(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6239259号
(P6239259)
(45)発行日　平成29年11月29日(2017.11.29)　(24)登録日　平成29年11月10日(2017.11.10)

(51)Int.Cl.　F I
H04L 9/10 (2006.01)　H04L 9/00 621A

請求項の数 20 (全 18 頁)

(21)出願番号　特願2013-97518(P2013-97518)
(22)出願日　平成25年5月7日(2013.5.7)
(65)公開番号　特開2013-236376(P2013-236376A)
(43)公開日　平成25年11月21日(2013.11.21)
審査請求日　平成28年3月17日(2016.3.17)
(31)優先権主張番号　10-2012-0047743
(32)優先日　平成24年5月4日(2012.5.4)
(33)優先権主張国　韓国(KR)

(73)特許権者　390019839
三星電子株式会社
Ｓａｍｓｕｎｇ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｃｏ．，Ｌｔｄ．
大韓民国京畿道水原市霊通区三星路１２９
１２９，Ｓａｍｓｕｎｇ－ｒｏ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　110000051
特許業務法人共生国際特許事務所
(72)発明者　李　憲　洙
大韓民国　京畿道　華城市　石隅洞　禮堂マウルウミリン第１プンギョンチェアパート　１２２棟　１４０２号
最終頁に続く

(54)【発明の名称】システムオンチップとその動作方法、及びそれを含むシステムインパッケージ

(57)【特許請求の範囲】
【請求項１】
システムオンチップ（ＳｏＣ）の動作方法であって、
前記ＳｏＣに含まれるエンジンが、前記ＳｏＣに含まれるデータバスを介して平文データを受信する段階と、
前記エンジンが、前記ＳｏＣに含まれるＣＰＵによってセキュリティモードで入力された暗号キーを用いて前記平文データを暗号文データに変換する段階と、
前記エンジンが、前記暗号文データを前記ＳｏＣに含まれるメモリコントローラに前記データバスを介すること無く、直接伝送する段階と、を有し、
前記メモリコントローラは、不揮発性メモリの動作を制御することを特徴とするシステムオンチップの動作方法。
【請求項２】
前記平文データを暗号文データに変換する段階の前に、前記平文データを前記ＣＰＵの制御によってメインメモリから前記データバスを介してリードする段階を更に含むことを特徴とする請求項１に記載のシステムオンチップの動作方法。
【請求項３】
システムオンチップ（ＳｏＣ）の動作方法であって、
前記ＳｏＣに含まれるエンジンが、前記ＳｏＣに含まれるメモリコントローラから暗号文データを直接受信する段階と、
前記エンジンが、前記ＳｏＣに含まれるＣＰＵによってセキュリティモードで前記エン

ジンに入力された暗号キーを用いて前記暗号文データを平文データに変換する段階と、を有し、
前記メモリコントローラは、不揮発性メモリの動作を制御することを特徴とするシステムオンチップの動作方法。
【請求項４】
前記暗号文データを平文データに変換する段階の前に、前記平文データを前記ＳｏＣに含まれるＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ）ユニットから前記エンジンに伝送する段階を更に含むことを特徴とする請求項３に記載のシステムオンチップの動作方法。
【請求項５】
システムオンチップ（ＳｏＣ）であって、
ＣＰＵと、
前記ＣＰＵによってセキュリティモードで入力された暗号キーを用いて、第１平文データを第１暗号文データに暗号化し、第２暗号文データを第２平文データに復号化する暗号化／復号化エンジンと、
前記暗号化／復号化エンジンに直接接続され、前記第１暗号文データを不揮発性メモリに伝送し、前記不揮発性メモリから前記第２暗号文データを受信するメモリコントローラと、を有し、
前記暗号化／復号化エンジンと前記メモリコントローラとは直接接続され、前記暗号化／復号化エンジンと前記メモリコントローラとの間にはいかなる装置も接続されないことを特徴とするシステムオンチップ。
【請求項６】
前記暗号キーを保存するワンタイムプログラマブル（ＯＴＰ）メモリを更に含むことを特徴とする請求項５に記載のシステムオンチップ。
【請求項７】
前記システムオンチップ（ＳｏＣ）の外部にある装置から受信した前記第１平文データを前記暗号化／復号化エンジンに伝送し、前記暗号化／復号化エンジンから受信した前記第２平文データを前記装置に伝送するＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ）ユニットを更に含むことを特徴とする請求項５に記載のシステムオンチップ。
【請求項８】
前記ＣＰＵは、前記システムオンチップ（ＳｏＣ）の外部にある装置と前記暗号化／復号化エンジンとの間で前記第１平文データ又は前記第２平文データの伝送を制御することを特徴とする請求項５に記載のシステムオンチップ。
【請求項９】
請求項５に記載のシステムオンチップ（ＳｏＣ）と、
前記ＳｏＣの制御によって、不揮発性メモリとデータを通信する装置と、を備えることを特徴とするシステムインパッケージ。
【請求項１０】
請求項５に記載のシステムオンチップ（ＳｏＣ）と、
不揮発性メモリと、
前記ＳｏＣの制御によって、前記不揮発性メモリとデータを通信する装置と、を備えることを特徴とするシステムインパッケージ。
【請求項１１】
システムオンチップ（ＳｏＣ）であって、
ＣＰＵと、
外部の揮発性メモリから平文データを受信する揮発性メモリコントローラと、
不揮発性メモリコントローラに直接接続され、前記揮発性メモリコントローラから送信された前記平文データを、前記ＣＰＵによってセキュリティモードで入力された暗号キーを用いて暗号文データに暗号化する暗号化エンジンと、
前記ＣＰＵ及び前記揮発性メモリコントローラに接続されたデータバスと、

