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

特許第6516610号
(P6516610)

(45)発行日　令和1年5月22日(2019.5.22)　(24)登録日　平成31年4月26日(2019.4.26)

(51)Int.Cl.		F I		
H04L 9/10	(2006.01)	H04L	9/00	621A
G06F 21/55	(2013.01)	G06F	21/55	380
G06F 21/75	(2013.01)	G06F	21/75	
H04L 9/16	(2006.01)	H04L	9/00	643

請求項の数 8　(全 17 頁)

(21)出願番号　特願2015-145324(P2015-145324)
(22)出願日　平成27年7月22日(2015.7.22)
(65)公開番号　特開2017-28506(P2017-28506A)
(43)公開日　平成29年2月2日(2017.2.2)
審査請求日　平成29年6月22日(2017.6.22)

(73)特許権者　591128453
株式会社メガチップス
大阪府大阪市淀川区宮原一丁目1番1号
(74)代理人　100136353
弁理士　高尾　建吾
(72)発明者　菅原　崇彦
大阪市淀川区宮原一丁目1番1号　株式会社メガチップス内
(72)発明者　油谷　大武
大阪市淀川区宮原一丁目1番1号　株式会社メガチップス内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】メモリ装置、ホスト装置、及びメモリシステム

(57)【特許請求の範囲】
【請求項１】
ホスト装置に接続されるメモリ装置であって、
通常動作として入力データに基づいて第１の一時データを生成する第１の一時データ生成回路を有する、第１の暗号モジュールと、
通常動作として前記第１の一時データ生成回路によって生成された第１の一時データに基づいて第１のストリームデータを生成する第１のストリームデータ生成回路を有する、第２の暗号モジュールと、
ダミー動作としてダミーの入力データに基づいて第２の一時データを生成する第２の一時データ生成回路と、ダミー動作として前記第２の一時データ生成回路によって生成された第２の一時データに基づいて第２のストリームデータを生成する第２のストリームデータ生成回路とを有する、第３の暗号モジュールと、
前記第３の暗号モジュールの動作を制御する制御回路と、
を備え、
前記制御回路は、
前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１の一時データ生成回路のみが通常動作を実行する期間において、前記第２のストリームデータ生成回路にダミー動作を実行させ、
前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１のストリームデータ生成回路のみが通常動作を実行する期間において、前記第２の一時

データ生成回路にダミー動作を実行させる、メモリ装置。
【請求項２】
前記制御回路はさらに、前記第２の暗号モジュールが通常動作を実行し前記第１の暗号モジュールが通常動作を実行しない期間において、前記第１の暗号モジュールにダミー動作を実行させる、請求項１に記載のメモリ装置。
【請求項３】
前記制御回路はさらに、前記第１の暗号モジュール及び前記第２の暗号モジュールの双方が同時に通常動作を実行する期間において、前記第３の暗号モジュールにダミー動作を実行させる、請求項２に記載のメモリ装置。
【請求項４】
前記ホスト装置からの不正アクセスを検出する不正アクセス検出回路をさらに備え、
前記制御回路は、前記不正アクセス検出回路が不正アクセスを検出した場合に、前記第３の暗号モジュールにダミー動作を実行させる、請求項１～３のいずれか一つに記載のメモリ装置。
【請求項５】
メモリ装置が接続されるホスト装置であって、
通常動作として入力データに基づいて第１の一時データを生成する第１の一時データ生成回路を有する、第１の暗号モジュールと、
通常動作として前記第１の一時データ生成回路によって生成された第１の一時データに基づいて第１のストリームデータを生成する第１のストリームデータ生成回路を有する、第２の暗号モジュールと、
ダミー動作としてダミーの入力データに基づいて第２の一時データを生成する第２の一時データ生成回路と、ダミー動作として前記第２の一時データ生成回路によって生成された第２の一時データに基づいて第２のストリームデータを生成する第２のストリームデータ生成回路とを有する、第３の暗号モジュールと、
前記第３の暗号モジュールの動作を制御する制御回路と、
を備え、
前記制御回路は、
前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１の一時データ生成回路のみが通常動作を実行する期間において、前記第２のストリームデータ生成回路にダミー動作を実行させ、
前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１のストリームデータ生成回路のみが通常動作を実行する期間において、前記第２の一時データ生成回路にダミー動作を実行させる、ホスト装置。
【請求項６】
前記制御回路はさらに、前記第２の暗号モジュールが通常動作を実行し前記第１の暗号モジュールが通常動作を実行しない期間において、前記第１の暗号モジュールにダミー動作を実行させる、請求項５に記載のホスト装置。
【請求項７】
前記制御回路はさらに、前記第１の暗号モジュール及び前記第２の暗号モジュールの双方が同時に通常動作を実行する期間において、前記第３の暗号モジュールにダミー動作を実行させる、請求項６に記載のホスト装置。
【請求項８】
請求項１～４のいずれか一つに記載のメモリ装置と、
請求項５～７のいずれか一つに記載のホスト装置と、
を備える、メモリシステム。

【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、メモリ装置、ホスト装置、及びそれらを備えるメモリシステムに関する。
【背景技術】
【０００２】
ホスト装置とそれに接続されるメモリ装置とを備えるメモリシステムにおいて、両装置間で送受信されるコマンドやデータを暗号化することによってセキュリティ性を向上させたメモリシステムが実用化されている。
【０００３】
現在使用されている暗号方式は、暗号学的な解析手法に対して計算量的に安全であるとされている。しかし、実際にメモリシステムに暗号モジュールを実装する場合には、消費電力や処理時間のような、実装に依存したリークが発生する。そのような動作状況を様々な物理的手段で観察することにより、秘密鍵等の秘密情報を不正に取得しようとするサイドチャネル攻撃の脅威が増している。
【０００４】
サイドチャネル攻撃の一つとして、装置の消費電力を測定することによって秘密情報を解析する電力解析攻撃がある。その中でも、測定した複数の消費電力波形に対して統計処理による解析を行う差分電力解析（ＤＰＡ：Differential Power Analysis）が、特に強力な攻撃法として報告されている（下記非特許文献１参照）。
【０００５】
そのため近年では、ＤＰＡ攻撃に対する種々の対策回路が提案されており、例えば下記非特許文献２には、ＲＳＬ（Random Switching Logic）回路及びＷＤＤＬ（Wave Dynamic Differential Logic）回路が提案されている。ＲＳＬ回路は、乱数を用いて論理回路の動作モードを切り替えることによって状態遷移確率の偏りをなくし、それによって暗号鍵に依存しないよう消費電力をランダム化する。ＷＤＤＬ回路は、プリチャージ動作を行った後、演算時のビット値の違いに起因する消費電流の相違を相補回路によって低減することにより、消費電力を均一化する。
【先行技術文献】
【非特許文献】
【０００６】
【非特許文献１】Paul Kocher、他２名、”Introduction to Differential Power Analysis and related Attacks”、[online]、Cryptography Research、平成２７年７月１日検索、インターネット＜http://www.cryptography.com/public/pdf/DPATechInfo.pdf＞
【非特許文献２】Daisuke Suzuki、他２名、"Random Switching Logic: A Countermeasure against DPA based on Transition Probability"、[online]、International Association for Cryptologic Research、平成２７年７月１日検索、インターネット＜http://eprint.iacr.org/2004/346.pdf＞
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかし、ホスト装置とメモリ装置とを備えるメモリシステムにおいて、上述したＲＳＬ回路又はＷＤＤＬ回路を装置に実装する場合には、これらの回路を実装しない装置と比較して、演算時間、回路規模、及び消費電力が２～３倍以上に増大するため、コストが増大する。
【０００８】
本発明はかかる事情に鑑みて成されたものであり、ＤＰＡ攻撃に対する対策を低コストで実装することが可能な、メモリ装置、ホスト装置、及びそれらを備えるメモリシステムを得ることを目的とするものである。
【課題を解決するための手段】
【０００９】
本発明の第１の態様に係るメモリ装置は、ホスト装置に接続されるメモリ装置であって、通常動作として入力データに基づいて第１の一時データを生成する第１の一時データ生

