

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号
特開2007-281994
(P2007-281994A)

(43) 公開日 平成19年10月25日(2007. 10. 25)

(51) Int. Cl.

F I

テーマコード (参考)

HO 4 L 9/14 (2006. 01)

GO 6 F 21/24 (2006. 01)

HO 4 L 9/00 6 4 1

GO 6 F 12/14 5 4 O P

5 B O 1 7

5 J I O 4

審査請求 未請求 請求項の数 19 O L (全 19 頁)

(21) 出願番号	特願2006-107220 (P2006-107220)	(71) 出願人	503121103 株式会社ルネサステクノロジ 東京都千代田区大手町二丁目6番2号
(22) 出願日	平成18年4月10日 (2006. 4. 10)	(74) 代理人	100089071 弁理士 玉村 静世
		(72) 発明者	進藤 誠 東京都千代田区丸の内二丁目4番1号 株式会社ルネサステクノロジ内
		(72) 発明者	丹野 洋祐 東京都千代田区丸の内二丁目4番1号 株式会社ルネサステクノロジ内
		(72) 発明者	小林 誠治 東京都千代田区丸の内二丁目4番1号 株式会社ルネサステクノロジ内

最終頁に続く

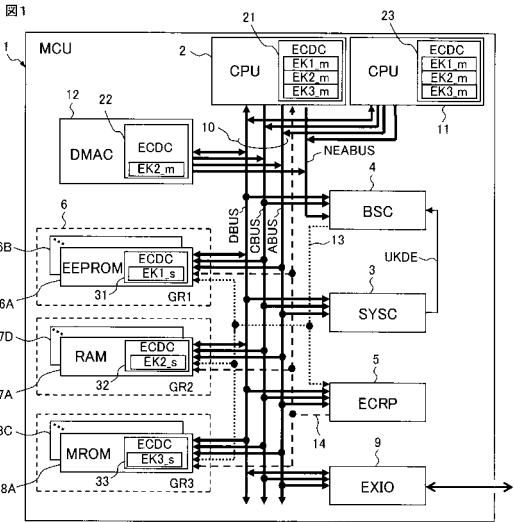
(54) 【発明の名称】 半導体集積回路

(57) 【要約】

【課題】 内部バス上における転送情報の暗号化及び復号に用いる暗号鍵の更新動作に要する電力消費を低減する。

【解決手段】 夫々のバススレーブ（6，7，8）はその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第1の暗号鍵生成回路（EK1_s、EK2_s、EK3_s）を有し、その暗号鍵を用いて内部バス（10）への出力情報の暗号化と入力情報の復号を行う。夫々のバスマスタ（2，12）は前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路（EK1_m、EK2_m、EK3_m）を有し、その暗号鍵を用いて内部バスへの出力情報の暗号化と入力情報の復号を行う。暗号鍵制御回路（5）バスコントローラ（4）によりアクセス対象として選択されたバススレーブが属するグループ内の前記第1の暗号鍵生成回路と当該グループに対応する第2の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

複数のバススレーブ、内部バスを介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ、及び前記バスマスタがアクセスしようとするバススレーブをアクセス対象として選択するバスコントローラを有する半導体集積回路であって、

前記夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第 1 の暗号鍵生成回路を有し、前記暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行い、

前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第 2 の暗号鍵生成回路を有し、アクセス対象とするバススレーブに対応する第 2 の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行い、

前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第 1 の暗号鍵生成回路と当該グループに対応する第 2 の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路を有する半導体集積回路。

【請求項 2】

前記バスマスタ及びバススレーブは内部バスのデータバス上におけるデータ情報に対する暗号化及び復号を行う請求項 1 記載の半導体集積回路。

【請求項 3】

前記バスマスタは内部バスのアドレスバスに出力するアドレス情報に対する暗号化を行い、

前記バススレーブは内部バスのアドレスバスから入力するアドレス情報に対する復号を行い、

前記バスコントローラは前記バスマスタから暗号化前のアドレス情報を受け取って当該バスマスタがアクセスしようとするバススレーブをアクセス対象として選択する請求項 2 記載の半導体集積回路。

【請求項 4】

前記第 1 及び第 2 の暗号鍵生成回路が生成する暗号鍵はアドレス情報の暗号化復号とデータ情報の暗号化復号との双方に対して共通化される請求項 3 記載の半導体集積回路。

