または復号で使用されることを特徴とする請求項１１に記載のカード。
【請求項１８】
前記コントローラが前記回路を設定し、前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを複数の連続する段階で暗号化処理することを特徴とする請求項１１に記載のカード。
【請求項１９】
前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを、２つ以上の鍵を使用して、複数の連続する段階で暗号化処理することを特徴とする請求項１８に記載のカード。
【請求項２０】
前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを２つ以上の暗号化処理によって、複数の連続する段階で暗号化処理することを特徴とする請求項１８記載にカード。
【請求項２１】
暗号化されたデータを保存するメモリカードにおいて、
不揮発性のフラッシュメモリセルと、
前記セルからの、又は前記セルへのデータストリーム中のデータに対して暗号化処理を実行する回路と、
データをページで前記セルに書き込ませ、または、前記セルから読み出させるコントローラを備え、
前記回路は、各々１ページ未満のデータユニットに暗号化処理を実行し、
前記コントローラの関与なしで、前記データストリームの１ページ以上が暗号化処理され、複数のソースの中から選択されたデータソースと複数の行き先の中から選択された行き先を用いて、書き込まれ、又は、読取られる、
ことを特徴とするメモリカード。
【請求項２２】
セルおよび暗号化回路を制御するコントローラを有するメモリシステムの不揮発性のフラッシュメモリセルにおけるデータを暗号化および／または復号する方法において、
暗号化アルゴリズムを用いて、前記セルからの、又は前記セルへのデータストリーム中のデータに暗号化処理を実行する回路を設定するためにコントローラを用いるステップと、
前記回路が設定された後に前記コントローラの関与なしで、前記データストリーム中のデータが、前記回路によって暗号化処理されるステップと、
を含むことを特徴とする方法。
【請求項２３】
データがページで前記セルに書き込まれ、または前記セルから読取られ、前記回路が各々１ページ未満のデータユニットに暗号化処理を実行し、前記コントローラを使用する方法は、前記コントローラを用いて前記回路を設定し、前記回路が設定された後、前記回路が、前記コントローラの関与なしにデータの複数のページに暗号化処理することを特徴とする請求項２２に記載の方法。
【請求項２４】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
前記データストリームが複数のソースの中から選択されたデータソースおよび複数の行き先の中から選択された行き先を有することを特徴とする請求項２２に記載の方法。

【請求項２５】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
前記データストリーム中のデータが前記セルから生じ、前記コントローラ又はホスト装置に仕向けられることを特徴とする請求項２４に記載の方法。
【請求項２６】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
前記データストリーム中のデータが前記セルに仕向けられ、前記コントローラ又はホスト装置から生じることを特徴とする請求項２４に記載の方法。
【請求項２７】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
前記データストリームが前記セルからホスト装置まで、又は前記ホスト装置から前記セルまででであって、前記回路をバイパスすることを特徴とする請求項２４に記載の方法。
【請求項２８】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
選択された暗号化アルゴリズムが前記暗号化処理に使用されることを特徴とする請求項２２に記載の方法。
【請求項２９】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを複数の連続する段階で暗号化処理することを特徴とする請求項２２に記載の方法。
【請求項３０】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを、２つ以上の鍵を使用して、複数の連続する段階で暗号化処理することを特徴とする請求項２９に記載の方法。
【請求項３１】
前記コントローラを用いるステップは、前記コントローラを用いて前記回路を設定し、
前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを２つ以上の暗号化処理によって、複数の連続する段階で暗号化処理することを特徴とする請求項２９に記載の方法。
【請求項３２】
セルおよび暗号化回路を制御するコントローラを有するメモリシステムの不揮発性のフラッシュメモリセルにおけるデータを暗号化および／または復号する方法において、
前記コントローラの関与なしで、前記回路を用いて１ページ以上のデータを暗号化処理するステップであって、データがページ単位で書き込まれ、または読取られ、また、前記回路が、各々１ページ未満のデータユニットに暗号化処理をするステップと、
前記データストリームが、前記コントローラの関与なしで、複数のソースの中から選択されたデータソースと、複数の行き先の中から選択された行き先を有するように、前記データストリームを制御するステップと、
を含むことを特徴とする方法。
【請求項３３】
前記暗号化回路を設定することをさらに含み、前記暗号化処理および前記制御するステップが、前記回路の設定によって可能にされることを特徴とする請求項３２に記載の方法。
【請求項３４】
前記回路を設定することで、複数の暗号化アルゴリズム中から１つ以上の暗号化アルゴリズムの選択が可能となり、前記コントローラの関与なしに、前記選択された暗号化アルゴリズムを使用する前記回路によって、前記データストリーム中のデータが暗号化処理されることを特徴とする請求項３３に記載の方法。
【請求項３５】