不揮発性メモリを制御し、前記平文データを送信するために用いられる前記データバスを介すること無く、前記暗号文データを前記暗号化エンジンから直接受信する不揮発性メモリコントローラと、を有し、
前記ＳｏＣは、前記ＳｏＣの外部にある装置と前記不揮発性メモリとの間のデータの伝送を制御し、
前記不揮発性メモリコントローラ及び前記暗号化エンジンは、前記データを伝送するための第１データパスに該当し、
前記暗号化エンジンと前記不揮発性メモリコントローラとは直接接続され、前記暗号化エンジンと前記不揮発性メモリコントローラとの間にはいかなる装置も接続されないことを特徴とするシステムオンチップ。
【請求項１２】
暗号キーを保存するためのワンタイムプログラマブル（ＯＴＰ）メモリを更に含み、
前記暗号化エンジンは、前記ＯＴＰメモリに保存された暗号キーを用いて、前記データを暗号化することを特徴とする請求項１１に記載のシステムオンチップ。
【請求項１３】
前記第１データパスは、前記装置から受信した前記データを前記暗号化エンジンに伝送し、前記暗号化エンジンから受信した前記データを前記装置に伝送するＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ）ユニットを更に含むことを特徴とする請求項１１に記載のシステムオンチップ。
【請求項１４】
前記ＤＭＡユニットは、前記暗号化エンジンに直接接続されることを特徴とする請求項１３に記載のシステムオンチップ。
【請求項１５】
暗号化されていない前記データを伝送する第２データパスを更に含むことを特徴とする請求項１４に記載のシステムオンチップ。
【請求項１６】
選択信号に基づいて、前記第１データパス及び前記第２データパスのうちの何れか１つを選択するための選択回路を更に含むことを特徴とする請求項１５に記載のシステムオンチップ。
【請求項１７】
システムオンチップ（ＳｏＣ）であって、
ＣＰＵと、
前記ＣＰＵに接続されたデータバスと、
前記データバスに平文データを出力するメインメモリコントローラと、
前記データバスから受信した前記平文データを、前記ＣＰＵによってセキュリティモードで入力された暗号キーを用いて暗号文データに暗号化するエンジンと、
前記データバスを介すること無く、前記暗号文データを前記エンジンから直接受信する不揮発性メモリコントローラと、
前記エンジンをバイパスして前記データバスを前記不揮発性メモリコントローラに接続させる第１電気的経路と、
前記エンジンを介して前記データバスを前記不揮発性メモリコントローラに接続させる第２電気的経路と、を有し、
前記ＳｏＣは、非セキュリティモードで、前記平文データを前記データバスから前記不揮発性メモリコントローラに伝送するために前記第１電気的経路のみを活性化させ、
前記ＳｏＣは、セキュリティモードで、前記平文データを前記エンジンに伝送し、前記エンジンから受信した前記暗号文データを前記不揮発性メモリコントローラに伝送するために前記第２電気的経路のみを活性化させ、
前記エンジンと前記不揮発性メモリコントローラとは直接接続され、前記エンジンと前記不揮発性メモリコントローラとの間にはいかなる装置も接続されないことを特徴とするシステムオンチップ。

【請求項１８】
前記第１電気的経路は、マルチプレクサ及びデマルチプレクサを介して前記平文データを前記不揮発性メモリコントローラに伝送するための経路を含むことを特徴とする請求項１７に記載のシステムオンチップ。
【請求項１９】
前記第２電気的経路は、前記マルチプレクサを介して前記平文データを前記エンジンに伝送するための経路と、前記デマルチプレクサを介して前記暗号文データを前記不揮発性メモリコントローラに伝送するための経路とを含むことを特徴とする請求項１８に記載のシステムオンチップ。
【請求項２０】
前記エンジンは、前記第２電気的経路を介して前記不揮発性メモリコントローラから受信した暗号文データを復号化することを特徴とする請求項１７に記載のシステムオンチップ。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、システムオンチップ（Ｓｙｓｔｅｍ　Ｏｎ　Ｃｈｉｐ：ＳｏＣ）に係り、より詳細には、暗号化／復号化エンジンとメモリコントローラとが直接接続されたシステムオンチップとその動作方法、及びそれを含むシステムインパッケージに関する。
【背景技術】
【０００２】
メインメモリは、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）が実行するプログラムとＣＰＵで必要なデータを、他の記録媒体、例えば不揮発性メモリ装置から受信する。また、メインメモリは、データを保存するために、データを他の記録媒体、例えば不揮発性メモリ装置に伝送する。
【０００３】
メインメモリと不揮発性メモリ装置との間のデータ送受信過程で、データがプロービング（ｐｒｏｂｉｎｇ）されることを防止するために、データ送受信途中でデータを暗号化する過程が含まれ得る。メインメモリと不揮発性メモリ装置とを含むシステムの性能は、メインメモリと不揮発性メモリ装置との間でデータを送受信するためのデータ伝送経路、即ちデータパスによって決定される。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
本発明は、上記従来技術に鑑みてなされたものであって、本発明の目的は、システムオンチップに含まれる暗号化／復号化エンジンとメモリコントローラとを直接接続することによって、データ伝送経路を減少させるシステムオンチップとその動作方法、及びそれを含むシステムインパッケージを提供することにある。
【課題を解決するための手段】
【０００５】
上記目的を達成するためになされた本発明の一態様によるシステムオンチップ（ＳｏＣ）の動作方法は、前記ＳｏＣに含まれるエンジンによって、暗号キーを用いて平文データを暗号文データに変換する段階と、前記エンジンによって、前記暗号文データを前記ＳｏＣに含まれるメモリコントローラに直接伝送する段階と、を有し、前記メモリコントローラは、不揮発性メモリの動作を制御する。
【０００６】
前記ＳｏＣの動作方法は、前記平文データを暗号文データに変換する段階の前に、前記平文データをＣＰＵの制御によってメインメモリからバスを介してリードする段階を更に含み得る。

【０００７】
上記目的を達成するためになされた本発明の他の態様によるシステムオンチップ（ＳｏＣ）の動作方法は、前記ＳｏＣに含まれるエンジンによって、前記ＳｏＣに含まれるメモリコントローラから暗号文データを直接受信する段階と、前記エンジンによって、暗号キーを用いて前記暗号文データを平文データに変換する段階と、を有し、前記メモリコントローラは、不揮発性メモリの動作を制御する。
【０００８】
前記ＳｏＣの動作方法は、前記暗号文データを平文データに変換する段階の前に、前記平文データを前記ＳｏＣに含まれるＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ）ユニットから前記エンジンに伝送する段階を更に含み得る。
【０００９】
上記目的を達成するためになされた本発明の一態様によるシステムオンチップ（ＳｏＣ）は、暗号キーを用いて、第１平文データ（ｐｌａｉｎ　ｄａｔａ）を第１暗号文データ（ｃｉｐｈｅｒ　ｄａｔａ）に暗号化し、第２暗号文データを第２平文データに復号化する暗号化／復号化エンジンと、前記暗号化／復号化エンジンに直接接続され、前記第１暗号文データを不揮発性メモリに伝送し、該不揮発性メモリから前記第２暗号文データを受信するメモリコントローラと、を有する。
【００１０】
前記ＳｏＣは、前記暗号キーを保存するワンタイムプログラマブル（ＯＴＰ）メモリを更に含み得る。
前記ＳｏＣは、前記ＳｏＣの外部にある装置から受信した前記第１平文データを前記暗号化／復号化エンジンに伝送し、該暗号化／復号化エンジンから受信した前記第２平文データを前記装置に伝送するＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ）ユニットを更に含み得る。
前記ＳｏＣは、前記ＳｏＣの外部にある装置と前記暗号化／復号化エンジンとの間で前記第１平文データ又は前記第２平文データの伝送を制御するＣＰＵを更に含み得る。
【００１１】
上記目的を達成するためになされた本発明の一態様によるシステムインパッケージ（Ｓｙｓｔｅｍ－ｉｎ　Ｐａｋａｇｅ）は、上記システムオンチップ（ＳｏＣ）と、前記ＳｏＣの制御によって、不揮発性メモリとデータを通信する装置と、を備える。
【００１２】
上記目的を達成するためになされた本発明の他の態様によるシステムインパッケージは、上記ＳｏＣと、不揮発性メモリと、前記ＳｏＣの制御によって、前記不揮発性メモリとデータを通信する装置と、を備える。
【００１３】
上記目的を達成するためになされた本発明の他の態様によるシステムオンチップ（ＳｏＣ）は、不揮発性メモリを制御するメモリコントローラと、前記メモリコントローラに直接接続され、データを暗号化又は復号化する暗号化／復号化エンジン（ｅｎｇｉｎｅ）と、を有し、前記ＳｏＣは、前記ＳｏＣの外部にある装置と前記不揮発性メモリとの間でデータの伝送を制御し、前記メモリコントローラ及び前記暗号化／復号化エンジンは、前記データを伝送するための第１データパスに該当する。
【００１４】
前記ＳｏＣは、暗号キーを保存するためのワンタイムプログラマブル（ＯＴＰ）メモリを更に含み、前記暗号化／復号化エンジンは、前記ＯＴＰメモリに保存された暗号キーを用いて、前記データを暗号化又は復号化することができる。
前記第１データパスは、前記装置から受信した前記データを前記暗号化／復号化エンジンに伝送し、該暗号化／復号化エンジンから受信した前記データを前記装置に伝送するＤＭＡ（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ）ユニットを更に含み得る。
前記ＤＭＡユニットは、前記暗号化／復号化エンジンに直接接続され得る。
前記ＳｏＣは、暗号化されていない前記データを伝送する第２データパスを更に含み得