【請求項 5】

前記バスマスタを複数個有する請求 1 記載の半導体集積回路。

【請求項 6】

前記バススレーブのグループは、単数又は複数の RAM を含む RAM モジュール、単数又は複数のマスク ROM を含むマスク ROM モジュール、及び単数又は複数の電氣的に書換え可能なプログラマブル ROM モジュールである請求項 5 記載の半導体集積回路。

【請求項 7】

前記バスマスタは内部クロック信号に同期して内部バスにアドレス信号を出力したとき次のクロックサイクルで、書込みデータを内部バスのデータバスに出力し、又は内部バスのデータバスから読出しデータを取り込む制御を行う請求項 1 記載の半導体集積回路。

【請求項 8】

前記第 1 及び第 2 の暗号鍵生成回路は、前記データバスへのデータ出力又はデータバスからのデータ入力のクロックサイクルの開始タイミングに同期して前記暗号鍵の同期的更新動作を行なう請求項 7 記載の半導体集積回路。

【請求項 9】

前記第 1 の暗号鍵生成回路及び第 2 の暗号鍵生成回路は、初段への帰還経路に乱数発生器の出力と論理演算を行う論理ゲートを備えたリングカウンタを有し、前記リングカウンタの計数値が暗号鍵とされる請求項 1 記載の半導体集積回路。

【請求項 10】

前記リングカウンタは前記内部バスを介して初期値がプリセット可能にされた請求項 9

10

20

30

40

50

記載の半導体集積回路。

【請求項 1 1】

複数のバススレーブ、内部バスを介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ、及び前記バスマスタがアクセスしようとするバススレーブをアクセス対象として選択するバスコントローラを有する半導体集積回路であって、

前記夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第 1 の暗号鍵生成回路を有し、前記暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスのアドレスバスからの入力情報の復号を行い、

前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第 2 の暗号鍵生成回路を有し、アクセス対象とするバススレーブに対応する第 2 の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスのアドレスバスへの出力情報の暗号化を行い、

前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第 1 の暗号鍵生成回路と当該グループに対応する第 2 の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路を有する半導体集積回路。

【請求項 1 2】

複数のバススレーブ、内部バスを介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ、及び前記バスマスタがアクセスしようとするバススレーブをアクセス対象として選択するバスコントローラを有する半導体集積回路であって、

前記夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第 1 の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行い、

前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第 2 の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行い、

前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第 1 の暗号鍵生成回路と当該グループに対応する第 2 の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路を有する半導体集積回路。

【請求項 1 3】

前記バスマスタ及びバススレーブは内部バスのデータバス上におけるデータ情報に対する暗号化及び復号を行う請求項 1 2 記載の半導体集積回路。

【請求項 1 4】

前記バスマスタは内部バスのアドレスバスに出力するアドレス情報に対する暗号化を行い、

前記バススレーブは内部バスのアドレスバスから入力するアドレス情報に対する復号を行い、

前記バスコントローラは前記バスマスタから暗号化前のアドレス情報を受け取って当該バスマスタがアクセスしようとするバススレーブをアクセス対象として選択する請求項 1 3 記載の半導体集積回路。

【請求項 1 5】

複数のバススレーブ、内部バスを介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ、及び前記バスマスタがアクセスしようとするバススレーブをアクセス対象として選択するバスコントローラを有する半導体集積回路であって、

前記夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第 1 の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスのアドレスバスからの入力情報の復号を行い、

前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第 2 の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスのアドレスバスへの出力情報の暗号化を行い

10

20

30

40

50

、
前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第1の暗号鍵生成回路と当該グループに対応する第2の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路を有する半導体集積回路。

【請求項16】

複数のバススレーブ、内部バスを介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ、及び前記バスマスタがアクセスしようとするバススレーブをアクセス対象として選択するバスコントローラを有する半導体集積回路であって、

前記夫々のバススレーブはその数よりも少ない数にグループ化され、グループ毎に当該グループの暗号鍵を生成する第1の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行う第1の暗号化復号回路を有し、

前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行う第2の暗号化復号回路有し、

前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第1の暗号鍵生成回路と当該グループに対応する第2の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路を有する半導体集積回路。