前記回路が設定され、前記データストリーム中のデータが前記セルから生じ、前記コントローラ又はホスト装置に仕向けられることを特徴とする請求項３３に記載の方法。
【請求項３６】
前記回路が設定され、前記データストリーム中のデータが前記セルに仕向けられ、前記コントローラ又はホスト装置から生じることを特徴とする請求項３３に記載の方法。
【請求項３７】
前記回路が設定され、前記データストリームが前記セルからホスト装置まで、又は前記ホスト装置から前記セルまでであり、前記回路をバイパスすることを特徴とする請求項３３に記載の方法。
【請求項３８】
前記回路が設定され、前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを複数の連続する段階で暗号化処理することを特徴とする請求項３３に記載の方法。
【請求項３９】
前記回路が設定され、前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを、２つ以上の鍵を使用して、複数の連続する段階で暗号化処理することを特徴とする請求項３８に記載の方法。
【請求項４０】
前記回路が設定され、前記設定後に前記コントローラの関与なしで、前記回路が前記データストリーム中のデータを、２つ以上の暗号化処理によって複数の連続する段階で暗号化処理することを特徴とする請求項３８に記載の方法。
【請求項４１】
暗号化されたデータ保存用のメモリシステムにおいて、
不揮発性のフラッシュメモリセルと、
前記セルから又は前記セルへの２つ以上のデータストリーム中のデータに暗号化処理を実行する回路と、
前記セルと前記回路を制御し、異なったデータストリーム中のデータがインターリーブ方式で暗号化処理されるコントローラを備え、
前記セルからのデータをアクセスするための少なくとも１つのセッションは、他のセッションによって割り込まれ、
前記コントローラは前記セッションのセキュリティコンフィギュレーション情報を、前記割り込み前に保存させ、該情報は前記割り込み後に読取ることができることを特徴とするシステム。
【請求項４２】
前記セキュリティコンフィギュレーション情報は、データのソースあるいは行き先に関連する情報、暗号化鍵、暗号化アルゴリズム、および／またはメッセージ認証コードを含むことを特徴とする請求項４１に記載のシステム。
【請求項４３】
前記コントローラは前記セッションの再開時に、前記セッション用に保存された前記セキュリティコンフィギュレーション情報を読取らせることを特徴とする請求項４１に記載のシステム。
【請求項４４】
前記コントローラは、２つ以上のデータストリーム毎に前記セキュリティコンフィギュレーション情報を保存させ、割り込み後に前記情報が読取らせることを特徴とする請求項４１に記載のシステム。
【請求項４５】
前記データストリームからのデータの処理が再開される時に、前記コントローラは、２つ以上のデータストリーム毎に保存された前記セキュリティコンフィギュレーション情報を読取らせることを特徴とする請求項４４に記載のシステム。
【請求項４６】

前記コントローラは、前記割り込み以前に保存された、メッセージ認証コードを含む前記セキュリティコンフィギュレーション情報を読取り、前記割り込まれたセッションが再開されるときに、前記読取られたメッセージ認証コードから更新したメッセージ認証コードを導出することを特徴とする請求項４１に記載のシステム。
【請求項４７】
不揮発性のフラッシュメモリセルと暗号化回路を含む、暗号化されたデータ保存用のメモリシステムにおけるデータを処理する方法において、
前記セルからの、又は前記セルへのデータストリーム中のデータに暗号化処理を行うために前記回路を用いるステップと、
インターリーブ方式で、異なったデータストリーム中のデータを前記回路に暗号化処理させるステップであって、前記セルへの、または前記セルからのデータを処理する、少なくとも１セッションが、他のセッションに割り込まれ、前記少なくとも前記１セッションのセキュリティコンフィギュレーション情報が、前記割り込み前に保存され、前記割り込み後に読取ることができるステップと、
を含むことを特徴とする方法。
【請求項４８】
前記セキュリティコンフィギュレーション情報は、データのソースあるいは行き先に関連する情報、暗号化鍵、暗号化アルゴリズム、および／またはメッセージ認証コードを含むことを特徴とする請求項４７に記載の方法。
【請求項４９】
前記暗号化処理させるステップが、前記異なったデータストリーム毎に前記セキュリティコンフィギュレーション情報を保存させ、前記割り込み後、前記情報が読取ることができることを特徴とする請求項４７に記載の方法。
【請求項５０】
前記暗号化処理させるステップは、前記データストリームからのデータ処理が再開される時に、前記異なったデータストリーム毎に保存された前記セキュリティコンフィギュレーション情報を読取らせるようにすることを特徴とする請求項４７に記載の方法。
【請求項５１】
前記割り込み以前に保存された、メッセージ認証コードを含む前記セキュリティコンフィギュレーション情報を更に読取るステップを更に有し、前記割り込まれたセッションが再開されるときに、前記読取られたメッセージ認証コードから更新したメッセージ認証コードを導出することを特徴とする請求項４７に記載の方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【発明の詳細な説明】
【発明の名称】インーストリームデータ暗号化/復号の機能を有するメモリシステム
【技術分野】
【０００１】
本発明は一般にメモリシステムに関し、特にインーストリームデータ暗号化/復号機能を有するメモリシステムに関する。
【背景技術】
【０００２】
モバイル機器市場は、より多くのデータ交換を発生させることにより平均収入の増加を図るよう、コンテンツストレージを備える方向に進んでいる。これは、モバイル機器に保存されている時に、そのコンテンツが保護されていなければならないことを意味する。
【０００３】
数年来、ポータブル記憶装置は商業用途に使用されており、データをコンピューティン

グデバイスから他のコンピューティングデバイスへ持ち運んだり、あるいはバックアップデータを保存するために用いられている。ポータブルハードディスクドライブ、ポータブルフラッシュメモリディスクおよびフラッシュメモリカードのようなもっと高機能なポータブル記憶装置は、ストレージ管理の制御用マイクロプロセッサを含んでいる。

【０００４】

ポータブル記憶装置に保存されたコンテンツを保護するために、保存されているデータは通常、暗号化され、許可されたユーザだけがデータを復号することが許される。

【０００５】

旧来の暗号化の機能を有するポータブル記憶装置では、ストレージ管理用のマイクロプロセッサも暗号化と復号の処理に深く関与している。そのようなシステムは、例えば米国特許６，４５７，１２６号に記載されている。この場合では、記憶装置の処理能力および機能はひどく影響を受ける可能性がある。従って、前記の問題を大幅に軽減するローカル記憶装置を提供することは望ましい。