成回路を有する、第１の暗号モジュールと、通常動作として前記第１の一時データ生成回路によって生成された第１の一時データに基づいて第１のストリームデータを生成する第１のストリームデータ生成回路を有する、第２の暗号モジュールと、ダミー動作としてダミーの入力データに基づいて第２の一時データを生成する第２の一時データ生成回路と、ダミー動作として前記第２の一時データ生成回路によって生成された第２の一時データに基づいて第２のストリームデータを生成する第２のストリームデータ生成回路とを有する、第３の暗号モジュールと、前記第３の暗号モジュールの動作を制御する制御回路と、を備え、前記制御回路は、前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１の一時データ生成回路のみが通常動作を実行する期間において、前記第２のストリームデータ生成回路にダミー動作を実行させ、前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１のストリームデータ生成回路のみが通常動作を実行する期間において、前記第２の一時データ生成回路にダミー動作を実行させることを特徴とするものである。

【００１０】
第１の態様に係るメモリ装置によれば、制御回路は、第１の暗号モジュール及び第２の暗号モジュールの一方が通常動作を実行する期間において、第３の暗号モジュールにダミー動作を実行させる。このように、第３の暗号モジュールにダミー動作を実行させることにより、通常動作を実行している第１又は第２の暗号モジュールが具有する消費電力特性を隠蔽することができる。その結果、ＤＰＡ攻撃に対する対策を低コストで実装することが可能となる。
また、第１の態様に係るメモリ装置によれば、制御回路は、第１の一時データ生成回路のみが通常動作を実行する期間においては第２のストリームデータ生成回路にダミー動作を実行させ、第１のストリームデータ生成回路のみが通常動作を実行する期間においては第２の一時データ生成回路にダミー動作を実行させる。これにより、メモリ装置全体の消費電力を均一化できるため、ＤＰＡ攻撃による消費電力特性の解析を困難化することが可能となる。

【００１１】
本発明の第２の態様に係るメモリ装置は、第１の態様に係るメモリ装置において特に、前記制御回路はさらに、前記第２の暗号モジュールが通常動作を実行し前記第１の暗号モジュールが通常動作を実行しない期間において、前記第１の暗号モジュールにダミー動作を実行させることを特徴とするものである。
【００１２】
第２の態様に係るメモリ装置によれば、制御回路は、第２の暗号モジュールが通常動作を実行し第１の暗号モジュールが通常動作を実行しない期間において、第１の暗号モジュールにダミー動作を実行させる。このように、第２の暗号モジュールのみが通常動作を実行する期間において第１の暗号モジュールをダミー動作させることにより、第２の暗号モジュールが具有する消費電力特性をさらに隠蔽することができる。
【００１３】
本発明の第３の態様に係るメモリ装置は、第２の態様に係るメモリ装置において特に、前記制御回路はさらに、前記第１の暗号モジュール及び前記第２の暗号モジュールの双方が同時に通常動作を実行する期間において、前記第３の暗号モジュールにダミー動作を実行させることを特徴とするものである。
【００１４】
第３の態様に係るメモリ装置によれば、制御回路は、第１の暗号モジュール及び第２の暗号モジュールの双方が同時に通常動作を実行する期間において、第３の暗号モジュールにダミー動作を実行させる。このように、第１の暗号モジュール及び第２の暗号モジュールの双方が通常動作を同時に実行する期間において第３の暗号モジュールをダミー動作させることにより、第１の暗号モジュール及び第２の暗号モジュールが具有する消費電力特

性をさらに隠蔽することができる。

【００２３】

本発明の第４の態様に係るメモリ装置は、第１～第３のいずれか一つの態様に係るメモリ装置において特に、前記ホスト装置からの不正アクセスを検出する不正アクセス検出回路をさらに備え、前記制御回路は、前記不正アクセス検出回路が不正アクセスを検出した場合に、前記第３の暗号モジュールにダミー動作を実行させることを特徴とするものである。

【００２４】

第４の態様に係るメモリ装置によれば、制御回路は、不正アクセス検出回路が不正アクセスを検出した場合に、第３の暗号モジュールにダミー動作を実行させる。従って、システムの可用性を確保できるとともに、不正アクセスを検出しない場合にダミー動作を実行させることに起因する消費電力の増大を回避することが可能となる。

【００２５】

本発明の第５の態様に係るホスト装置は、メモリ装置が接続されるホスト装置であって、通常動作として入力データに基づいて第１の一時データを生成する第１の一時データ生成回路を有する、第１の暗号モジュールと、通常動作として前記第１の一時データ生成回路によって生成された第１の一時データに基づいて第１のストリームデータを生成する第１のストリームデータ生成回路を有する、第２の暗号モジュールと、ダミー動作としてダミーの入力データに基づいて第２の一時データを生成する第２の一時データ生成回路と、ダミー動作として前記第２の一時データ生成回路によって生成された第２の一時データに基づいて第２のストリームデータを生成する第２のストリームデータ生成回路とを有する、第３の暗号モジュールと、前記第３の暗号モジュールの動作を制御する制御回路と、を備え、前記制御回路は、前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１の一時データ生成回路のみが通常動作を実行する期間において、前記第２のストリームデータ生成回路にダミー動作を実行させ、前記第１の一時データ生成回路及び前記第１のストリームデータ生成回路のうち前記第１のストリームデータ生成回路のみが通常動作を実行する期間において、前記第２の一時データ生成回路にダミー動作を実行させることを特徴とするものである。