る。
前記ＳｏＣは、選択信号に基づいて、前記第１データパス及び前記第２データパスのうちの何れか１つを選択するための選択回路を更に含み得る。
【００１５】
上記目的を達成するためになされた本発明の更に他の態様によるシステムオンチップ（ＳｏＣ）は、データバスと、前記データバスに平文データを出力するメインメモリコントローラと、前記データバスから受信した前記平文データを、キー（ｋｅｙ）を使って暗号文データに暗号化するエンジンと、不揮発性メモリコントローラと、前記エンジンをバイパス（ｂｙｐａｓｓ）して前記データバスを前記不揮発性メモリコントローラに接続させる第１電気的経路と、前記エンジンを介して前記データバスを前記不揮発性メモリコントローラに接続させる第２電気的経路と、を有し、前記ＳｏＣは、非セキュリティモード（Ｎｏｎ－Ｓｅｃｕｒｅ　Ｍｏｄｅ）で、前記平文データを前記データバスから前記不揮発性メモリコントローラに伝送するために前記第１電気的経路のみを活性化させ、前記ＳｏＣは、セキュリティモードで、前記平文データを前記エンジンに伝送し、該エンジンから受信した前記暗号文データを前記不揮発性メモリコントローラに伝送するために前記第２電気的経路のみを活性化させる。
【００１６】
前記第１電気的経路は、マルチプレクサ（ｍｕｌｔｉｐｌｅｘｅｒ）とデマルチプレクサ（ｄｅｍｕｌｔｉｐｌｅｘｅｒ）とを介して前記平文データを前記不揮発性メモリコントローラに伝送するための経路を含み得る。
前記第２電気的経路は、前記マルチプレクサを介して前記平文データを前記エンジンに伝送するための経路と、前記デマルチプレクサを介して前記暗号文データを前記不揮発性メモリコントローラに伝送するための経路とを含み得る。
前記エンジンは、前記第２電気的経路を介して前記不揮発性メモリコントローラから受信した暗号文データを復号化することができる。

【発明の効果】
【００１７】
本発明のシステムオンチップ（ＳｏＣ）によれば、ＳｏＣの内部でデータを暗号化するため、ＳｏＣの外部からデータをプロービングすることができない。ＳｏＣは、暗号化に必要な暗号キーをＳｏＣの内部に保存するため、暗号キーの露出を防止することができる。
また、ＳｏＣは、暗号化に必要な暗号キーをソフトウェアでアクセスすることができないため、ハッキングによって暗号キーが流出することを防止することができる。ＳｏＣのソフトウェアは、暗号化に介入しないので、ソフトウェアの負担を増加させない。
また、ＳｏＣは、ＳｏＣの内部に具現された暗号化／復号化エンジンとメモリコントローラとを直接接続することによって、ＳｏＣの内部のデータ伝送経路を減少させることができる。従って、ＳｏＣの性能が向上する。
【図面の簡単な説明】
【００１８】
【図１】本発明の一実施形態によるシステムオンチップを含むシステムのブロック図である。
【図２】図１に示したシステムオンチップの一実施形態によるブロック図である。
【図３】図２に示した暗号化／復号化エンジンに暗号キーを入力するセキュリティモードを説明するための概念図である。
【図４】図１に示したシステムオンチップの他の実施形態によるブロック図である。
【図５】図１に示したシステムオンチップの更に他の実施形態によるブロック図である。
【図６】図１に示したシステムオンチップの更に他の実施形態によるブロック図である。
【図７】図１に示したシステムオンチップの更に他の実施形態によるブロック図である。

【図８】図７に示した選択回路及び暗号化／復号化エンジンのブロック図である。
【図９】図１に示したシステムオンチップの更に他の実施形態によるブロック図である。
【図１０】本発明の一実施形態によるシステムオンチップの動作方法を説明するフローチャートである。
【図１１】本発明の他の実施形態によるシステムオンチップの動作方法を説明するフローチャートである。
【図１２】本発明の更に他の実施形態によるシステムオンチップの動作方法を説明するフローチャートである。
【図１３】本発明の更に他の実施形態によるシステムオンチップの動作方法を説明するフローチャートである。
【図１４】図１に示したシステムを含むデータ処理装置の一実施形態によるブロック図である。
【図１５】図１に示したシステムを含むデータ処理装置の他の実施形態によるブロック図である。
【図１６】図１に示したシステムを含むデータ処理装置の更に他の実施形態によるブロック図である。
【図１７】図１に示したシステムオンチップを含むシステムインパッケージ及び不揮発性メモリ装置のブロック図である。
【図１８】図１に示したシステムオンチップを含むシステムインパッケージの他の実施形態によるブロック図である。
【発明を実施するための形態】
【００１９】
本明細書で“直接伝送する”と言及した場合には、伝送中に他の構成による処理過程を経ずにデータを伝送することを意味する。本明細書で“直接接続される”と言及した場合には、中間に他の構成を置かずに配線（ｗｉｒｉｎｇ）、マルチプレクサ、及び／又はデマルチプレクサなどを介して接続されることを意味する。
【００２０】
以下、本発明を実施するための形態の具体例を、図面を参照しながら詳細に説明する。
【００２１】
図１は、本発明の一実施形態によるシステムオンチップを含むシステムのブロック図である。図１を参照すると、システム１０は、システムオンチップ（ＳｏＣ）１００、不揮発性メモリ装置２００、及びメインメモリ３００を含む。実施形態として、システム１０は、ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）、データサーバ（Ｄａｔａ Ｓｅｒｖｅｒ）、又は携帯用電子装置として具現可能である。
【００２２】
例えば、携帯用電子装置は、ラップトップコンピュータ、携帯電話、スマートフォン、タブレットＰＣ、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ）、ＥＤＡ（Ｅｎｔｅｒｐｒｉｓｅ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ）、デジタルスチルカメラ、デジタルビデオカメラ、ＰＭＰ（Ｐｏｒｔａｂｌｅ Ｍｕｌｔｉｍｅｄｉａ Ｐｌａｙｅｒ）、ＰＤＮ（Ｐｅｒｓｏｎａｌ Ｎａｖｉｇａｔｉｏｎ Ｄｅｖｉｃｅ又はＰｏｒｔａｂｌｅ Ｎａｖｉｇａｔｉｏｎ Ｄｅｖｉｃｅ）、携帯用ゲームコンソール、又は電子ブックなどとして具現可能である。
【００２３】
ＳｏＣ１００は、不揮発性メモリ装置２００とメインメモリ３００との間のデータの送受信を制御する。ＳｏＣ１００の構成と動作は、図２、及び図４～図９を参照して詳しく説明する。
【００２４】
不揮発性メモリ装置２００は、各種のプログラム及びデータを保存する。実施形態として、不揮発性メモリ装置２００は、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ）、フラッシ