【請求項17】

前記バスマスタ及びバススレーブは内部バスのデータバス上におけるデータ情報に対する暗号化及び復号を行う請求項16記載の半導体集積回路。

【請求項18】

前記バスマスタは内部バスのアドレスバスに出力するアドレス情報に対する暗号化を行い、

前記バススレーブは内部バスのアドレスバスから入力するアドレス情報に対する復号を行い、

前記バスコントローラは前記バスマスタから暗号化前のアドレス情報を受け取って当該バスマスタがアクセスしようとするバススレーブをアクセス対象として選択する請求項17記載の半導体集積回路。

【請求項19】

複数のバススレーブ、内部バスを介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ、及び前記バスマスタがアクセスしようとするバススレーブをアクセス対象として選択するバスコントローラを有する半導体集積回路であって、

前記夫々のバススレーブはその数よりも少ない数にグループ化され、グループ毎に当該グループの暗号鍵を生成する第1の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスのアドレスバスからの入力情報の復号を行う第1の暗号化復号回路を有し、

前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスのアドレスバスへの出力情報の暗号化を行う第2の暗号化復号回路有し、

前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第1の暗号鍵生成回路と当該グループに対応する第2の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路を有する半導体集積回路。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、バスマスタとバススレーブ間の内部バス上に転送される情報を暗号化した半導体集積回路に関し、例えばICカード用マイクロコンピュータ（ICカードマイコンとも記す）に適用して有効な技術に関する。

10

20

30

40

50

【背景技術】

【0002】

機密保護データを扱うICカードマイコンのような半導体集積回路（LSI）に対する不正アクセスの手段には電源系ノイズを観測してデータを不正に解析したりする手法がある。これに対してプロセッサとメモリ間のバス上において転送データを暗号化する技術が特許文献1に記載がある。特に特許文献1ではデータの暗号化復号に用いる鍵をテーブルに保持し、プロセッサは暗号化に際してテーブルのインデックスを生成し、メモリはそのインデックスをメモリに蓄え、プロセッサは暗号化データをインデックスと共にメモリに転送し、メモリはインデックスを用いて検索した鍵を暗号化データの復号に用いるものである。これによって暗号化復号動作に伴う電力消費を低減しようとするものである。

10

【0003】

【特許文献1】特開2003-198534

【発明の開示】

【発明が解決しようとする課題】

【0004】

本発明者はICカードマイコンにオンチップされたバスマスタと複数のバススレーブを接続する内部バス上における転送情報の暗号化について検討した。例えばバスマスタから出力されたデータは暗号鍵を用いて暗号化されてバスに供給され、これを受けるバススレーブ側は当該暗号鍵を用いてバス上のデータを復号する。暗号化及び復号にはビット毎に2入力排他的論理和ゲート等を用いればよい。暗号化と復号に利用する暗号鍵は逐次変更されることが望ましいため、バススレーブとバスマスタは夫々同期して暗号鍵を更新する暗号鍵生成回路を持つことが必要である。例えばバスマスタによるバスアクセス毎に暗号鍵を更新するように制御すればよい。あるバスマスタによってアクセス可能な複数のバススレーブがオンチップされているとき、バスマスタが一つのバススレーブをアクセスするときであっても残りのバススレーブに対しても暗号鍵生成回路による暗号鍵の更新を制御しなければ、バスマスタとバススレーブとの間の暗号鍵の整合を維持することができなくなる。しかしながら、オンチップされるバスマスタ及びバススレーブの数や種類が多くなったとき、アクセス対象とされない全てのバスマスタ及びバススレーブに係る暗号鍵生成回路についてもバスアクセスサイクルの度に暗号鍵の更新動作を行わなければならないとなると、電力消費が著しく増大してしまうことが本発明者によって明らかにされた。特許文献1ではそのような意味での低消費電力化について考慮されていない。

20

30

【0005】

本発明の目的は、バスマスタ及びバススレーブの数や種類が増えてもそれらが接続される内部バス上における転送情報の暗号化及び復号に用いる暗号鍵の更新動作に要する電力消費を低減できる半導体集積回路を提供することにある。