【００２６】

第５の態様に係るホスト装置によれば、制御回路は、第１の暗号モジュール及び第２の暗号モジュールの一方が通常動作を実行する期間において、第３の暗号モジュールにダミー動作を実行させる。このように、第３の暗号モジュールにダミー動作を実行させることにより、通常動作を実行している第１又は第２の暗号モジュールが具有する消費電力特性を隠蔽することができる。その結果、ＤＰＡ攻撃に対する対策を低コストで実装することが可能となる。

また、第５の態様に係るホスト装置によれば、制御回路は、第１の一時データ生成回路のみが通常動作を実行する期間においては第２のストリームデータ生成回路にダミー動作を実行させ、第１のストリームデータ生成回路のみが通常動作を実行する期間においては第２の一時データ生成回路にダミー動作を実行させる。これにより、ホスト装置全体の消費電力を均一化できるため、ＤＰＡ攻撃による消費電力特性の解析を困難化することが可能となる。

【００２７】

本発明の第６の態様に係るホスト装置は、第５の態様に係るホスト装置において特に、前記制御回路はさらに、前記第２の暗号モジュールが通常動作を実行し前記第１の暗号モジュールが通常動作を実行しない期間において、前記第１の暗号モジュールにダミー動作を実行させることを特徴とするものである。

【００２８】
第６の態様に係るホスト装置によれば、制御回路は、第２の暗号モジュールが通常動作を実行し第１の暗号モジュールが通常動作を実行しない期間において、第１の暗号モジュールにダミー動作を実行させる。このように、第２の暗号モジュールのみが通常動作を実行する期間において第１の暗号モジュールをダミー動作させることにより、第２の暗号モジュールが具有する消費電力特性をさらに隠蔽することができる。

【００２９】
本発明の第７の態様に係るホスト装置は、第６の態様に係るホスト装置において特に、前記制御回路はさらに、前記第１の暗号モジュール及び前記第２の暗号モジュールの双方が同時に通常動作を実行する期間において、前記第３の暗号モジュールにダミー動作を実行させることを特徴とするものである。

【００３０】
第７の態様に係るホスト装置によれば、制御回路は、第１の暗号モジュール及び第２の暗号モジュールの双方が同時に通常動作を実行する期間において、第３の暗号モジュールにダミー動作を実行させる。このように、第１の暗号モジュール及び第２の暗号モジュールの双方が通常動作を同時に実行する期間において第３の暗号モジュールをダミー動作させることにより、第１の暗号モジュール及び第２の暗号モジュールが具有する消費電力特性をさらに隠蔽することができる。

【００３９】
本発明の第８の態様に係るメモリシステムは、第１～第４のいずれか一つの態様に係るメモリ装置と、第５～第７のいずれか一つの態様に係るホスト装置と、を備えることを特徴とするものである。

【００４０】
第８の態様に係るメモリシステムによれば、メモリ装置及びホスト装置の双方においてＤＰＡ攻撃に対する対策がそれぞれ実装されているため、メモリシステム全体としてＤＰＡ攻撃に対する耐性を高めることが可能となる。

【発明の効果】
【００４１】
本発明によれば、ＤＰＡ攻撃に対する対策を低コストで実装することが可能となる。
【図面の簡単な説明】
【００４２】
【図１】本発明の実施の形態に係るメモリシステムの構成を示す図である。
【図２】メモリ装置の暗号ブロックの構成を示す図である。
【図３】セッション鍵生成回路、ストリームデータ生成回路、及び暗号モジュールの処理内容を示すタイミングチャートである。
【図４】ホスト装置の暗号ブロックの構成を示す図である。
【図５】セッション鍵生成回路、ストリームデータ生成回路、及び暗号モジュールの処理内容を示すタイミングチャートである。
【図６】メモリ装置の暗号ブロックの構成を示す図である。
【図７】メモリ装置の暗号ブロックの構成を示す図である。
【図８】セッション鍵生成回路及びストリームデータ生成回路の処理内容を示すタイミングチャートである。
【図９】セッション鍵生成回路、ストリームデータ生成回路、及び暗号モジュールの処理内容を示すタイミングチャートである。

【発明を実施するための形態】
【００４３】
以下、本発明の実施の形態について、図面を用いて詳細に説明する。なお、異なる図面において同一の符号を付した要素は、同一又は相応する要素を示すものとする。
【００４４】
図１は、本発明の実施の形態に係るメモリシステム１の構成を簡略化して示す図である。図１に示すようにメモリシステム１は、ホスト装置２と、ホスト装置２に着脱自在に接続される半導体メモリ等のメモリ装置３とを備えて構成されている。
【００４５】
ホスト装置２は、ＣＰＵ１１、内部メモリ１２、主制御回路１３、及び暗号ブロック１４を有している。メモリ装置３は、暗号ブロック１４と同様の暗号ブロック２１と、コンテンツデータ等の任意のデータが格納されたメモリアレイ２２とを有している。暗号ブロック１４，２１は、ホスト装置２とメモリ装置３との間で送受信されるコマンドやデータに対して、暗号化処理及び復号化処理を実行する。
【００４６】
図２は、メモリ装置３の暗号ブロック２１の構成を示す図である。図２に示すように暗号ブロック２１は、制御回路３１、暗号モジュール３２～３４、及び演算回路３５を有している。暗号モジュール３２は、セッション鍵生成回路４２を有している。セッション鍵生成回路４２は、一時データ生成回路として機能し、入力データとしての鍵情報（秘密鍵Ｋ１１）に基づいて、一時データとしてのセッション鍵Ｄ１２を生成する。暗号モジュール３３は、ストリームデータ生成回路４３を有している。ストリームデータ生成回路４３は、暗号処理回路として機能し、鍵情報（秘密鍵Ｋ１３）と、セッション鍵生成回路４２から入力されたセッション鍵Ｄ１２とに基づいて、ストリーム暗号のためのストリームデータＤ１３を生成する。演算回路３５は、ホスト装置２から受信した暗号化コマンドＳ１１と、ストリームデータ生成回路４３から入力されたストリームデータＤ１３との排他的論理和を演算することにより、非暗号のコマンドＳ１２を復元する。また、演算回路３５は、メモリアレイ２２から読み出された非暗号のデータＳ１３と、ストリームデータ生成回路４３から入力されたストリームデータＤ１３との排他的論理和を演算することにより、暗号化データＳ１４を生成する。
【００４７】
暗号モジュール３４は、暗号モジュール３２，３３とは異なる暗号アルゴリズムの暗号モジュールであり、コマンドやデータの暗号化及び復号化には寄与しないダミー動作を実行する。暗号モジュール３４には、制御回路３１から制御信号Ｓ２０と鍵情報（ダミー鍵Ｋ１２）とが入力される。ダミー鍵Ｋ１２は、固定値であっても良いし、乱数生成器を用いた変動値であっても良い。あるいは、ダミー鍵Ｋ１２は秘密鍵Ｋ１１又は秘密鍵Ｋ１３と同一であっても良い。なお、暗号モジュール３４は、暗号モジュール３２又は暗号モジュール３３と同一の暗号アルゴリズムの暗号モジュールであっても良く、その場合には、ダミー鍵Ｋ１２として秘密鍵Ｋ１１，Ｋ１３とは異なる鍵が使用される。
【００４８】
図３は、セッション鍵生成回路４２、ストリームデータ生成回路４３、及び暗号モジュール３４の処理内容を示すタイミングチャートである。
【００４９】
コマンド処理期間（時刻Ｔ１１～Ｔ１２）において、ストリームデータ生成回路４３は、コマンド又はデータの暗号化又は復号化を実行するための通常動作として、ストリームデータＤ１３の生成処理を行い、これにより暗号化コマンドＳ１１の復号化が実行される。また、コマンド処理期間において、セッション鍵生成回路４２は動作せず、暗号モジュール３４はストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。
【００５０】
レイテンシ期間（時刻Ｔ１２～Ｔ１３）において、まずセッション鍵生成回路４２は、通常動作としてセッション鍵Ｄ１２の更新処理を行う。次にストリームデータ生成回路４