【特許文献１】米国特許６，４５７，１２６号

【発明の開示】

【発明が解決しようとする課題】

【０００６】

この発明の一側面は、データストリーム中のデータが不揮発性メモリセルに送信され、又は該不揮発性メモリセルから取出しされる時に、あらゆるコントローラあるいはマイクロプロセッサとも密接な関与せず、データストリーム中のデータを回路によって暗号化処理する場合に、メモリシステムの処理能力が改善できる認識に基づくものである。ある実施例では、前記コントローラは暗号化処理に使用されるパラメーターを規定することだけに関与し、処理には関与しない。この実施例の実行では、パラメーターは、コンフィギュレーションレジスタによって設定される。

【０００７】

好ましくは、メモリセルはフラッシュメモリセルを有する。さらに、メモリセル、データ暗号化および／または復号に使用する回路、セルおよび回路を制御するコントローラは、メモリカードかメモリスティックのような物体の中に取付けされ、カプセル化されることが好ましい。

【０００８】

データは、ページで前記メモリセルに書き込まれ、またはそれから読出されることができる。暗号化および復号に使用される従来の暗号化アルゴリズムの多くは、通常、ページより小さなデータの単位で作動する。したがって、本発明の他の側面は、前記暗号化回路が、読取りまたは書き込み中の前記データストリーム中の１ページ以上のデータを暗号化処理することと、すべて前記コントローラの関与なしで、前記データストリームが複数のソースの中から選択されたデータソースと複数の行き先（ｄｅｓｔｉｎａｔｉｏｎ）の中から選択された行き先を持つように、制御される認識に基づくものである。

【０００９】

発明の他の側面によれば、前記暗号化回路は、コントローラあるいはマイクロプロセッサの関与なしで、暗号化および／または復号に対する複数のアルゴリズム中で１つ以上の暗号化アルゴリズムの選択ができるように設定できる。設定後、前記コントローラの関与なしで、前記回路は、複数の連続する段階で前記データストリーム中のデータを暗号化処理するようにも、前記回路を設定できる。設定後前記コントローラの関与なしで、複数の連続する段階で、前記暗号化処理は２つ以上の鍵を使用し、２つ以上のタイプの暗号化処理を使用することができる。

【００１０】

あるアプリケーションでは、前記メモリシステムは、２つ以上の前記データストリームを取り扱うことが望ましい。この場合では、異なったデータストリーム中のデータがインターリーブ方式で暗号化処理されるように、前記コントローラは前記メモリセルと前記回路を制御する。好ましくは、前記データストリームの処理がインタリービングの間に割り

込まれる場合に、各データストリームの暗号化処理用の様々なパラメーターが保存されるので、該データストリームの処理が再開される時、暗号化処理を継続するようパラメーターが回復できる。この特徴の一実施例では、暗号化処理用の様々なパラメーターをセットするために、セキュリティコンフィギュレーションレコードを書き込み操作の最初に作成し、セッションの終了にこれらのパラメーターを保存する。その後、読み込み操作の開始時にこのレコードをメモリから取り戻し、操作の終了に廃棄する。他のデータストリームの処理をさせるために、前記データストリームが一時的に割り込まれる場合、そのようなレコードも保存され、元のデータストリームの処理が再開される時に取り戻される。

【００１１】

本発明の上記の様相は、個々に、あるいはそれの任意の組み合せで使用できる。

【発明を実施するための最良の形態】

【００１２】

図1のブロック図を用いて、本発明の様々な部分が実行できる実例的なメモリシステムを説明する。図1に示すように、メモリシステム１０は、中央処理装置（ＣＰＵ）１２と、バッファ管理ユニット（ＢＭＵ）１４と、ホストインタフェースモジュール（ＨＩＭ）１６と、フラッシュインタフェースモジュール（ＦＩＭ）１８と、フラッシュメモリ２０と、ペリフェラルアクセスモジュール（ＰＡＭ）２２を有する。メモリシステム１０は、ホストインタフェースバス２６およびポート２６ａを介してホスト装置２４と通信する。NANDタイプでもよいフラッシュメモリ２０はホスト装置２４用のデータ記憶装置を提供する。また、ＣＰＵ１２用のソフトウェアコードはフラッシュメモリ２０に保存されてもよい。ＦＩＭ１８は、フラッシュインタフェースバス２８とポート２８ａを介してフラッシュメモリ２０に接続される。ＨＩＭ１６は、例えばディジタルカメラと、パソコンと、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）と、ディジタルメディアプレーヤーと、ＭＰ－３プレーヤーと携帯電話、あるいは他のディジタル装置等のホストシステムに接続するのに適する。ペリフェラルアクセスモジュール２２は、ＣＰＵ１２との通信用の例えばFIMと、HIMとBMU等の適切なコントローラモジュールを選択する。一つの実施例において、点線に囲まれた枠内のシステム10の中のすべてのコンポーネントを、例えばメモリカードあるいはメモリスティック１０’の単一のユニットに封入することができ、好ましくは、カードあるいはスティック中にカプセル化できる。

【００１３】

バッファ管理ユニット１４は、ホストダイレクトメモリアクセス（ＨＤＭＡ）３２と、フラッシュダイレクトメモリアクセス（ＦＤＭＡ）コントローラ３４と、アービタ３６と、バッファランダムアクセスメモリ（ＢＲＡＭ）３８と、暗号化エンジン４０を有する。アービタ３６は共有バスアービタであるので、いつでも、ただ一つのマスタあるいはイニシエータ（ＨＤＭＡ３２、ＦＤＭＡ３４あるいはＣＰＵ１２でもよい）だけがアクティブ可能になり、スレーブまたはターゲットはＢＲＡＭ　３８である。アービタは、適切なイニシエータの要求をＢＲＡＭ３８に向ける。ＨＤＭＡ３２とＦＤＭＡ３４は、ＨＩＭ１６、ＦＩＭ１８、およびＢＲＡＭ３８と、あるいはＣＰＵランダムアクセスメモリ（ＣＰＵ　ＲＡＭ）１２ａとの間に伝送されたデータに関与する。ＨＤＭＡ３２およびＦＤＭＡ３４の作動は従来の通りで、ここに詳述する必要はない。ＢＲＡＭ３８は、ホスト装置２４、フラッシュメモリ２０およびＣＰＵ　ＲＡＭ　１２ａの間で伝送されるデータを一時的に保持するものである。ＨＤＭＡ３２とＦＤＭＡ３４は、ＨＩＭ１６／ＦＩＭ１８とＢＲＡＭ３８あるいはＣＰＵ　ＲＡＭ　１２ａとの間にデータ伝送し、セクター伝送完了を指示するものである。