【0006】

本発明の前記並びにその他の目的と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。

【課題を解決するための手段】

【0007】

本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記の通りである。

40

【0008】

〔1〕本発明に係る半導体集積回路（1）は、複数のバススレーブ（6A～6B、7A～7D、8A～8C）、内部バス（10）を介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ（2、11、12）及び前記バスマスタがアクセスしよとするバススレーブをアクセス対象として選択するバスコントローラ（4）を有する。前記夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第1の暗号鍵生成回路（EK1__s、EK2__s、EK3__s）を有し、前記暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスへの出力情報

50

の暗号化と前記内部バスからの入力情報の復号を行う。前記夫々のバスマスタは前記グループ（６，７，８）毎の暗号鍵を生成する複数の第２の暗号鍵生成回路（EK 1 __m、EK 2 __m、EK 3 __m）を有し、アクセス対象とするバススレーブに対応する第２の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行う。前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第１の暗号鍵生成回路と当該グループに対応する第２の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路（５）を有する。

【０００９】

上記した手段によれば、バススレーブのグループ毎にバスマスタ及びバススレーブにおける暗号鍵の生成と更新をグループ化したから、バスアクセス動作において動作される暗号鍵生成回路はアクセス主体のバスマスタとアクセス対象とされるバススレーブを含むバススレーブのグループとに限定される。このように動作すべき暗号鍵生成回路を限定することにより、暗号鍵の更新動作等に伴う消費電力を低減することが可能になる。また、バススレーブはその数より少ない数にグループ化されグループ毎に暗号鍵を割り当て、全てのバススレーブ毎に個別の暗号鍵を割り当てるものではないから、一つのバスマスタが保有すべき第２の暗号鍵生成回路の数はバススレーブの数よりも少なくなり、チップ面積の増大が過大なることはない。低消費電力とチップ面積増大のトレードオフを考慮すると、グループ化は例えば１０グループ以下にするのがよい。チップ面積はグループ化数に比例して増えるが、消費電力はグループ化数が１０程度までは漸次減少するがそれ以上では電力消費の低減率が収束してしまうからである。グループ化数が１０程度を超えると暗号鍵生成回路の数が増える分だけ逆にそれぞれの記憶段等で消費される電力の増大を無視できなくなるからである。

【００１０】

本発明の一つの具体的な形態として、前記バスマスタ及びバススレーブは内部バスのデータバス上におけるデータ情報に対する暗号化及び復号を行うものである。内部バスのデータバス上におけるデータの暗号化が行われる。また、前記バスマスタは内部バスのアドレスバスに出力するアドレス情報に対する暗号化を行い、前記バススレーブは内部バスのアドレスバスから入力するアドレス情報に対する復号を行ってもよい。これにより、内部バス上のアドレスバス上におけるアドレス情報に対する暗号化も行われる。ただし、前記バスコントローラは前記バスマスタから暗号化前のアドレス情報を受け取って当該バスマスタがアクセスしようとするバススレーブをアクセス対象として選択することが必要である。このとき、前記第１及び第２の暗号鍵生成回路が生成する暗号鍵はアドレス情報の暗号化復号とデータ情報の暗号化復号との双方に対して共通化されてもよい。前記バスマスタは複数個であってもよい。また、前記バススレーブグループは、例えば単数又は複数のRAMを含むRAMモジュール、単数又は複数のマスクROMを含むマスクROMモジュール、及び単数又は複数の電氣的に書換え可能なプログラマブルROMモジュールである。

【００１１】

本発明の別の具体的な形態として、前記バスマスタは内部クロック信号に同期して内部バスにアドレス信号を出力したとき次のクロックサイクルで、書込みデータを内部バスのデータバスに出力し、又は内部バスのデータバスから読出しデータを取り込む制御を行う。このとき、前記第１及び第２の暗号鍵生成回路は前記データバスへのデータ出力又はデータバスからのデータ入力のクロックサイクルの開始タイミングに同期して前記暗号鍵の同期的更新動作を行なう。したがって、データバス上のデータ情報は今回のアクセス動作期間中に更新された暗号鍵を用いて暗号化及び復号が行われる。一方、アドレスバス上のアドレス情報は前回のアクセス動作期間中に既に更新されている暗号鍵を用いて暗号化及び復号が行われる。