３は、通常動作として、更新後のセッション鍵Ｄ１２を用いて初期化処理を行う。また、レイテンシ期間において、暗号モジュール３４はセッション鍵生成回路４２及びストリームデータ生成回路４３の各動作期間に同期してダミー動作を実行する。

【００５１】

メモリアレイ２２からのデータの読み出しが完了した後のデータ処理期間（時刻Ｔ１３～Ｔ１４）において、ストリームデータ生成回路４３は、通常動作としてストリームデータＤ１３の生成処理を行い、これにより非暗号のデータＳ１３の暗号化が実行される。また、データ処理期間において、セッション鍵生成回路４２は動作せず、暗号モジュール３４はストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。

【００５２】

以下、メモリアレイ２２に格納されているデータをメモリ装置３からホスト装置２に読み出す処理を例にとり、メモリ装置３の動作を詳細に説明する。

【００５３】

メモリシステム１が起動されると、制御回路３１は、メモリアレイ２２の所定場所に格納されているＤＰＡ制御情報Ｄ１１（ＯＮ又はＯＦＦのフラグ情報）を読み出す。制御回路３１は、ＤＰＡ制御情報Ｄ１１がＯＮに設定されている場合には以下に述べるＤＰＡ対策処理を実行し、ＯＦＦに設定されている場合には実行しない。本実施の形態の例では、ＤＰＡ制御情報Ｄ１１はＯＮに設定されているものとする。なお、ＤＰＡ制御情報Ｄ１１は、ホスト装置２から発行されるコマンドの一部に格納されていても良く、この場合には、ＤＰＡ対策処理の実行の要否をホスト装置２によって簡易に切り替えることが可能となる。

【００５４】

次に制御回路３１は、ＤＰＡ対策処理として暗号モジュール３４のダミー動作を実行するために、制御信号Ｓ２０及びダミー鍵Ｋ１２を暗号モジュール３４に入力する。

【００５５】

次にホスト装置２は、ＣＰＵ１１が発行した読み出しコマンドを暗号ブロック１４によって暗号化することにより、暗号化コマンドＳ１１をメモリ装置３に送信する。

【００５６】

次にコマンド処理期間（時刻Ｔ１１～Ｔ１２）において、ストリームデータ生成回路４３は、通常動作として、セッション鍵生成回路４２から入力された最新のセッション鍵Ｄ１２に基づいてストリームデータＤ１３の生成処理を行い、これにより暗号化コマンドＳ１１の復号化が実行される。また、暗号モジュール３４は、ストリームデータ生成回路４３の動作期間に同期して、ダミー鍵Ｋ１２に基づいてダミー動作を実行する。暗号モジュール３４のダミー動作によって生成されたデータは、メモリ装置３内で廃棄しても良いし、ダミーデータとしてメモリ装置３の外部に出力しても良い。

【００５７】

次にレイテンシ期間（時刻Ｔ１２～Ｔ１３）において、まずセッション鍵生成回路４２は、通常動作としてセッション鍵Ｄ１２の更新処理を行うことにより、新たなセッション鍵Ｄ１２を生成する。また、暗号モジュール３４は、セッション鍵生成回路４２の動作期間に同期してダミー動作を実行する。次にストリームデータ生成回路４３は、通常動作として、更新後のセッション鍵Ｄ１２を用いて初期化処理を行う。また、暗号モジュール３４は、セッション鍵生成回路４２の動作期間に同期してダミー動作を実行する。次に、上述した暗号化コマンドＳ１１の復号化によって復元された非暗号のコマンドＳ１２に基づいて、メモリアレイ２２から所望のデータＳ１３が読み出される。

【００５８】

次にデータ処理期間（時刻Ｔ１３～Ｔ１４）において、ストリームデータ生成回路４３は、通常動作として、セッション鍵生成回路４２から入力された更新後のセッション鍵Ｄ１２に基づいてストリームデータＤ１３の生成処理を行い、これにより非暗号のデータＳ１３の暗号化が実行される。暗号化データＳ１４は、メモリ装置３からホスト装置２に送信される。また、暗号モジュール３４は、ストリームデータ生成回路４３の動作期間に同

期してダミー動作を実行する。

【００５９】

このように本実施の形態に係るメモリ装置３によれば、制御回路３１は、暗号モジュール３２（第１の暗号モジュール）及び暗号モジュール３３（第２の暗号モジュール）の一方が通常動作を実行する期間において、暗号モジュール３４（第３の暗号モジュール）にダミー動作を実行させる。このように、暗号モジュール３４にダミー動作を実行させることにより、通常動作を実行している暗号モジュール３２又は暗号モジュール３３が具有する消費電力特性を隠蔽することができる。その結果、ＤＰＡ攻撃に対する対策を低コストで実装することが可能となる。

【００６０】

また、ダミー鍵Ｋ１２をあえて固定値とし、何らかの鍵データの生成処理が実行されていることを攻撃者に予見させることにより、解析によってダミー鍵Ｋ１２を特定するという無駄な作業を攻撃者に行わせる効果が期待できる。その結果、秘密鍵Ｋ１１，Ｋ１３を長期間保護することが可能となる。また、ダミー鍵Ｋ１２を固定値とすることにより、ダミー動作に伴う暗号モジュール３４の消費電力を均一化することが可能となる。

【００６１】

また、ダミー鍵Ｋ１２を変動値とすることにより、ダミー鍵Ｋ１２が変動する度に暗号モジュール３４の消費電力も変動するため、メモリ装置３全体の消費電力を変動させることができる。その結果、ＤＰＡ攻撃による消費電力特性の解析を困難化することが可能となる。