ュメモリ、ＭＲＡＭ（Ｍａｇｎｅｔｉｃ　ＲＡＭ）、スピン注入トルクＭＲＡＭ（Ｓｐｉｎ－Ｔｒａｎｓｆｅｒ　Ｔｏｒｑｕｅ　ＭＲＡＭ）、Ｃｏｎｄｕｃｔｉｖｅ　Ｂｒｉｄｇｉｎｇ　ＲＡＭ（ＣＢＲＡＭ）：ＦｅＲＡＭ（Ｆｅｒｒｏｅｌｅｃｔｒｉｃ　ＲＡＭ）、ＰＲＡＭ（Ｐｈａｓｅ　ｃｈａｎｇｅ　ＲＡＭ）、抵抗メモリ（Ｒｅｓｉｓｔｉｖｅ　ＲＡＭ：ＲｅＲＡＭ）、ナノチューブＲｅＲＡＭ（Ｎａｎｏｔｕｂｅ　ＲｅＲＡＭ）、ポリマーＲＡＭ（Ｐｏｌｙｍｅｒ　ＲＡＭ：ＰｏＲＡＭ）、ナノ浮遊ゲートメモリ（Ｎａｎｏ　Ｆｌｏａｔｉｎｇ　Ｇａｔｅ　Ｍｅｍｏｒｙ：ＮＦＧＭ）、ホログラフィックメモリ（Ｈｏｌｏｇｒａｐｈｉｃ　Ｍｅｍｏｒｙ）、分子電子メモリ素子（Ｍｏｌｅｃｕｌａｒ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｍｅｍｏｒｙ　Ｄｅｖｉｃｅ）、又は絶縁抵抗変化メモリ（Ｉｎｓｕｌａｔｏｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｃｈａｎｇｅ　Ｍｅｍｏｒｙ）などとして具現可能であるが、本発明の範囲はこれに限定されるものではない。

【００２５】

メインメモリ３００は、ＳｏＣ１００で実行されるプログラムとＳｏＣ１００で必要なデータとをＳｏＣ１００を介して不揮発性メモリ装置２００から受信する。メインメモリ３００は、保存されるデータを、ＳｏＣ１００を介して不揮発性メモリ装置２００に伝送する。実施形態として、メインメモリ３００は、揮発性メモリであるＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、例えばＤＲＡＭ（Ｄｙｎａｍｉｃ　ＲＡＭ）又はＳＲＡＭ（Ｓｔａｔｉｃ　ＲＡＭ）として具現可能であるが、本発明の範囲はこれに限定されるものではない。

【００２６】

図２は、図１に示したシステムオンチップの一実施形態によるブロック図である。図２を参照すると、図１のＳｏＣ１００の一実施形態によるＳｏＣ１００Ａは、バス（ｂｕｓ）１１０、ＣＰＵ１２０、メモリコントローラ１３０、不揮発性メモリコントローラ１４０、及び暗号化／復号化エンジン１５０を含む。

【００２７】

ＣＰＵ１２０は、バス１１０に接続され、ＳｏＣ１００Ａの全般的な動作を制御する。メモリコントローラ１３０は、メインメモリ３００の動作、例えばリード（ｒｅａｄ）動作又はライト（ｗｒｉｔｅ）動作を制御する。メモリコントローラ１３０は、バス１１０に接続される。

【００２８】

不揮発性メモリコントローラ１４０は、不揮発性メモリ装置２００のデータアクセス動作、例えばリード動作、ライト動作、プログラム（ｐｒｏｇｒａｍ）動作、又はイレーズ（ｅｒａｓｅ）動作などを制御する。

【００２９】

暗号化／復号化エンジン１５０は、メインメモリ３００からメモリコントローラ１３０とバス１１０とを介して伝送された平文データを暗号文データに変換、即ち暗号化する。暗号化／復号化エンジン１５０は、暗号文データを、バス１１０を経由せずに不揮発性メモリコントローラ１４０に直接、例えばオンザフライ（ｏｎ－ｔｈｅ－ｆｌｙ）で伝送する。

【００３０】

暗号化／復号化エンジン１５０は、不揮発性メモリコントローラ１４０から出力された暗号文データを、バス１１０を経由せずに直接、例えばオンザフライで受信する。暗号化／復号化エンジン１５０は、暗号文データを平文データに変換、例えば復号化する。

【００３１】

暗号化／復号化エンジン１５０の暗号化過程又は復号化過程には、暗号キーが使われる。暗号化／復号化エンジン１５０は、暗号キーを保存するための記憶媒体（図示せず）を含む。他の実施形態として、暗号キーは、セキュリティモード（Ｓｅｃｕｒｅ　Ｍｏｄｅ）でのみ記憶媒体にアクセス可能になるように設定し得る。セキュリティモードは、図３を参照して詳しく説明する。

【００３２】

暗号化／復号化エンジン１５０は、データを所定サイズ、例えば６４ビット、１２８ビット、又は２５６ビットのブロック（ｂｌｏｃｋ）単位で暗号化又は復号化する。この場合、暗号化又は復号化のための暗号キーとアルゴリズム（ａｌｇｏｒｉｔｈｍ）は、ブロック単位で適用可能である。

【００３３】

暗号化アルゴリズムは、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）アルゴリズム又はＡＥＳ（Ａｄｖａｎｃｅｄ　ＥｎｃｒｙｐｔｉｏｎＳｔａｎｄａｒｄ）アルゴリズムであり得るが、これに限定されるものではない。実施形態として、暗号化／復号化エンジン１５０がデータをブロック単位で変換、例えば暗号化又は復号化する方法を決定する暗号モードは、ＥＣＢ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｄｅ　Ｂｏｏｋ）モード、ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モード、ＰＣＢＣ（Ｐｒｏｐａｇａｔｉｎｇ　Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モード、又はＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄ　Ｂａｃｋ）モードであり得るが、本発明の範囲はこれに限定されるものではない。

【００３４】

データが、不揮発性メモリ装置２００にライトされる時のライトデータパス（ｗｒｉｔｅ　ｄａｔａ　ｐａｔｈ：ＷＰ）を説明すると、メインメモリ３００から出力された平文データがメモリコントローラ１３０とバス１１０とを介してＣＰＵ１２０に伝送された後、平文データは、ＣＰＵ１２０からバス１１０を介して暗号化／復号化エンジン１５０に伝送される。即ち、ＣＰＵ１２０の制御によって、平文データは、暗号化／復号化エンジン１５０に伝送される。