【００１４】

まず最初に、フラッシュメモリ２０からのデータをホスト装置２４によって読取る場合、メモリ２０中の暗号化されたデータは、バス２８、ＦＩＭ１８、ＦＤＭＡ３４、暗号化されたデータを復号する暗号化エンジン（Ｃｒｙｐｔｏ－Ｅｎｇｉｎｅ）４０によってフェッチされ、ＢＲＡＭ３８に保存される。その後、復号されたデータは、ＢＲＡＭ３８からＨＤＭＡ３２、ＨＩＭ１６、バス２６を介してホスト装置２４へ送信される。メモリ２

０に保存されたデータが復号される鍵及び／またはアルゴリズムと異なる鍵及び／またはアルゴリズムによってホスト装置２４に伝送されるデータを再暗号化するように、ＢＲＡＭ３８からフェッチされたデータは、ＨＤＭＡ３２に伝送される前に、暗号化エンジン（Ｃｒｙｐｔｏ－Ｅｎｇｉｎｅ）４０によって再暗号化できる。さらに代わりの実施例では、データが不正アクセスに対して脆弱となりがちな、ＢＲＡＭ３８に復号されたデータを保存する上述の処理よりも、メモリ２０からのデータが、ＢＲＡＭ３８に伝送される前に復号されて、暗号化エンジン４０によって再暗号化されるのが好ましい。その後、前述したように、ＢＲＡＭ３８中の暗号化されたデータは、ホスト装置２４へ伝送される。これで読取り処理の際のデータストリームを説明した。

【００１５】

データがホスト装置２４によってメモリ２０に書き込まれる場合は、データストリームの方向が逆にされる。例えば、暗号化されていないデータをホスト装置を利用して、バス２６、ＨＩＭ１６、ＨＤＭＡ３２によって暗号化エンジン４０へ伝送する場合、これらのデータは、ＢＲＡＭ３８に保存される前にエンジン４０によって暗号化されてもよい。その代わりに、暗号化されていないデータをＢＲＡＭ３８に保存してもよい。その後、このデータは、ＦＤＭＡ３４に伝送される前に、メモリ２０へ伝送される途中で暗号化される。書き込まれたデータが多段の暗号化処理を経過する場合、処理済みのデータをＢＲＡＭ３８に保存する前に、エンジン４０が前記の処理を完了するのが好ましい。

【００１６】

本発明の１つの側面は、ホスト装置２４とメモリ２０との間で伝送されるデータストリーム中のデータの前述した暗号化処理を、ＣＰＵ１２の関与が最小となるように実行できれば、装置１０の処理能力とそれによる性能を非常に改善することができるという認識に基づいているものである。これは以下説明するように図1に示す。

【００１７】

上記の処理では、２つの異なったデータソースおよび行き先があるデータストリームを説明した。読取り処理では、データソースはメモリ２０であり、行き先はホスト装置２４である。書き込み処理では、データソースはホスト装置２４であり、行き先はメモリ２０である。さらに、データソース（あるいは行き先）は、対応する行き先（あるいはデータソース）がメモリ２０であるＣＰＵ１２でもよい。さらに、他のオペレーションでは、バルク暗号化およびハッシュオペレーションに対して、データストリームはＢＭＵ１４からＣＰＵ１２までででもよい。ソースの中のデータと出力データの行き先及び適用されうる対応する暗号化処理の様々な組み合わせを下記の表に述べる。

【表１】

オペレーション	エンジン	ソース中のデータ	データの行き先	内容
FDMAのCPUへの書き込み	AES/DES/HASH	FDMA CPU BUS	CPU	当該データフローによって、安全な記憶装置からCPUにロードされたデータの暗号化オペレーション(復号)を可能にする。
FDMAのCPUからの読み取り	AES/DES/HASH	CPU	FDMA	当該データフローによって、CPUを利用して安全な記憶装置に保存されたデータの暗号化オペレーション(暗号化)を可能にする。
FDMAのBRAMへの書き込み	AES/DES/HASH	FDMA BRAM BUS	BRAM	当該データフローによって、FIMからBRAMまでのデータストリーム伝送の暗号化オペレーションを可能にする。
FDMAのBRAMからの読み取り	AES/DES/HASH	BRAM	FDMA	当該データフローによって、BRAMからFIMまでのデータストリーム伝送の暗号化オペレーションを可能にする。
PAMのアクセス	AES/DES/HASH/PKI	PAM	PAM	当該データフローによってCPUがバルク暗号化及びハッシュオペレーション用のハードウェアコアをアクセスすることを可能にする。
BYPASS	n/a	書き込みなし	書き込みなし	当該データフローによって、FDMAが、データストリーム上での暗号化処理なしに、CPUあるいはBRAMをアクセスすることを可能にする。