【００６２】

また、入力データとして秘密鍵Ｋ１１（鍵情報）を入力することにより、セッション鍵生成回路４２は、一時データとしてセッション鍵Ｄ１２を生成することが可能となる。

【００６３】

＜第１の変形例＞

上記実施の形態では、ＤＰＡ対策をメモリ装置３に実装する例について説明したが、ＤＰＡ対策をホスト装置２に実装しても良い。

【００６４】

図４は、ホスト装置２の暗号ブロック１４の構成を示す図である。図４に示すように暗号ブロック１４は、制御回路５１、暗号モジュール５２～５４、及び演算回路５５を有している。暗号モジュール５２は、セッション鍵生成回路６２を有している。セッション鍵生成回路６２は、一時データ生成回路として機能し、入力データとしての鍵情報（秘密鍵Ｋ２１）に基づいて、一時データとしてのセッション鍵Ｄ２２を生成する。暗号モジュール５３は、ストリームデータ生成回路６３を有している。ストリームデータ生成回路６３は、暗号処理回路として機能し、鍵情報（秘密鍵Ｋ２３）と、セッション鍵生成回路６２から入力されたセッション鍵Ｄ２２とに基づいて、ストリーム暗号のためのストリームデータＤ２３を生成する。演算回路５５は、メモリ装置３から受信した暗号化データＳ２３と、ストリームデータ生成回路６３から入力されたストリームデータＤ２３との排他的論理和を演算することにより、非暗号のデータＳ２４を復元する。また、演算回路５５は、主制御回路１３から入力された非暗号のコマンドＳ２１と、ストリームデータ生成回路６３から入力されたストリームデータＤ２３との排他的論理和を演算することにより、暗号化コマンドＳ２２を生成する。

【００６５】

暗号モジュール５４は、暗号モジュール５２，５３とは異なる暗号アルゴリズムの暗号モジュールであり、コマンドやデータの暗号化及び復号化には寄与しないダミー動作を実行する。暗号モジュール５４には、制御回路５１から制御信号Ｓ３０と鍵情報（ダミー鍵Ｋ２２）とが入力される。ダミー鍵Ｋ２２は、固定値であっても良いし、乱数生成器を用いた変動値であっても良い。あるいは、ダミー鍵Ｋ２２は秘密鍵Ｋ２１又は秘密鍵Ｋ２３と同一であっても良い。なお、暗号モジュール５４は、暗号モジュール５２又は暗号モジュール５３と同一の暗号アルゴリズムの暗号モジュールであっても良く、その場合には、

ダミー鍵Ｋ２２として秘密鍵Ｋ２１，Ｋ２３とは異なる鍵が使用される。

【００６６】

図５は、セッション鍵生成回路６２、ストリームデータ生成回路６３、及び暗号モジュール５４の処理内容を示すタイミングチャートである。

【００６７】

コマンド処理期間（時刻Ｔ２１～Ｔ２２）において、ストリームデータ生成回路６３は、コマンド又はデータの暗号化又は復号化を実行するための通常動作として、ストリームデータＤ２３の生成処理を行い、これにより非暗号のコマンドＳ２１の暗号化が実行される。また、コマンド処理期間において、セッション鍵生成回路６２は動作せず、暗号モジュール５４はストリームデータ生成回路６３の動作期間に同期してダミー動作を実行する。

【００６８】

レイテンシ期間（時刻Ｔ２２～Ｔ２３）において、まずセッション鍵生成回路６２は、通常動作としてセッション鍵Ｄ２２の更新処理を行う。次にストリームデータ生成回路６３は、通常動作として、更新後のセッション鍵Ｄ２２を用いて初期化処理を行う。また、レイテンシ期間において、暗号モジュール５４はセッション鍵生成回路６２及びストリームデータ生成回路６３の各動作期間に同期してダミー動作を実行する。

【００６９】

データ処理期間（時刻Ｔ２３～Ｔ２４）において、ストリームデータ生成回路６３は、通常動作としてストリームデータＤ２３の生成処理を行い、これにより暗号化データＳ２３の復号化が実行される。また、データ処理期間において、セッション鍵生成回路６２は動作せず、暗号モジュール５４はストリームデータ生成回路６３の動作期間に同期してダミー動作を実行する。

【００７０】

以下、メモリアレイ２２に格納されているデータをメモリ装置３からホスト装置２に読み出す処理を例にとり、ホスト装置２の動作を詳細に説明する。

【００７１】

メモリシステム１が起動されると、制御回路５１は、メモリアレイ２２の所定場所に格納されているＤＰＡ制御情報Ｄ１１を読み出す。制御回路５１は、ＤＰＡ制御情報Ｄ１１がＯＮに設定されている場合には以下に述べるＤＰＡ対策処理を実行し、ＯＦＦに設定されている場合には実行しない。本変形例では、ＤＰＡ制御情報Ｄ１１はＯＮに設定されているものとする。

【００７２】

次にＣＰＵ１１は、非暗号の読み出しコマンドＳ２１を発行する。コマンドＳ２１は、主制御回路１３を介して暗号ブロック１４に入力される。

【００７３】

次にコマンド処理期間（時刻Ｔ２１～Ｔ２２）において、ストリームデータ生成回路６３は、通常動作として、セッション鍵生成回路６２から入力された最新のセッション鍵Ｄ２２に基づいてストリームデータＤ２３の生成処理を行い、これにより非暗号のコマンドＳ２１の暗号化が実行される。また、暗号モジュール５４は、ストリームデータ生成回路６３の動作期間に同期して、ダミー鍵Ｋ２２に基づいてダミー動作を実行する。暗号モジュール５４のダミー動作によって生成されたデータは、ホスト装置２内で廃棄しても良いし、ダミーデータとしてホスト装置２の外部に出力しても良い。

【００７４】

次にレイテンシ期間（時刻Ｔ２２～Ｔ２３）において、まずセッション鍵生成回路６２は、通常動作としてセッション鍵Ｄ２２の更新処理を行うことにより、新たなセッション鍵Ｄ２２を生成する。また、暗号モジュール５４は、セッション鍵生成回路６２の動作期間に同期してダミー動作を実行する。次にストリームデータ生成回路６３は、通常動作として、更新後のセッション鍵Ｄ２２を用いて初期化処理を行う。また、暗号モジュール５４は、セッション鍵生成回路６２の動作期間に同期してダミー動作を実行する。