【００１２】

本発明の更に別の具体的な形態として、前記第１の暗号鍵生成回路及び第２の暗号鍵生

10

20

30

40

50

成回路は、初段への帰還経路に乱数発生器の出力と論理演算を行う論理ゲート（E O R 1）を備えたリングカウンタ（L F S R）を有し、前記リングカウンタの計数値が暗号鍵とされる。前記リングカウンタは例えば前記内部バスを介して初期値がプリセット可能にされる。リセット信号により一定値に初期化される場合に比べて暗号鍵の機密性が増す。

【0013】

〔2〕アドレス情報の暗号化に特化する観点では半導体集積回路は、複数のバススレーブ、内部バスを介して前記複数のバススレーブに接続され前記複数のバススレーブをアクセス可能なバスマスタ、及び前記バスマスタがアクセスしようとするバススレーブをアクセス対象として選択するバスコントローラを有する。前記夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第1の暗号鍵生成回路を有し、前記暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスのアドレスバスからの入力情報の復号を行う。前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路を有し、アクセス対象とするバススレーブに対応する第2の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスのアドレスバスへの出力情報の暗号化を行う。前記バスコントローラによりアクセス対象として選択されたバススレーブが属するグループ内の前記第1の暗号鍵生成回路と当該グループに対応する第2の暗号鍵生成回路とに対して暗号鍵の同期的更新を指示する暗号鍵制御回路を有する。

10

【0014】

上記した手段同様に、バスアクセス動作において動作される暗号鍵生成回路はアクセス主体のバスマスタとアクセス対象とされるバススレーブを含むバススレーブグループとに限定されるから、暗号鍵の更新動作等に伴う消費電力を低減することが可能になる。更に、暗号鍵生成回路の数が多数に及ぶことによってチップ面積の増大が過大となることもない。

20

【0015】

〔3〕本発明の別の観点では第1の暗号鍵生成回路をグループ単位で設ける。即ち、夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第1の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行い、前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行ってもよい。要するに、第1の暗号鍵生成回路はそれぞれのバススレーブが保有しなくてもよい。グループ毎に保有してもよい。この場合も上記同様に、前記バスマスタ及びバススレーブは内部バスのデータバス上におけるデータ情報に対する暗号化及び復号を行う。また、前記バスマスタは内部バスのアドレスバスに出力するアドレス情報に対する暗号化を行い、前記バススレーブは内部バスのアドレスバスから入力するアドレス情報に対する復号を行う。

30

【0016】

更に同様の観点より、夫々のバススレーブはその数よりも少ない数にグループ化された当該グループの暗号鍵を生成する第1の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスのアドレスバスからの入力情報の復号を行い、夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスのアドレスバスへの出力情報の暗号化を行ってもよい。

40

【0017】

暗号鍵生成回路をグループ単位で設けるという観点においては、チップ面積は低減するが暗号鍵を伝達する配線の引き回しが長くなり、暗号鍵それ自体に対する不正アクセスの攻撃を受け易くなる点に注意が必要である。

【0018】

〔4〕本発明の更に別の観点ではバススレーブの暗号化復号回路をグループ単位で設ける。即ち、前記夫々のバススレーブはその数よりも少ない数にグループ化され、グループ毎に当該グループの暗号鍵を生成する第1の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行う第1の暗

50

号化復号回路を有し、前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスへの出力情報の暗号化と前記内部バスからの入力情報の復号を行う第2の暗号化復号回路を有する。この場合も上記同様に、前記バスマスタ及びバススレーブは内部バスのデータバス上におけるデータ情報に対する暗号化及び復号を行う。また、前記バスマスタは内部バスのアドレスバスに出力するアドレス情報に対する暗号化を行い、前記バススレーブは内部バスのアドレスバスから入力するアドレス情報に対する復号を行う。

【0019】

更に同様の観点より、前記夫々のバススレーブはその数よりも少ない数にグループ化され、グループ毎に当該グループの暗号鍵を生成する第1の暗号鍵生成回路で生成された暗号鍵を用いて前記内部バスのアドレスバスからの入力情報の復号を行う第1の暗号化復号回路を有し、前記夫々のバスマスタは前記グループ毎の暗号鍵を生成する複数の第2の暗号鍵生成回路で生成される暗号鍵を用いて前記内部バスのアドレスバスへの出力情報の暗号化を行う第2の暗号化復号回路を有するようにしてもよい。