【００１８】

上記の表に示したように、１つの追加されたオペレート可能なモードは、バイパスモードである。バイパスモードは、暗号化エンジン４０が存在せずＨＤＭＡとＦＭＤＡがアービタ３６を介して該バイパス路に沿ってＢＲＡＭ３８に直接接続されているように、バイパス路（図1に示せず）に沿って、データストリームに暗号処理せずに、ＦＤＭＡ３４がＣＰＵ１２あるいはＢＲＡＭ３８にアクセスすることができる。本発明の一実施例によれば、例えばデータソースとデータ行き先等のプロセッシング、例えば適用される（あるいは、バイパスモード）暗号化アルゴリズム等の暗号化パラメータは、図1の暗号化エンジン４０の機能的ブロックのうち一部のブロック図である図２のコンフィギュレーションレジスタ１０２をセットすることで、複数のデータソースと、複数の行き先および複数のアルゴリズムからＣＰＵ１２を用いてあらかじめ選択できる。

【００１９】

図２は暗号化エンジン４０のブロック図で、その構成要素の一部をより詳細に示す。図２に示すように、暗号化エンジン４０は、暗号化ブロック５０とコンフィギュレーションレジスタ５２とを有する。コンフィギュレーションレジスタ５２は、選択されたデータソースと、選択されたデータ行き先、および使用される暗号化アルゴリズムあるいはバイパスモードとに関するセキュリティコンフィギュレーション情報あるいはセキュリティコンフィギュレーションレコードを、上記の表と使用すべき鍵（バイパスモードを除いて）に従い、データが暗号化か、復号か、あるいはハッシュされることになっているか（以上こ

れらは「暗号化処理される」という表現に含まれる）、あるいは暗号化処理されないかどうかによって保存するものである。セキュリティコンフィギュレーション情報あるいはレコードは、ＣＰＵ１２によってレジスタ５２に書き込まれてもよい。この情報をレジスタ５２に保存した後、エンジン４０は、ＣＰＵ１２の関与なしで暗号化処理を実施することができる。多くの通常の暗号化アルゴリズムは、データを、１２８ビットを１単位として処理する。これは、フラッシュメモリのような記憶装置に一度に書き込まれるかまたはそれから読取られるデータのページのサイズより小さくすることができる。各ページは、通常１つ以上のセクターのデータを保存するが、該セクターのサイズは、ホストシステムによって規定されている。１例は磁気ディスクドライブで確立された規格によるユーザデータの５１２バイトのセクターで、ユーザデータおよび／またはそれが保存されているブロックに関するオーバーヘッド情報の若干のバイトがプラスされる。

【００２０】

ＣＰＵ１２がエンジン４０による暗号化処理に関与する必要がないように、また、データの全ページがエンジン４０によって一度に１ページより小さな単位で暗号化処理されるように、ロジック回路（図示されていない）をブロック４０で使用することができる。一実施例では、暗号化エンジン４０はハードウェア回路である。

【００２１】

図２に示すように、ブロック５４、５６および58は、暗号化ブロック５０によって実施されるようＣＰＵが選択できる３つの異なる暗号化アルゴリズム（それぞれＨａｓｈ、ＤＥＳ及びＡＥＳ）を表わす。これらのアルゴリズムと異なる暗号化アルゴリズムも使用できるし、又、本発明の範囲内にある。暗号化ブロック５０で処理されるデータと、ホスト装置２４あるいはメモリ２０、或いはＣＰＵ１２から発生するデータは、先ず入力バッファ６２に保存されて、レジスタ５２で特定された暗号化アルゴリズムにより暗号化ブロック５０で暗号化処理される。そして、暗号化処理されたデータは、レジスタ５２中の行き先情報により、行き先へ伝送される前に、出力バッファ６４に保存される。図２はさらに、メモリ２０に書き込まされ、又、それから読取られるデータを暗号化処理しない、入力バッファ62から出力バッファ６４までのバイパス路７２を含み、これは表のモードのうち１つであり、上述した１つものである。

【００２２】

コンフィギュレーションレジスタ５２はさらに、暗号化処理中で使用される鍵を保存できる。一実施例では、この鍵は、ＣＰＵ１２（例えば、メモリ２０等から）によって読出されて、暗号化ブロック５０による暗号化又は復号の前にレジスタ５２に保存される。上述した処理は、ＣＰＵ１２がレジスタ５２に適切な情報を書き込んだ後、ＣＰＵ１２の関与なしでブロック４０中で実施される。図２を簡単化するために、ブロック４０中のアルゴリズム、データソースおよび行き先を選択するためにレジスタ５２中の情報を使用し、唯一の鍵と選択されたアルゴリズムを暗号化処理に使用するロジック回路は省略されている。処理されたデータが出力バッファ６４へ伝送される前に、入力バッファ６２中のデータを処理するために、暗号化ブロック５０を２度以上使用することが可能である。例えば、データソースからのデータを先ず復号し、データをバッファ６４に伝送する前に、異なる鍵および／または異なるアルゴリズムを使用して、復号されたデータを暗号化するのが望ましい。データの暗号化または復号に加えて、データのインテグリティを保証する目的では、データの要約あるいはハッシュ値を得るようにハッシングアルゴリズムをデータに適用することは有用である。これらすべての状況では、復号するためにある鍵を使用した後、暗号化するために異なった鍵を使用するか、データを暗号化するか復号するかだけでなく、要約を得るように、暗号化ブロック５０でデータを２度処理することが望ましい。言うまでもなく、データは更に、該データが復号され、ハッシングされ、暗号化される場合、暗号化ブロック５０で２回以上処理できる。これらのオペレーションがシーケンシャル段階（多段処理）で連続的に発生する。言いかえれば、多段（即ち、２段階以上）の処理では、暗号化ブロック５０でより多く処理するよう暗号化ブロック５０によって既に出力バッファ６４で処理されたデータを、フィードバックパス６６を介して、入力バッファ