【００７５】
次にデータ処理期間（時刻Ｔ２３～Ｔ２４）において、ストリームデータ生成回路６３は、通常動作として、セッション鍵生成回路６２から入力された更新後のセッション鍵Ｄ２２に基づいてストリームデータＤ２３の生成処理を行い、これにより暗号化データＳ２３の復号化が実行される。復号化されたデータＳ２４は、主制御回路１３を介してＣＰＵ１１に入力される。
【００７６】
このように本変形例に係るホスト装置２によれば、制御回路５１は、暗号モジュール５２（第１の暗号モジュール）及び暗号モジュール５３（第２の暗号モジュール）の一方が通常動作を実行する期間において、暗号モジュール５４（第３の暗号モジュール）にダミー動作を実行させる。このように、暗号モジュール５４にダミー動作を実行させることにより、通常動作を実行している暗号モジュール５２又は暗号モジュール５３が具有する消費電力特性を隠蔽することができる。その結果、ＤＰＡ攻撃に対する対策を低コストで実装することが可能となる。
【００７７】
また、ダミー鍵Ｋ２２をあえて固定値とし、何らかの鍵データの生成処理が実行されていることを攻撃者に予見させることにより、解析によってダミー鍵Ｋ２２を特定するという無駄な作業を攻撃者に行わせる効果が期待できる。その結果、秘密鍵Ｋ２１，Ｋ２３を長期間保護することが可能となる。また、ダミー鍵Ｋ２２を固定値とすることにより、ダミー動作に伴う暗号モジュール５４の消費電力を均一化することが可能となる。
【００７８】
また、ダミー鍵Ｋ２２を変動値とすることにより、ダミー鍵Ｋ２２が変動する度に暗号モジュール５４の消費電力も変動するため、ホスト装置２全体の消費電力を変動させることができる。その結果、ＤＰＡ攻撃による消費電力特性の解析を困難化することが可能となる。
【００７９】
また、入力データとして秘密鍵Ｋ２１（鍵情報）を入力することにより、セッション鍵生成回路６２は、一時データとしてセッション鍵Ｄ２２を生成することが可能となる。
【００８０】
＜第２の変形例＞
上記実施の形態では、ＤＰＡ制御情報Ｄ１１に基づいてＤＰＡ対策処理の実行の要否が判定されたが、ホスト装置２からメモリ装置３への不正アクセスがあったことを条件として、ＤＰＡ対策処理を実行しても良い。
【００８１】
図６は、メモリ装置３の暗号ブロック２１の構成を示す図である。図２に示した構成に対して不正アクセス検出回路３６が追加されている。不正アクセス検出回路３６には、復号化によって復元された非暗号のコマンドＳ１２が、演算回路３５から入力される。
【００８２】
不正アクセス検出回路３６は、例えば、所定のアクセス禁止領域へのアクセス要求、メモリアレイ２２のデータ容量を超えるアクセス要求、コマンドＩＤが定義されていない未定義コマンドによるアクセス要求、及び、規定のコマンドシーケンス以外のシーケンスによるアクセス要求等をホスト装置２から受けた場合に、そのアクセスを不正アクセスとして検出し、不正アクセス検出信号Ｄ１４を制御回路３１に入力する。
【００８３】
制御回路３１は、不正アクセス検出信号Ｄ１４が入力されたことを実行条件として、上記実施の形態で説明したＤＰＡ対策処理を実行する。
【００８４】
このように本変形例に係るメモリ装置３によれば、制御回路３１は、不正アクセス検出回路３６が不正アクセスを検出した場合に、ＤＰＡ対策処理を実行する。従って、メモリシステム１の可用性を確保できるとともに、不正アクセスを検出しない場合にダミー動作

を実行させることに起因する消費電力の増大を回避することが可能となる。

【００８５】

＜第３の変形例＞

図７は、メモリ装置３の暗号ブロック２１の構成を示す図である。図７に示すように暗号ブロック２１は、制御回路３１、暗号モジュール３２～３４、及び演算回路３５を有している。暗号モジュール３４は、セッション鍵生成回路４２（第１の一時データ生成回路）と同様のセッション鍵生成回路７２（第２の一時データ生成回路）と、ストリームデータ生成回路４３（第１の暗号処理回路）と同様のストリームデータ生成回路７３（第２の暗号処理回路）とを有している。

【００８６】

図８は、セッション鍵生成回路４２，７２及びストリームデータ生成回路４３，７３の処理内容を示すタイミングチャートである。

【００８７】

コマンド処理期間（時刻Ｔ１１～Ｔ１２）において、ストリームデータ生成回路４３は、通常動作としてストリームデータＤ１３の生成処理を行い、これにより暗号化コマンドＳ１１の復号化が実行される。この時、セッション鍵生成回路４２及びストリームデータ生成回路７３は動作せず、セッション鍵生成回路７２はストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。

【００８８】

レイテンシ期間（時刻Ｔ１２～Ｔ１３）において、まずセッション鍵生成回路４２は、通常動作としてセッション鍵Ｄ１２の更新処理を行う。この時、ストリームデータ生成回路４３及びセッション鍵生成回路７２は動作せず、ストリームデータ生成回路７３はセッション鍵生成回路４２の動作期間に同期してダミー動作を実行する。次にストリームデータ生成回路４３は、通常動作として、更新後のセッション鍵Ｄ１２を用いて初期化処理を行う。この時、セッション鍵生成回路４２及びストリームデータ生成回路７３は動作せず、セッション鍵生成回路７２はストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。

【００８９】

データ処理期間（時刻Ｔ１３～Ｔ１４）において、ストリームデータ生成回路４３は、通常動作としてストリームデータＤ１３の生成処理を行い、これにより非暗号のデータＳ１３の暗号化が実行される。この時、セッション鍵生成回路４２及びストリームデータ生成回路７３は動作せず、セッション鍵生成回路７２はストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。

【００９０】

このように本変形例に係るメモリ装置３によれば、制御回路３１は、セッション鍵生成回路４２のみが通常動作を実行する期間においてはストリームデータ生成回路７３にダミー動作を実行させ、ストリームデータ生成回路４３のみが通常動作を実行する期間においてはセッション鍵生成回路７２にダミー動作を実行させる。これにより、メモリ装置３全体の消費電力を均一化できるため、ＤＰＡ攻撃による消費電力特性の解析を困難化することが可能となる。

【００９１】

なお、以上の説明では本変形例をメモリ装置３に適用する例について説明したが、本変形例はホスト装置２にも適用することが可能であり、同様の効果を得ることができる。

【００９２】

＜第４の変形例＞

図９は、セッション鍵生成回路４２、ストリームデータ生成回路４３、及び暗号モジュール３４の処理内容を示すタイミングチャートである。

【００９３】

コマンド処理期間（時刻Ｔ１１～Ｔ１２）において、ストリームデータ生成回路４３は、通常動作としてストリームデータＤ１３の生成処理を行い、これにより暗号化コマンド

Ｓ１１の復号化が実行される。この時、セッション鍵生成回路４２及び暗号モジュール３４は、ストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。

【００９４】

制御回路３１は、セッション鍵生成回路４２のダミー動作を実行するために、セッション鍵生成回路４２の現在の設定内容を示す状態遷移情報を暗号モジュール３２から読み出し、制御回路３１が内部に有する保持回路に当該状態遷移情報を保持する。また、制御回路３１は、秘密鍵Ｋ１１に代えて固定値又は変動値のダミー鍵をセッション鍵生成回路４２に入力する。セッション鍵生成回路４２は、当該ダミー鍵に基づいてダミーのセッション鍵Ｄ１２を生成する。