10

【0020】

暗号化復号回路をグループ単位で設けると言う観点においては、チップ面積は低減するが、暗号化前及び復号後の情報伝達距離が長くなるので、不正アクセスの攻撃を受け易くなる点に注意が必要である。

【発明の効果】

【0021】

本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。

20

【0022】

すなわち、暗号鍵の更新動作等に伴う消費電力を低減することができる。このとき、暗号鍵生成回路の数が多数に及ぶことによってチップ面積の増大が過大になることはない。

【発明を実施するための最良の形態】

【0023】

《ICカードマイコン》

図1には本発明に係る半導体集積回路の一例としてICカードマイコンが例示される。同図に示されるICカードマイコン1は例えば単結晶シリコン等の半導体基板にCMOS集積回路製造技術によって形成される。CPU2はメインCPUであり、CPU11はメインCPU2からのコマンドに応答して演算処理を行なうサブCPUである。ともにアドレッシング機能を備え、命令をフェッチし、フェッチした命令をデコードし、デコード結果に従ってデータロード、演算及び演算結果のストア等を行って、その命令を実行する。システムコントローラ(SYSC)3はシステムリセット及びパワーオンリセットに伴うハードウェア制御を行うと共に、ICカードマイコン1の動作モード等を制御する。内部バス10としてデータバス(DBUS)、アドレスバス(ABUS)、及びコントロールバス(CBUS)を有する。詳細は後述するが、データバス(DBUS)及びアドレスバス(ABUS)で転送されるデータ情報及びアドレス情報は暗号化された情報とされる。内部バス10にはバススレーブモジュールとしてエレクトリカリ・イレーザブル・アンド・プログラマブルROM(EEPROM)6A~6B、ランダムアクセスメモリ(RAM)7A~7D、及びマスクROM(MROM)8A~8Cが接続される。内部バス10にはCPU2、11以外のバスマスタとしてダイレクトメモリアクセスコントローラ(DMAC)12が接続される。CPU2、11又はDMAC12はバスアクセスを行うとき、暗号化したアドレス情報をアドレスバスABUSに出力するが、これに並行して、暗号化前のアドレス情報を非暗号化アドレスバスNEABUSに出力する。バスコントローラ(BSC)4は、ICカードマイコン1のアドレス空間に対してバススレーブ等に対するエリア毎にアクセスサイクル数やデータ入出力ビット数等のバスアクセス制御情報が初期設定され、非暗号化アドレスNEABUS上のアドレス情報からアクセス対象のバススレーブを判定し、その動作を選択するための複数ビットのモジュール選択信号13等を出力する

30

40

50

。暗号化されたアドレス情報に基づいて正しいモジュール選択を行うことはできないからである。尚、非暗号化アドレスNEABUSはCPU2やDMAC12等のロジック回路に接続されており、そのバス配線はメモリに接続するバス配線のように規則的にはならないから、当該非暗号化アドレスNEABUSの所在の特定は難しく、暗号化しなくても不正アクセスを受ける虞は極めて小さいと考えられる。

【0024】

EEPROM6A～6Bは電氣的に書換え可能な不揮発性メモリである。RAM7A～7Dは例えばスタティックRAMによって構成される。RAM7A～7DはCPU1のワーク領域及びデータバッファ等に利用され、EEPROM6A～6B及びMROM8A～8Cはプログラム領域又はデータ領域として利用される。認証処理等に利用されるパスワードや個人情報等の機密情報はEEPROM6A～6BやMROM8A～8Cが保有し、CPU2, 11はその機密情報を読み出し、RAM7A～7Dを用いて認証処理等を行なう。内部バス10にはその他に外部入出力インタフェース回路(EXIO)9等が接続される。外部インタフェース回路9はホスト装置との間でコマンド入力及びデータ入出力等を行う。外部インタフェース回路9のインタフェース形態は外部端子を介する接触インタフェース或いはアンテナを介する非接触インタフェースの何れか一方又であっても、双方であってもよい。