６２へ伝送することにより、データを２度以上、暗号化ブロック５０を通して伝送してもよい。２段階以上を考慮する場合、データは追加処理のために、更に追加の回数でフィードバックすることができる。処理の各段階では、異なったアルゴリズムおよび／または鍵を使用してもよい。

【００２３】

多段の処理が望まれる場合、ＣＰＵ１２が、データを暗号化処理する回数および多段の処理の各段階で使用される鍵および／またはアルゴリズムを指定するために、セキュリティコンフィギュレーション情報あるいはレコードをレジスタ５２に入力するために使用されてもよい。この情報がレジスタ５２に書き込まれた後、ＣＰＵ１２は多段の処理に全く関与する必要がなくなる。

【００２４】

図1のメモリシステム１０はフラッシュメモリを有しているが、このシステムは例えば磁気ディスク、光ディスクＣＤｓ等の他のタイプの不揮発性メモリ、他のすべてのタイプの書き換え可能な不揮発性メモリシステムをさらに含んでもよく、上述した様々な利点は、これらの選択できる実施例に同様に適用できる。選択できる実施例では、このメモリは更に、メモリシステムの残りのコンポーネントと共に、同じ物体（例えば、メモリカードやメモリステック等）にカプセル化することが好ましい。

【００２５】

オペレーティングシステム１０の読取り処理を図３のフローチャートに示す。ＣＰＵ１２は、ホスト装置２４から読取りコマンドを受け取った後、読取り操作を始める（楕円１５０）。その後、ＣＰＵ１２は、レジスタ５２に適切なセキュリティコンフィギュレーション情報あるいはレコードを書き込むことにより、暗号化エンジン４０を設定し、さらに読取り操作用にＢＭＵ１４を設定し、オペレーション用（ブロック１５２、１５４）にＢＲＡＭ３８中での例えばメモリスペースの割り付け等の他のパラメーターを設定する。ＣＰＵ１２はさらに、データが読まれるメモリ２０中の区域を指定するなど、ＦＩＭ１８を設定する（ブロック１５６）。その後、暗号化処理を含む上記処理がＣＰＵ（エラー訂正を除いて）の関与なしで実行されるように、ＨＤＭＡエンジン３２およびＦＤＭＡエンジン３４を開始する。ブロック１５８を参照して、ＣＰＵは、割り込みを受信すると、それがＦＩＭの割り込みかどうかチェックする（菱形１６０）。ＣＰＵはＦＩＭ割り込みが受信された場合、割り込みがデータストリーム中に一つ以上のエラーがあることを示す割り込みであるかどうかをチェックする（１６２）。エラーがあることが示される場合、ＢＲＡＭ３８中のエラーを修正する為に進み（ブロック１６４）、データが次に読まれるメモリ２０中の区域を変更するよう、ＦＩＭ１８の設定に戻る（ブロック１５６）。ＦＩＭ割り込みがデータストリーム中のエラーを示さなかった場合、ＦＩＭがオペレーションを完了し、又ＣＰＵがＦＩＭの再設定のためにブロック１５６に戻ることを表す。ＣＰＵに検知された割り込みがＦＩＭ割り込みでない場合、ＣＰＵはデータ割り込みの終了かどうかをチェックする（菱形１６６）。そうであれば、読取り操作は終了する（楕円１６８）。そうでなければ、この割り込みは、データの暗号化処理と無関係であり（即ち、クロック割り込み）、又、ＣＰＵは当該割り込みを処理し（図示されていない）、割り込みをチェックするために菱形１６０に戻る。

【００２６】

書き込み操作には図３をわずか修正するだけでよい。メモリ２０に書き込むデータにＥＣＣエラーの取り扱いがないので、書き込み操作でＣＰＵ１２は菱形１６２及びブロック１６４中の処理を省くことができる。ＣＰＵ１２が、書き込み操作中にＦＩＭ割り込みを受信する場合、これは、ＦＩＭがそのオペレーションの完了したことを表し、ＣＰＵもＦＩＭを再設定するためにブロック１５６に戻る。この違いを除けば、書き込み操作は実質的に読取り操作に似ている。したがって、暗号化エンジン４０、ＢＭＵ１４およびＦＩＭ１８を一度設定すると、システム１０は、ＣＰＵ１２の関与なしで、たとえ暗号化エンジン４０がページよりはるかに小さな単位でデータを処理することがあっても、データをすべて暗号化処理し（バイパス・モード以外）、そのセッションのページのすべての書き込