【００９５】

次にレイテンシ期間（時刻Ｔ１２～Ｔ１３）において、制御回路３１は、保持回路が保持している状態遷移情報をセッション鍵生成回路４２に書き戻す。これにより、セッション鍵生成回路４２の設定内容は、ダミー動作を実行する前の状態に再設定される。また、制御回路３１は、ダミー鍵に代えて秘密鍵Ｋ１１をセッション鍵生成回路４２に入力する。セッション鍵生成回路４２は、通常動作としてセッション鍵Ｄ１２の更新処理を行うことにより、次回に使用する新たなセッション鍵Ｄ１２を生成する。それと同時にストリームデータ生成回路４３は、通常動作として、現在入力されている更新前のセッション鍵Ｄ１２を用いて初期化処理を行う。この時、暗号モジュール３４は、セッション鍵生成回路４２及びストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。

【００９６】

次にデータ処理期間（時刻Ｔ１３～Ｔ１４）において、ストリームデータ生成回路４３は、通常動作としてストリームデータＤ１３の生成処理を行い、これにより非暗号のデータＳ１３の暗号化が実行される。この時、セッション鍵生成回路４２及び暗号モジュール３４は、ストリームデータ生成回路４３の動作期間に同期してダミー動作を実行する。

【００９７】

このように本変形例に係るメモリ装置３によれば、制御回路３１は、暗号モジュール３３が通常動作を実行し暗号モジュール３２が通常動作を実行しない期間（コマンド処理期間及びデータ処理期間）において、暗号モジュール３２，３４にダミー動作を実行させる。このように、暗号モジュール３３のみが通常動作を実行する期間において暗号モジュール３２，３４をダミー動作させることにより、暗号モジュール３３が具有する消費電力特性をさらに隠蔽することができる。

【００９８】

また、制御回路３１は、暗号モジュール３２，３３の双方が同時に通常動作を実行する期間（レイテンシ期間）において、暗号モジュール３４にダミー動作を実行させる。このように、暗号モジュール３２，３３の双方が通常動作を同時に実行する期間において暗号モジュール３４をダミー動作させることにより、暗号モジュール３２，３３が具有する消費電力特性をさらに隠蔽することができる。

【００９９】

なお、以上の説明では本変形例をメモリ装置３に適用する例について説明したが、本変形例はホスト装置２にも適用することが可能であり、同様の効果を得ることができる。

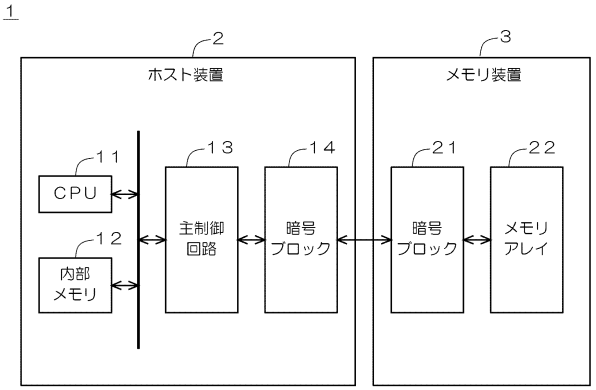
【符号の説明】

【０１００】

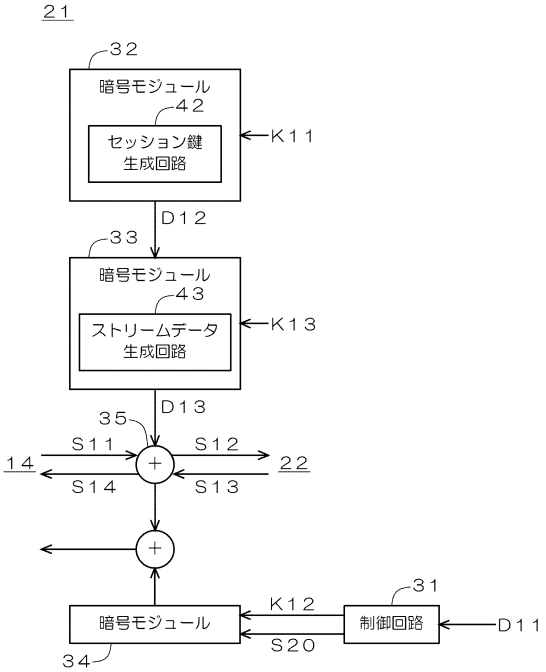
１　メモリシステム
２　ホスト装置
３　メモリ装置
１４，２１　暗号ブロック
３１，５１　制御回路
３２～３４，５２～５４　暗号モジュール
３６　不正アクセス検出回路
４２，６２，７２　セッション鍵生成回路

４３，６３，７３　ストリームデータ生成回路

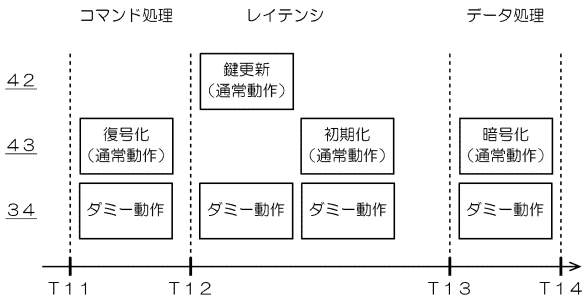
【図１】



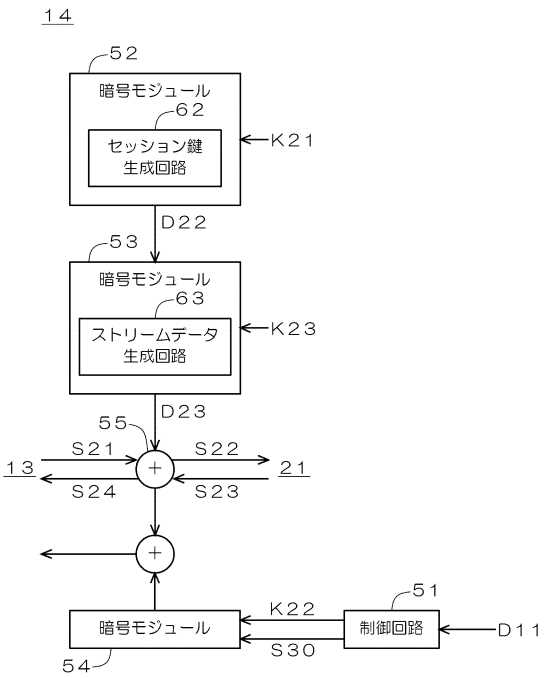
【図２】



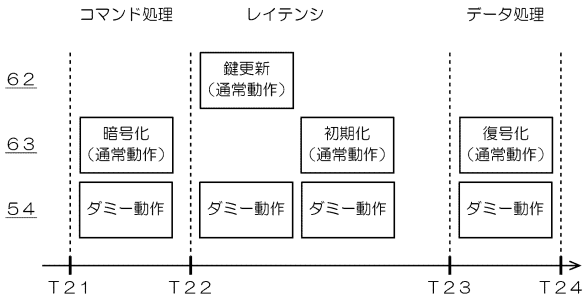
【図３】


コマンド処理
レイテンシ
データ処理
42
43
34
鍵更新
（通常動作）
復号化
（通常動作）
初期化
（通常動作）
暗号化
（通常動作）
ダミー動作
ダミー動作
ダミー動作
ダミー動作
T11
T12
T13
T14