【0025】

ICカードマイコン1は機密保護の観点よりバスマスタによるバススレーブのアクセスに際して内部バス10上のデータ及びアドレスを暗号化するバス暗号化機能を備える。ここでは夫々バスマスタであるCPU2、11及びDMAC12は前記内部バス10への出力情報の暗号化と前記内部バス10からの入力情報の復号を行う暗号化復号回路(ECD C)21～23を有する。それぞれのEEPROM6A～6Bは前記内部バス10への出力情報の暗号化と前記内部バス10からの入力情報の復号を行う暗号化復号回路31を有する。同様に、それぞれのRAM7A～7Dは暗号化復号回路32を有し、それぞれのMROM8A～8Cは暗号化復号回路33を有する。

【0026】

内部バス10上の情報に対する暗号化及び復号に用いる暗号鍵の割り当てに関し、EEPROM6A～6BをEPROMグループ(GR1)6とし、RAM7A～7DをRAMグループ(GR2)7とし、MROM8A～8CをMROMグループ(GR3)8とし、バススレーブの数よりも少ない数のグループにグループ化される。グループ毎に暗号鍵を割り当て、例えば夫々のバススレーブの暗号化復号回路31～33はそれに割り当てられたグループの暗号鍵を生成する暗号鍵生成回路(第1の暗号鍵生成回路)EK1__s～EK3__sを有する。即ち、夫々のEEPROM6A～6Bの暗号化復号回路31は、暗号鍵生成回路EK1__sを有し、前記暗号鍵生成回路EK1__sで生成された暗号鍵を用いて前記内部バス10への出力情報の暗号化と前記内部バス10からの入力情報の復号を行う。夫々のRAM7A～7Dの暗号化復号回路32は、暗号鍵生成回路EK2__sを有し、前記暗号鍵生成回路EK2__sで生成された暗号鍵を用いて前記内部バス10への出力情報の暗号化と前記内部バス10からの入力情報の復号を行う。夫々のMROM8A～8Cの暗号化復号回路33は、暗号鍵生成回路EK3__sを有し、前記暗号鍵生成回路EK3__sで生成された暗号鍵を用いて前記内部バス10への出力情報の暗号化と前記内部バス10からの入力情報の復号を行う。

【0027】

CPU2、11とDMAC12の暗号化復号回路21～23はアクセス可能な全てのバススレーブのグループに対応する暗号鍵を用いた暗号化及び復号機能を備える。即ち、暗号化復号回路21、23はそれぞれ暗号鍵生成回路(第2の暗号鍵生成回路)EK1__m～EK3__mを備える。暗号化復号回路22は暗号鍵生成回路(第2の暗号鍵生成回路)EK2__mを備える。暗号鍵生成回路EK1__mはEEPROMグループ6の暗号鍵生成回路EK1__sと同じ回路構成を有し、暗号鍵生成回路EK2__mはRAMグループ7の暗号鍵生成回路EK2__sと同じ回路構成を有し、暗号鍵生成回路EK3__mはMROM

グループ 8 の暗号鍵生成回路 E K 3 __ s と同じ回路構成を有する。暗号化復号回路 2 1 ~ 2 3 は自らが属するバスマスタがアクセスするバススレーブのグループに対応する暗号鍵生成回路 E K 1 __ m ~ E K 3 __ m の何れかで生成される暗号鍵を用いて、前記内部バス 1 0 への出力情報の暗号化と前記内部バス 1 0 からの入力情報の復号を行う。

【0028】

機密保護の実効性を上げるには暗号鍵の逐次更新が必要であるが、バスマスタとこれによってアクセスされるバススレーブの双方が用いる暗号鍵は相互に同じでなければならない。暗号鍵制御回路 (E C R P) 5 は、B S C 4 によりアクセス対象として選択されたバススレーブが属する一つのグループ内の暗号鍵生成回路 (E K 1 __ s ~ E K 3 __ s の何れか) と当該グループに対応するバスマスタモジュール内の一つの暗号鍵生成回路 (E K 1 __ m ~ E K 3 __ m の何れか) とに対して暗号鍵の同期的更新を複数ビットの更新制御信号 1 4 によって指示する。E C R P 5 はモジュール選択信号 1 3 を参照してアクセス対象とされるバススレーブのグループを判別し、前記更新制御信号 1 4 により、判別したグループのバススレーブと、当該グループをアクセス可能なバスマスタとに対して、暗号鍵生成回路に暗号鍵を更新する動作を指示する。更新が指示された暗号鍵生成回路は、例えばバスアクセスサイクルを規定するクロック信号の所定変化に同期して暗号鍵を更新する。