みあるいは読取りを完了することができる。
【００２７】
《インターリービングデータストリーム》
複数のホストアプリケーションが、複数のデータストリームを処理しながら同時に、メモリ２０にアクセスできることが望ましい。これが意味することは、あるデータストリームの暗号化処理は、メモリシステム１０が他のデータストリームを処理するために、割込んだ際に、完了していなかったかもしれないことである。異なったデータストリームの暗号化処理は、通常異なったパラメーター（例えば、異なった鍵とアルゴリズム、および異なったデータソースと行き先）を用いる。これらのパラメーターは、データストリームの対応するセキュリティコンフィギュレーションレコードに備えられている。特定のデータストリームの割り込まれた処理がその後再開される場合に、その対応するセキュリティコンフィギュレーションレコードが失われないことを保証するために、そのレコードは、ＣＰＵ　ＲＡＭ　１２ａに保存するのが好ましい。前に割り込まれたデータストリームの処理を再開する場合、ＣＰＵ１２は、そのデータストリーム用の保存されたセキュリティコンフィギュレーション記録を読取り、保存されている対応するセキュリティコンフィギュレーションレコードに基づいて、正確なパラメーターを用いて、そのデータストリームの再開された暗号化処理を行うことができる。
【００２８】
図４は、複数のデータストリームの処理およびセキュリティコンフィギュレーションレコードの利用の図１および図２のシステムの操作を説明するフローチャートである。ＣＰＵは、ホストコマンドが受信されたかをチェックする（ブロック２０２と菱形２０４）。ホストコマンドが受信されていた時、例えば最初のデータストリームを暗号化処理する場合、ＣＰＵは、コマンドが装置２４で実行する最初のアプリケーション等のスタートセッションコマンドかどうかについてチェックする（菱形２０６）。そうである場合、ＣＰＵは書き込みセッションが要求されたかどうかチェックする（菱形２０８）。若し書き込みセッションが要求されていた場合、ＣＰＵはホスト装置からの情報によってセキュリティコンフィギュレーションレコード（例えば選択されたデータソース、選択されたデータ行き先、上記の表テーブルと使用されるべき鍵によって用いられる暗号化アルゴリズム、および、データが暗号化、復号又はハッシュされるべきかどうか）を作成し（ブロック２１０）、第１データストリーム用の最初のセッションを始める。ＣＰＵ１２は、これらのセキュリティコンフィギュレーション情報あるいはレコードをＣＰＵ　ＲＡＭ　１２ａに保存する。もし要求されたセッションが読取りセッションである場合、ＣＰＵは、読取られるデータ用のセキュリティコンフィギュレーションレコードをメモリ２０から読取り（ブロック２４０）、それをＣＰＵ　ＲＡＭ　１２ａに保存する。その後、ＣＰＵは戻り、さらなるホストコマンドを待つ（２０２）。
【００２９】
ＣＰＵは、別のホストコマンドを受信すると、スタートセッションコマンドであるかを再びチェックする（菱形２０６）。そうである場合、ブロック２１０あるいはブロック２４０に進み、第２のセッションを始めることができる。これは、第２のデータストリームの暗号化処理を要求するホスト装置２４上で作動する、異なった第２のアプリケーション用の新しい第２のセッション等である。上記の第２のデータストリーム用のセキュリティコンフィギュレーション情報あるいはレコードは、ＣＰＵ　ＲＡＭ　１２ａに再び保存されるが、これは書き込みと読取りの両セッションがある場合である（ブロック２１０、２４０）。追加のセッションは同じ方法で追加のデータストリームのために作成できる。ＣＰＵはブロック２０２に戻り、ホストコマンドがスタートセッションコマンドであるかを確かめるために次のホストコマンドをチェックする（菱形２０６）。このようにして、ＣＰＵ１２が菱形２０６中のスタートセッションコマンドでないホストコマンドを検知するまで、前述したように追加セッションが作成される。
【００３０】
この場合には、ＣＰＵ１２は、ホストコマンドがセッション終了のコマンドであるかを

確かめるべく次のホストコマンドをチェックする（菱形２２２）。そうでない場合、ＣＰＵは、それがデータコマンドであるかをチェックする（菱形２２４）。それがデータコマンドであると仮定すれば、ＣＰＵは、どのデータストリームを処理するかを判断し、前記のデータストリームのセキュリティコンフィギュレーションレコードにより暗号化エンジン４０を設定し（レジスタ５２に書き込むことで）、暗号化エンジン４０は、例えば図３の処理などにより、上述した方式で読取りあるいは書き込み操作を実行する（或いは暗号化エンジン４０はバイパスモードでバイパスされる）（ブロック２２６）。

【００３１】

読取りあるいは書き込み処理に割り込みがない場合、セッションの間に処理されるすべてのページが処理されたことを表すセッション終了コマンドをＣＰＵが受信するまでに、処理は継続する（ブロック２２２）。しかしながら、割り込みがある場合、ＣＰＵは、システム１０が現在処理しているデータストリームとは異なるデータストリームからのデータを処理するホストデータコマンドを受信する。この場合、暗号化エンジン４０は、前記の異なるデータストリームを処理するよう再設定される必要がある。その後、ＣＰＵは、ＣＰＵ　ＲＡＭ　１２ａから前記の異なるデータストリーム用のセキュリティコンフィギュレーションレコードを読取り、そして、暗号化エンジン４０を再設定し（レジスタ５２に読取られたレコードを書き込むことによって）、その結果、エンジン４０が前記の異なったデータストリームを正確に処理する。

【００３２】

セッション終了コマンドが書き込みセッションで受け取られた場合（２２２ブロック）、ＣＰＵは、書き込まれたデータと共にセキュリティコンフィギュレーションレコードをメモリ２０に保存し、前記のレコードは、それに続く読取り操作で読取られ得る（菱形２２８およびブロック２３０）。読取り操作では、ＲＡＭ１２ａに保存されたセキュリティコンフィギュレーションレコードが廃棄されるが、メモリ２０に保存されたレコードは、将来起こり得る読取り操作のために保持される（ブロック２４２）。

【００３３】

あるアプリケーションにおいては、無許可な操作（ｔａｍｐｅｒｉｎｇ）に対してメモリ２０中のデータのインテグリティを維持することは重要であろう。メモリ２０に保存されているデータが変更、あるいは、破損されないことを保証するために、前記のデータのハッシュ値またはダイジェストを前記のデータから導出することが望ましく、前記のデータのハッシュ値またはダイジェストは前記のデータと共に保存されている。データを読取られると、ハッシュ値またはダイジェストも同様に読取られ、読取られたダイジェストあるいはハッシュ値は、前記の読取られたデータから計算されたダイジェストあるいはハッシュ値と比較され得る。もし、それらの間に差異があれば、メモリ２０のデータが変更されたか、破損されたのかもしない。

【００３４】

共通のハッシュ関数は連鎖ブロック暗号（ｃｈａｉｎｅｄ　ｂｌｏｃｋ　ｃｉｐｈｅｒ）（ＣＢＣ）であって、メッセージ認証コード（ＭＡＣ）は、書き込み中または読取り中のデータのブロックから時間系列に従って導き出される。共通のCBC関数は以下に通り。