【００３５】

暗号化／復号化エンジン１５０は、暗号キーを用いて平文データを暗号文データに変換する。暗号文データは、不揮発性メモリコントローラ１４０を介して不揮発性メモリ装置２００に伝送される。

【００３６】

データが、不揮発性メモリ装置２００からリードされる時のリードデータパス（ｒｅａｄ　ｄａｔａ　ｐａｔｈ：ＲＰ）を説明すると、不揮発性メモリ装置２００から出力された暗号文データは、不揮発性メモリコントローラ１４０を介して暗号化／復号化エンジン１５０に直接伝送される。

【００３７】

暗号化／復号化エンジン１５０は、暗号キーを用いて暗号文データを平文データに変換する。平文データがバス１１０を介してＣＰＵ１２０に伝送された後、平文データは、ＣＰＵ１２０からバス１１０とメモリコントローラ１３０とを介してメインメモリ３００に伝送される。即ち、ＣＰＵ１２０の制御によって、平文データは、バス１１０とメモリコントローラ１３０とを介してメインメモリ３００に伝送される。

【００３８】

図３は、図２に示した暗号化／復号化エンジンに暗号キーを入力するセキュリティモードを説明するための概念図である。図２及び図３を参照すると、オペレーティングシステム（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ：ＯＳ）は、ハードウェアを管理し、応用プログラム（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ）を実行させるために、ハードウェアに設けられる。

【００３９】

セキュリティ（Ｓｅｃｕｒｅ）ＯＳは、セキュリティが要求されるセキュリティ応用プログラム（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ）を実行させるために、一般的なオペレーティングシステム（ＯＳ）とは別個にハードウェアに設けられる。実施形態として、セキュリティＯＳは、所定時間内に実行が完了しなければならない応用プログラム、例えば、セキュリティ応用プログラムを実行させるために、リアルタイムオペレーティングシステム（Ｒｅａｌ　Ｔｉｍｅ　Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ：ＲＴＯＳ）として具現可能である。

【００４０】
非セキュリティモードとは、オペレーティングシステム（ＯＳ）によって応用プログラムが実行される場合を意味し、セキュリティモードとは、セキュリティＯＳによってセキュリティ応用プログラムが実行される場合を意味する。セキュリティモードでセキュリティ応用プログラムが実行されることによって、ＣＰＵ１２０は、暗号化／復号化エンジン１５０に暗号キーを入力するか、或いは暗号化／復号化エンジン１５０の内部又は外部に保存されている暗号キーにアクセスする。実施形態として、セキュリティモードでセキュリティ応用プログラムが実行されることによって、暗号キーは、変更又は再設定され得る。
【００４１】
図４は、図１に示したシステムオンチップの他の実施形態によるブロック図である。図１～図４を参照すると、図１のＳｏＣ１００の他の実施形態によるＳｏＣ１００Ｂは、バス１１０、ＣＰＵ１２０、メモリコントローラ１３０、不揮発性メモリコントローラ１４０、暗号化／復号化エンジン１５０、及び第１ＯＴＰメモリ（Ｏｎｅ－Ｔｉｍｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｍｅｍｏｒｙ）１６０を含む。第１ＯＴＰメモリ１６０は、暗号化／復号化エンジン１５０の暗号化過程又は復号化過程で使われる暗号キーを保存する。実施形態として、第１ＯＴＰメモリ１６０は、ヒューズ（ｆｕｓｅ）、アンチヒューズ（ａｎｔｉ－ｆｕｓｅ）、又は電子ヒューズとして具現可能である。
【００４２】
図４のＳｏＣ１００Ｂは、図２のＳｏＣ１００Ａとは異なって、セキュリティモードでセキュリティ応用プログラムが実行されても、ＣＰＵ１２０は、第１ＯＴＰメモリ１６０に保存された暗号キーにアクセス、例えばリード、ライト、又はイレーズできないように具現される。
【００４３】
データの暗号化又は復号化に使われる暗号キーが、第１ＯＴＰメモリ１６０から暗号化／復号化エンジン１５０に供給されることを除けば、図４のＳｏＣ１００Ｂのライトデータパスｗｐ及びリードデータパスＲＰのそれぞれは、図２のＳｏＣ１００Ａのライトデータパスｗｐ及びリードデータパスＲＰのそれぞれと実質的に同一である。
【００４４】
図５は、図１に示したシステムオンチップの更に他の実施形態によるブロック図である。図１及び図５を参照すると、図１のＳｏＣ１００の更に他の実施形態によるＳｏＣ１００Ｃは、バス１１０、ＣＰＵ１２０、メモリコントローラ１３０、不揮発性メモリコントローラ１４０、暗号化／復号化エンジン１５０、第１ＯＴＰメモリ１６０、及びＤＭＡユニット（Ｄｉｒｅｃｔ　Ｍｅｍｏｒｙ　Ａｃｃｅｓｓ　Ｕｎｉｔ）１７０を含む。
【００４５】
ＤＭＡユニット１７０は、ＣＰＵ１２０を介さずに必要な構成（例えば、１３０、１４０、又は１５０）を介してメインメモリ３００又は不揮発性メモリ装置２００にアクセスすることができる。この際、ＤＭＡユニット１７０は、バス１１０に接続される。
【００４６】
不揮発性メモリ装置２００が、データをライトする時のライトデータパスｗｐを説明すると、メインメモリ３００から出力された平文データは、メモリコントローラ１３０とバス１１０とを介してＤＭＡユニット１７０に伝送される。平文データは、ＤＭＡユニット１７０からバス１１０を介して暗号化／復号化エンジン１５０に伝送される。
【００４７】
暗号化／復号化エンジン１５０は、平文データを暗号文データに変換する。暗号化／復号化エンジン１５０から出力された暗号文データは、直接不揮発性メモリコントローラ１４０に伝送された後、不揮発性メモリ装置２００に伝送される。即ち、暗号化／復号化エンジン１５０は、暗号文データを不揮発性メモリコントローラ１４０に直接、例えばオンザフライで伝送する。
【００４８】

データが、不揮発性メモリ装置２００からリードされる時のリードデータパスＲＰを説明すると、不揮発性メモリ装置２００から出力された暗号文データは、不揮発性メモリコントローラ１４０を介して暗号化／復号化エンジン１５０に伝送される。即ち、暗号化／復号化エンジン１５０は、不揮発性メモリコントローラ１４０から出力された暗号文データを直接、例えばオンザフライで受信する。

【００４９】

暗号化／復号化エンジン１５０は、暗号文データを平文データに変換する。平文データは、バス１１０を介してＤＭＡユニット１７０に伝送される。平文データは、ＤＭＡユニット１７０からバス１１０とメモリコントローラ１３０とを介してメインメモリ３００に伝送される。

【００５０】

図６は、図１に示したシステムオンチップの更に他の実施形態によるブロック図である。図１及び図６を参照すると、図１のＳｏＣ１００の更に他の実施形態によるＳｏＣ１００Ｄは、バス１１０、ＣＰＵ１２０、メモリコントローラ１３０、不揮発性メモリコントローラ１４０、暗号化／復号化エンジン１５０、第１ＯＴＰメモリ１６０、及びＤＭＡユニット１７０を含む。