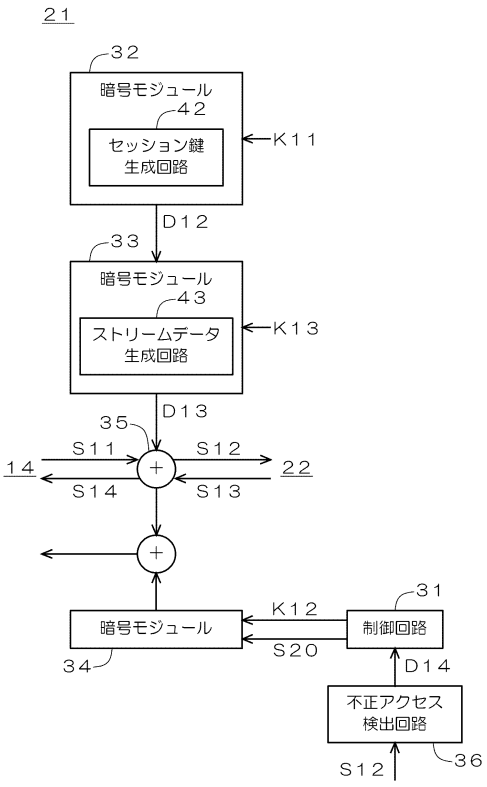
【図４】


14
52
暗号モジュール
62
セッション鍵
生成回路
K21
D22
53
暗号モジュール
63
ストリームデータ
生成回路
K23
D23
55
S21
S22
13
21
S24
S23
51
K22
暗号モジュール
制御回路
D11
S30
54

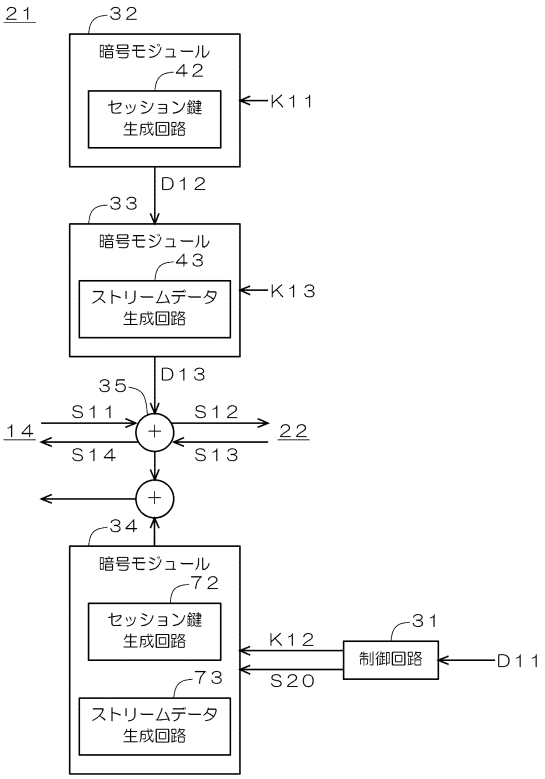
【図５】


コマンド処理
レイテンシ
データ処理
62
63
54
鍵更新
（通常動作）
暗号化
（通常動作）
初期化
（通常動作）
復号化
（通常動作）
ダミー動作
ダミー動作
ダミー動作
ダミー動作
T21
T22
T23
T24

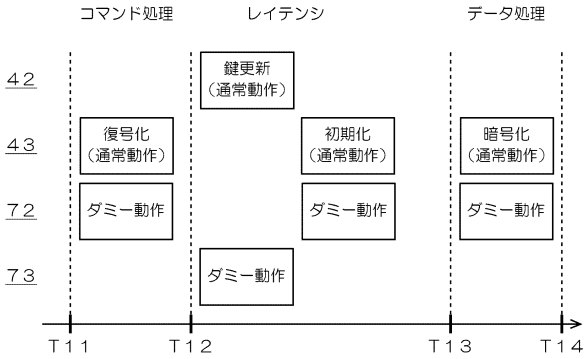
【図６】


21
32
暗号モジュール
42
セッション鍵
生成回路
K11
D12
33
暗号モジュール
43
ストリームデータ
生成回路
K13
D13
35
S11
S12
14
22
S14
S13
31
K12
暗号モジュール
制御回路
S20
34
D14
不正アクセス
検出回路
S12
36

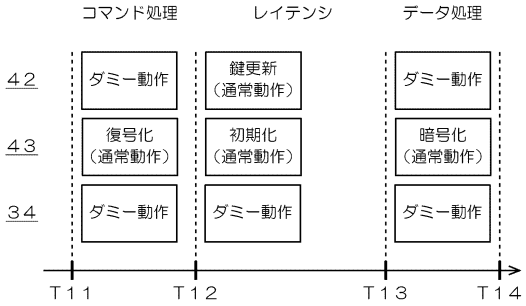
【図７】


21
32
暗号モジュール
42
セッション鍵
生成回路
K11
D12
33
暗号モジュール
43
ストリームデータ
生成回路
K13
D13
35
S11
S12
14
22
S14
S13
34
暗号モジュール
72
セッション鍵
生成回路
31
K12
制御回路
D11
S20
73
ストリームデータ
生成回路

【図８】


コマンド処理
レイテンシ
データ処理
42
43
72
73
鍵更新
（通常動作）
復号化
（通常動作）
初期化
（通常動作）
暗号化
（通常動作）
ダミー動作
ダミー動作
ダミー動作
ダミー動作
ダミー動作
T11
T12
T13
T14

【図９】


コマンド処理
レイテンシ
データ処理
42
43
34
ダミー動作
鍵更新
（通常動作）
ダミー動作
復号化
（通常動作）
初期化
（通常動作）
暗号化
（通常動作）
ダミー動作
ダミー動作
ダミー動作
T11
T12
T13
T14

フロントページの続き

(56)参考文献 特開２０１５－０２６８９２（ＪＰ，Ａ）
特表２００４－５１６７０６（ＪＰ，Ａ）
特開２００３－０１８１４３（ＪＰ，Ａ）
特開２０１３－１４３６５３（ＪＰ，Ａ）
米国特許第０９７３５９５３（ＵＳ，Ｂ１）
特開２００７－１９５１３２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０
Ｇ０６Ｆ　２１／５５
Ｇ０６Ｆ　２１／７５
Ｈ０４Ｌ　　９／１６