《暗号化》

入力：　ｍ－ビット鍵ｋ；ｌ－ビットⅣ；ｌ－ビット　プレーンテキストブロック$p_1, \cdots, p_r$

出力：　$1 \leqq i \leqq r$のとき$c_0 \leftarrow$Ⅳおよび$c_i \leftarrow e_k(c_{i-1} \leftarrow \oplus p_i)$であるような$c_0, \cdots, c_r$

《復号》

入力：　ｍ－ビット鍵ｋ；ｌ－ビットⅣ；ｌ－ビット　暗号テキストのブロック$c_1, \cdots, c_r$

出力：　$1 \leqq i \leqq r$のとき$p_0 \leftarrow$Ⅳおよび$p_i \leftarrow c_{i-1} \oplus e_k^{-1}(c_i)$であるような$p_0, \cdots, p_r$

【００３５】

上記の値$c_0, \cdots, c_r$は、データストリーム$p_1, \cdots, p_r$のメッセージ認証コード（ＭＡＣ）である。ＩＶはイニシエーション（開始）ベクトルであり、ｋは鍵で

ある。したがって、データp_1，・・・，p_rブロックをメモリ２０に書き込みたい場合、上記のＣＢＣ関数のようなハッシュ関数を使用して、ＭＡＣ値（例えばc_0，・・・，c_r）はシステム10における暗号化エンジン４０によって前記データブロックから計算され、ＭＡＣ値、IV、鍵ｋ、および上記の他のパラメータを含む関連セキュリティコンフィギュレーションレコードは、データ自体がメモリ２０に書き込まれると共に、メモリ２０に書き込まれる。上記の式で、e_k（ｘ）は、ｘが鍵ｋによって暗号化される処理を表し、e_k^{-1}（ｘ）は、ｘが鍵ｋを使用して復号されることを表す。

【００３６】

その後、データブロックp_1，・・・，p_rをメモリ２０か読取られるときに、関連するセキュリティコンフィギュレーションレコードも同様に読取られ、暗号化エンジン４０は、IV、セキュリティコンフィギュレーションレコード中の鍵ｋ、および読取られたデータから一組のＭＡＣ値を計算し、該一組の値をメモリ２０から読取った一組のＭＡＣ値と比較する。これは2組のＭＡＣ値の間に差がある場合、読取られたデータは変更、或いは破損されていたのかもしれない。例えば上記のＣＢＣ関数等のハッシュ関数については、シーケンス中の第１番目の値を除いて、各々ＭＡＣ値は前のＭＡＣから導びかれる。これは、ＭＡＣ値の組がこの場合に、時間の順に連続して導びかれることを表す。

【００３７】

ホスト装置２４中の複数のアプリケーションが、メモリ２０に並行してアクセスできることが望ましく、その結果、ユーザーは他のアプリケーションを使用してメモリ２０にアクセスする前に、当該メモリ２０の使用中のあるアプリケーションが完了することを待つ必要がない。これは、例えば、読取り処理が割り込まれた時に、データp_1，・・・，p_rのすべてのブロックがすでに読取られたわけではないことを表すので、前記のメモリシステム（例えば図１および図２に示すシステム１０）を装置２４で実行している他の異なったアプリケーションに使用できる。しかし、この場合では、全体のデータストリームが読取られる前、且つすべてのＭＡＣ値が計算される前に、上記のＭＡＣ値計算処理は割込まれてもよい。従って、前記のメモリシステムがデータp_1，・・・，p_r中の未読のブロックの読取りを再開する場合、前に計算されたＭＡＣ値の不完全な組が失われている可能性があり、残りのＭＡＣ値の計算は以前に計算したＭＡＣ値に依存するため、残りのＭＡＣ値を計算することは不可能となる。したがって、本発明の他の特徴は、以前に計算されたＭＡＣ値の不完全な組は、セキュリティコンフィギュレーションレコード内の残りの値（例えばIV、鍵ｋ、データソースおよび行き先、アルゴリズム）と共に、例えば図１のＣＰＵ　ＲＡＭ　１２ａなどへ保存することに基づくことである。従って、メモリシステムがデータp_1，・・・，p_r中の未読のブロックの読取りを再開する場合、以前に計算されたＭＡＣ値の不完全な組はまだ利用可能であるので、残りのＭＡＣ値を計算することが可能である。

【００３８】

ブロック２４２の読取りセッションの終わりで、セッション終了のコマンドをホスト２４によって検知した後、読取ったデータを認証するために、ＣＰＵは、メモリ２０から読取ったデータから計算されたＭＡＣ値をメモリ２０に保存された前記のＭＡＣ値と比較する。若し、受信したホストコマンドが上記のどれでもない場合、ＣＰＵ１２は単に該コマンドを実行して、ブロック２０２に戻る（ブロック２５０）。

【００３９】

本発明は様々な実施例を参照して以上述べたが、添付された請求の範囲及びそれに相当するものだけで規定する本発明の範囲を逸脱しない範囲に、変更および修正を行い得ることが理解されたい。ここに引用された文献はすべて参照により盛り込まれる。

【図面の簡単な説明】

【００４０】

【図１】図１は、本発明を説明するための、ホスト装置と通信するメモリシステムのブロック図である。

【図２】図２は、図１の暗号化エンジンの一部のブロック図である。

【図３】図３は、本発明の一部分の好適な実施例を説明するための、図１に示されたシステムの作動を説明するフローチャートである。
【図４】図４は、複数のデータストリームを取り扱う場合の図1に示されたシステムの操作およびセキュリティコンフィギュレーションレコードの利用を説明するのに有用なフローチャートである。　記述上の便宜から、本出願では、同一の構成について同じ番号を付している。