【００５１】

ＤＭＡユニット１７０は、バス１１０と暗号化／復号化エンジン１５０との間に接続される。データは、ＤＭＡユニット１７０と暗号化／復号化エンジン１５０との間で、オンザフライで伝送される。

【００５２】

不揮発性メモリ装置２００が、データをライトする時のライトデータパスＷＰを説明すると、メインメモリ３００から出力された平文データは、メモリコントローラ１３０、バス１１０、及びＤＭＡユニット１７０を介して暗号化／復号化エンジン１５０に伝送される。

【００５３】

暗号化／復号化エンジン１５０は、平文データを暗号文データに変換、例えば暗号化する。暗号文データは、不揮発性メモリコントローラ１４０を介して不揮発性メモリ装置２００に伝送される。この際、暗号化／復号化エンジン１５０は、不揮発性メモリコントローラ１４０に暗号文データを直接、例えばオンザフライで伝送する。

【００５４】

不揮発性メモリ装置２００が、データをリードする時のリードデータパスＲＰを説明すると、不揮発性メモリ装置２００から出力された暗号文データは、不揮発性メモリコントローラ１４０を介して暗号化／復号化エンジン１５０に伝送される。この際、暗号化／復号化エンジン１５０は、不揮発性メモリコントローラ１４０から暗号文データを直接、例えばオンザフライで受信する。

【００５５】

暗号化／復号化エンジン１５０は、暗号文データを平文データに変換、例えば復号化する。平文データは、ＤＭＡユニット１７０、バス１１０、及びメモリコントローラ１３０を介してメインメモリ３００に伝送される。

【００５６】

図７は、図１に示したシステムオンチップの更に他の実施形態によるブロック図である。図１、図３、及び図７を参照すると、図１のＳｏＣ１００の更に他の実施形態によるＳｏＣ１００Ｅは、バス１１０、ＣＰＵ１２０、メモリコントローラ１３０、不揮発性メモリコントローラ１４０、暗号化／復号化エンジン１５０、第１ＯＴＰメモリ１６０、ＤＭＡユニット１７０、レジスタ１８０、及び選択回路１９０を含む。

【００５７】

レジスタ１８０は、バス１１０に接続される。レジスタ１８０は、選択信号ＳＥＬを発生する選択信号発生器として作動する。レジスタ１８０は、ＣＰＵ１２０がセキュリティ応用プログラムを実行するか否か、即ちセキュリティモードを指示する指示信号に基づい

て選択信号ＳＥＬを変更する。指示信号は、ＣＰＵ１２０から出力される。

【００５８】

例えば、セキュリティモードで、指示信号のロジックレベルは、ハイ（ｈｉｇｈ）であり、非セキュリティモードで、指示信号のロジックレベルは、ロー（ｌｏｗ）である。選択回路１９０は、レジスタ１８０から出力された選択信号ＳＥＬによってデータパスを選択する。選択回路１９０の構造と動作は、図８を参照して詳しく説明する。

【００５９】

図８は、図７に示した選択回路及び暗号化／復号化エンジンのブロック図である。図３、図７、及び図８を参照すると、選択回路１９０は、第１選択器１９２と第２選択器１９４とを含む。

【００６０】

第１選択器１９２は、デマルチプレクサとして具現可能であり、第２選択器１９４は、マルチプレクサとして具現可能である。

【００６１】

選択回路１９０は、選択信号ＳＥＬのロジックレベルがハイである時、データが暗号化／復号化エンジン１５０を含むデータパスを選択する。ＣＰＵ１２０がセキュリティ応用プログラムを実行する時、即ちセキュリティモードである時、選択回路１９０は、暗号化／復号化エンジン１５０を含むデータパスを選択する。しかし、選択回路１９０は、選択信号ＳＥＬのロジックレベルがローである時、暗号化／復号化エンジン１５０を含まないデータパス、即ちバイパスを選択することができる。実施形態として、ＣＰＵ１２０が一般応用プログラムを実行する時、即ち非セキュリティモードである時、選択回路１９０は、暗号化／復号化エンジン１５０を含まないデータパス、即ちバイパスを選択する。

【００６２】

図９は、図１に示したシステムオンチップの更に他の実施形態によるブロック図である。図１、図８、及び図９を参照すると、図１のＳｏＣ１００の更に他の実施形態によるＳｏＣ１００Ｆは、バス１１０、ＣＰＵ１２０、メモリコントローラ１３０、不揮発性メモリコントローラ１４０、暗号化／復号化エンジン１５０、第１ＯＴＰメモリ１６０、ＤＭＡユニット１７０、第２ＯＴＰメモリ１８２、及び選択回路１９０を含む。

【００６３】

第２ＯＴＰメモリ１８２は、選択信号ＳＥＬを発生する選択信号発生器として作動する。第２ＯＴＰメモリ１８２は、１つのレベル、例えばハイレベルを有する選択信号ＳＥＬを発生するようにプログラムされる。この際、選択回路１９０は、暗号化／復号化エンジン１５０を含むデータパスのみを選択する。

【００６４】

図１０は、本発明の一実施形態によるシステムオンチップの動作方法を説明するフローチャートである。図２、図４～図７、図９、及び図１０を参照すると、暗号化／復号化エンジン１５０は、暗号キーを用いて平文データを暗号文データに変換、即ち暗号化する（ステップＳ１０）。

【００６５】

暗号化／復号化エンジン１５０は、暗号化データを不揮発性メモリコントローラ１４０に直接、例えばオンザフライで伝送する（ステップＳ１２）。従って、暗号キーと暗号化データは、ＳｏＣ１００の内部に存在するため、プロービングに強い効果がある。

【００６６】

図１１は、本発明の他の実施形態によるシステムオンチップの動作方法を説明するフローチャートである。図５～図７、図９、及び図１１を参照すると、暗号化／復号化エンジン１５０は、平文データをＤＭＡユニット１７０から受信する（ステップＳ２０）。暗号化／復号化エンジン１５０は、平文データをＤＭＡユニット１７０から直接、例えばオンザフライで受信する。

【００６７】

図１２は、本発明の更に他の実施形態によるシステムオンチップの動作方法を説明する

フローチャートである。図２、図４～図７、図９、及び図１２を参照すると、暗号化／復号化エンジン１５０は、不揮発性メモリコントローラ１４０から暗号文データを直接、例えばオンザフライで受信する（ステップＳ３０）。暗号化／復号化エンジン１５０は、暗号文データを平文データに復号化する（ステップＳ３２）。

【００６８】

図１３は、本発明の更に他の実施形態によるシステムオンチップの動作方法を説明するフローチャートである。図５～図７、図９、及び図１３を参照すると、暗号化／復号化エンジン１５０は、平文データをＤＭＡユニット１７０に伝送する（ステップＳ３４）。暗号化／復号化エンジン１５０は、平文データをＤＭＡユニット１７０に直接、例えばオンザフライで伝送する。

【００６９】

図１４は、図１に示したシステムを含むデータ処理装置の一実施形態によるブロック図である。図１及び図１４を参照すると、データ処理装置４００は、ＰＣ又はデータサーバとして具現可能である。

【００７０】

データ処理装置４００は、プロセッサ１００ａ、保存装置２００ａ、メモリ３００ａ、パワーソース４１０、入出力ポート４２０、拡張カード４３０、ネットワーク装置４４０、及びディスプレイ４５０を含む。実施形態として、データ処理装置４００は、カメラモジュール４６０を更に含み得る。

【００７１】

プロセッサ１００ａは、図１に示したＳｏＣ１００を意味する。プロセッサ１００ａは、マルチコア（Ｍｕｌｔｉ－Ｃｏｒｅ）プロセッサであり得る。実施形態として、プロセッサ１００ａは、図１に示したＳｏＣ１００を含む。プロセッサ１００ａは、構成要素（２００ａ、３００ａ、及び４１０～４６０）のうちの少なくとも１つの動作を制御する。

【００７２】

保存装置２００ａは、図１に示した不揮発性メモリ装置２００を意味する。保存装置２００ａは、ハードディスクドライブ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）又はＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）として具現可能である。

【００７３】

メモリ３００ａは、図１に示したメインメモリ３００を意味する。メモリ３００ａは、揮発性メモリ又は不揮発性メモリとして具現可能である。メモリ３００ａに対するデータアクセス動作、例えばリード動作、ライト動作（又は、プログラム動作）、又はイレーズ動作を制御するメモリコントローラ（図２の１４０）は、プロセッサ１００に集積又は内蔵され得る。

【００７４】

パワーソース４１０は、構成要素（１００ａ、２００ａ、３００ａ及び４２０～４６０）のうちの少なくとも１つに動作電圧を供給する。

【００７５】

入出力ポート４２０は、保存装置２００ａにデータを伝送するか、保存装置２００ａから出力されたデータを外部装置に伝送するポートを意味する。例えば、入出力ポート４２０は、コンピュータマウスのようなポインティング装置（ｐｏｉｎｔｉｎｇ　ｄｅｖｉｃｅ）を接続するためのポート、プリンターを接続するためのポート、又はＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ドライブを接続するためのポートである。

【００７６】

拡張カード４３０は、ＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）カード又はMMC（ＭｕｌｔｉＭｅｄｉａ　Ｃａｒｄ）として具現可能である。実施形態として、拡張カード４３０は、ＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）カード又はＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）カードであり得る。

【００７７】

ネットワーク装置４４０は、保存装置２００ａを有線ネットワーク又は無線ネットワークに接続させる装置を意味する。

【００７８】

ディスプレイ４５０は、保存装置２００ａ、メモリ３００ａ、入出力ポート４２０、拡張カード４３０、又はネットワーク装置４４０から出力されたデータを表示する。カメラモジュール４６０は、光学イメージを電気的なイメージに変換するモジュールを意味する。従って、カメラモジュール４６０から出力された電気的なイメージは、保存装置２００ａ、メモリ３００ａ、又は拡張カード４３０に保存される。また、カメラモジュール４６０から出力された電気的なイメージは、ディスプレイ４５０を通じて表示される。

【００７９】

図１５は、図１に示したシステムを含むデータ処理装置の他の実施形態によるブロック図である。図１及び図１５を参照すると、データ処理装置５００は、ラップトップ（ｌａｐｔｏｐ）コンピュータとして具現可能である。

【００８０】

図１６は、図１に示したシステムを含むデータ処理装置の更に他の実施形態によるブロック図である。図１及び図１６を参照すると、データ処理装置６００は、携帯用装置として具現可能である。携帯用装置６００は、携帯電話、スマートフォン、タブレットＰＣ、ＰＤＡ、ＥＤＡ、デジタルスチルカメラ、デジタルビデオカメラ、ＰＭＰ、ＰＤＮ、携帯用ゲームコンソール、又は電子ブックとして具現可能である。

【００８１】

図１７は、図１に示したシステムオンチップを含むシステムインパッケージ及び不揮発性メモリ装置のブロック図であり、図１８は、図１に示したシステムオンチップを含むシステムインパッケージの他の実施形態によるブロック図である。図１及び図１７を参照すると、ＳｏＣ１００及びメインメモリ３００は、システムインパッケージ（ＳｉＰ）７００にパッケージングされる。図１及び図１８を参照すると、ＳｏＣ１００、不揮発性メモリ装置２００、及びメインメモリ３００は、ＳｉＰ７００′にパッケージングされる。

【００８２】

以上、本発明の実施形態について図面を参照しながら詳細に説明したが、本発明は、上述の実施形態に限定されるものではなく、本発明の技術的範囲から逸脱しない範囲内で多様に変更実施することが可能である。

【符号の説明】

【００８３】

１０　システム

１００、１００Ａ、１００Ｂ、１００Ｃ、１００Ｄ、１００Ｅ、１００Ｆ　システムオンチップ（ＳｏＣ）

１００ａ　プロセッサ

１１０　バス

１２０　ＣＰＵ

１３０　メモリコントローラ

１４０　不揮発性メモリコントローラ

１５０　暗号化／復号化エンジン

１６０　第１ＯＴＰメモリ

１７０　ＤＭＡユニット

１８０　レジスタ

１８２　第２ＯＴＰメモリ

１９０　選択回路

１９２　第１選択器

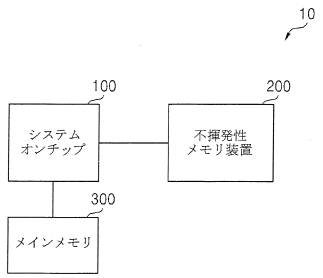
１９４　第２選択器

２００　不揮発性メモリ装置

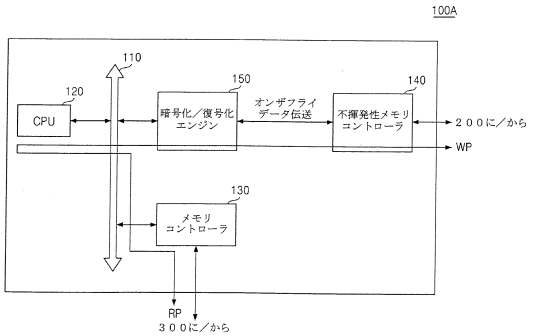
２００ａ　保存装置

３００　メインメモリ
３００ａ　メモリ
４００、５００、６００　データ処理装置
４１０、５１０、６１０　パワーソース
４２０、５２０、６２０　入出力ポート
４３０、５３０、６３０　拡張カード
４４０、５４０、６４０　ネットワーク装置
４５０、５５０、６５０　ディスプレイ
４６０、５６０、６６０　カメラモジュール
７００、７００′　システムインパッケージ（ＳｉＰ）

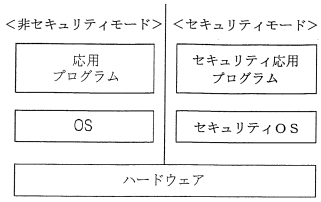
【図１】



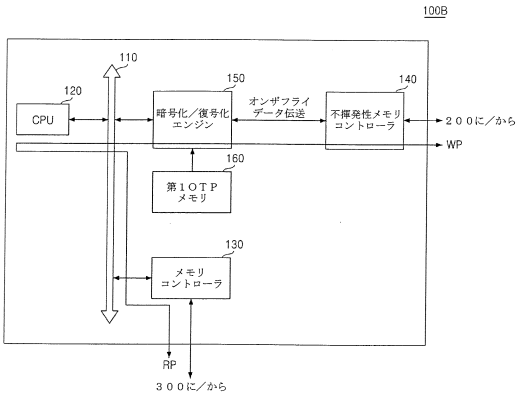
【図２】



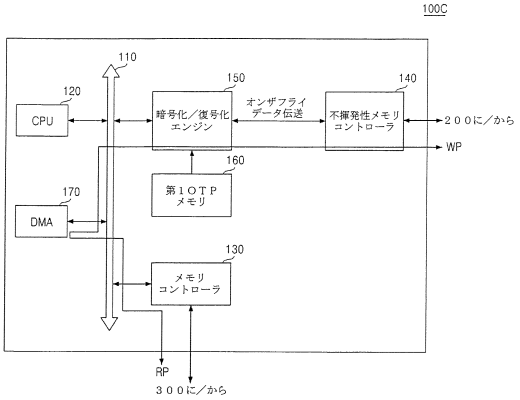
【図３】



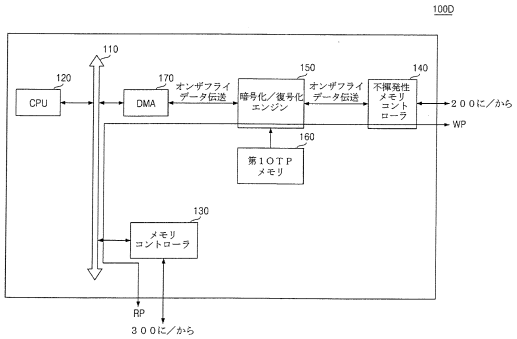
【図４】



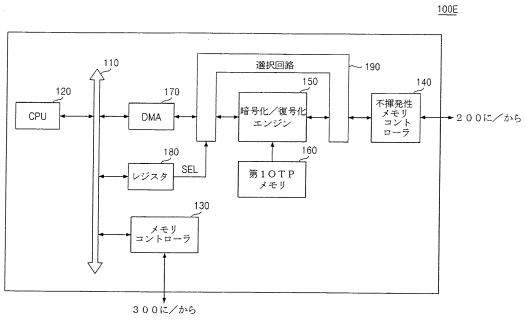
【図５】



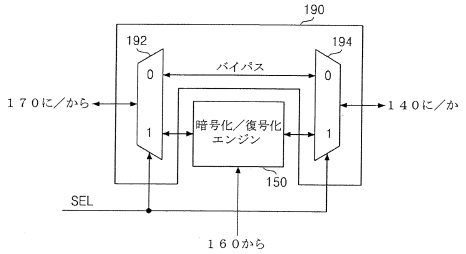
【図６】



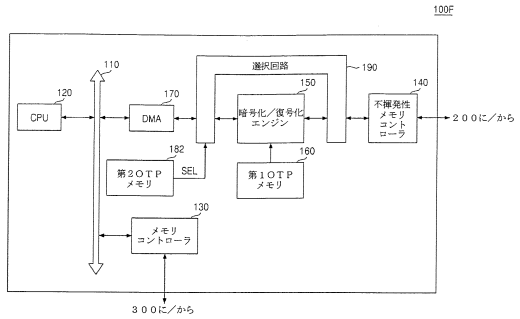
【図７】



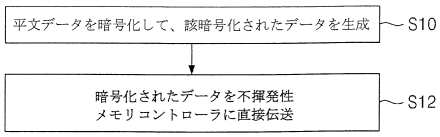
【図８】



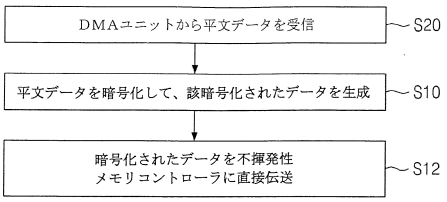
【図９】



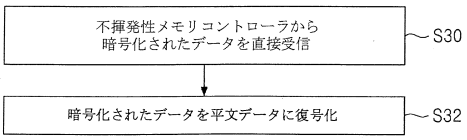
【図１０】



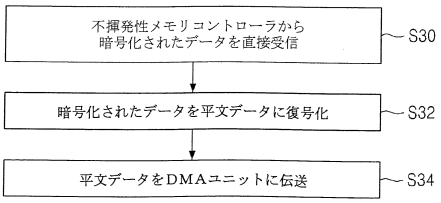
【図１１】



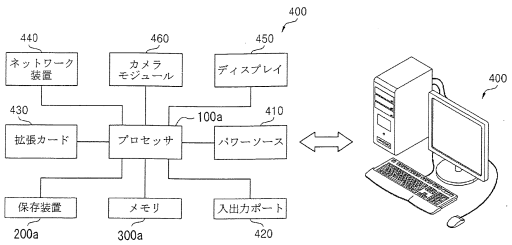
【図１２】



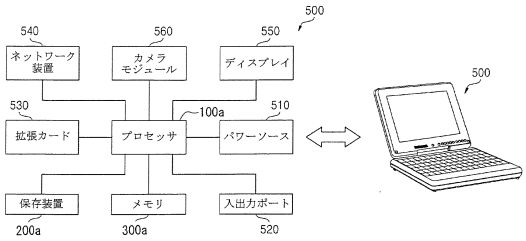
【図１３】



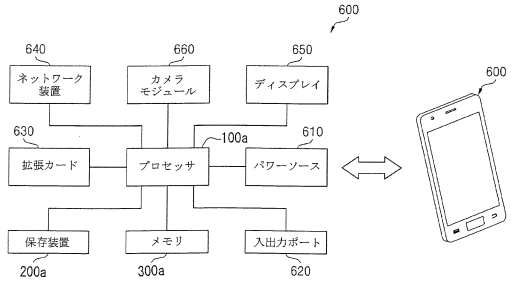
【図１４】



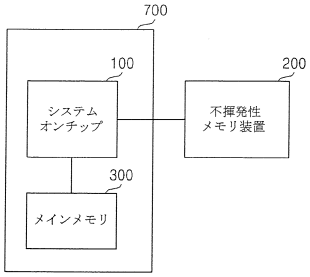
【図１５】



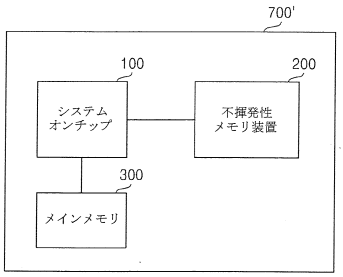
【図１６】



【図１７】



【図１８】



フロントページの続き

(72)発明者　崔　弘　默
大韓民国　京畿道　富川市　遠美区　上二洞　ハヤンマウル　２６１８棟　２１０３号
(72)発明者　朴　相　ヒョン
大韓民国　ソウル特別市　麻浦区　城山洞　６０４番地　城山二次イーピョンハンセサンアパート
２０１棟　１２０２号

審査官　宮司　卓佳

(56)参考文献　特開２０１２－００４６６１（ＪＰ，Ａ）
特表２０１０－５２５４３５（ＪＰ，Ａ）
特開２００３－１９８５３１（ＪＰ，Ａ）
特開２０１０－２３１７７８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０