10

【0029】

《データバスの暗号化復号機能》

図 2 には I C カードマイコンにおけるデータバスの暗号化復号機能の詳細が例示される。図 2 においてそれぞれの暗号化復号回路 2 1 ~ 2 3、3 1 ~ 3 3 において暗号鍵を用いた暗号化及び復号にはデータの各ビットに排他的論理和ゲート (E O R) を用いる。例えば図 3 に例示されるように、バスマスタにおいてデータ D 0、D 1 (= 1, 0) と暗号化鍵 K e c (= 1) を E O R に入力して暗号化し、暗号化されたデータ (= 0, 1) がデータバスを介してスレーブモジュールに入力される。入力された暗号化データ (= 0, 1) は暗号化時と同じ論理値の暗号化鍵 K e c (= 1) と一緒に E O R に入力されることにより、元のデータ D 0、D 1 (= 1, 0) に復号される。特に図示はしないが、データバス D B U S に出力端子が結合された E O R はトライステート出力が可能にされ、出力動作が指示されていないときは高出力インピーダンス状態 (H i Z) にされる。

20

【0030】

バスマスタ 2, 1 1 において暗号鍵生成回路 E K 1 __ m ~ E K 3 __ m はセレクタ S E L で選択される。その選択はバスマスタが自らアクセスしようとするバススレーブのグループに応じて行われる。図 2 において B S C 4 が出力するモジュール選択信号 1 3 は、E E P R O M グループ 6 のバススレーブ 6 A ~ 6 B に対するモジュール選択信号 1 3 __ 1、R A M グループ 7 のバススレーブ 7 A ~ 7 D に対するモジュール選択信号 1 3 __ 2、M R O M グループ 8 のバススレーブ 8 A ~ 8 C に対するモジュール選択信号 1 3 __ 3 を含み、それらは E C P R 5 に供給される。S Y S C 3 はパワーオンリセット又はシステムリセットの後に暗号鍵の更新制御イネーブル信号 U K D E を E C R P 5 にアサートする。このアサート期間において、E C R P 5 はアクセスされるバススレーブのグループ内の暗号鍵と当該グループに対応するバスマスタ内の暗号鍵との同期的更新制御が可能にされる。E C R P 5 が出力する更新制御信号 1 4 は、E E P R O M グループ 6 内の暗号鍵生成回路 E K 1 __ s と当該グループに対応するバスマスタ 2, 1 1 内のそれぞれの暗号鍵生成回路 E K 1 __ m とに対する更新制御信号 1 4 __ 1、R A M グループ 7 内の暗号鍵生成回路 E K 2 __ s と当該グループに対応するバスマスタ 2, 1 1, 1 2 内のそれぞれの暗号鍵生成回路 E K 2 __ m とに対する更新制御信号 1 4 __ 2、M R O M グループ 8 内の暗号鍵生成回路 E K 3 __ s と当該グループに対応するバスマスタ 2, 1 1 内のそれぞれ暗号鍵生成回路 E K 3 __ m とに対する更新制御信号 1 4 __ 3 を含む。図 2 においてそれぞれのバススレーブ及びバスマスタ内の I T N L で示される回路ブロックは、便宜上各々のバススレーブ及びバスマスタにおいて暗号化復号回路以外の回路部分を意味するものである。

30

40

【0031】

図 4 には図 2 の回路におけるデータの暗号化復号動作のタイミングチャートが例示され

50

る。バスコマンド（BCMD）はCPU 2等のバスマスタがアドレス信号と一緒にコントロールバスCBUSに出力するリード・ライト等のアクセス制御形態を指示する制御情報である。CLKはICカードマイコンにおけるバスアクセスサイクルを規定する内部クロック信号である。図4の例では、前記バスマスタは内部クロック信号CLKに同期して非暗号化アドレスバスNEABUSにアドレス信号を出力したとき次のクロックサイクルで、書込みデータをデータバスDBUSに出力し、又はデータバスDBUSから読出しデータを取り込む制御を行うようになっている。例えばCPU 2が時刻t 0にリードアクセスを指示し、時刻t 1にライトアクセスを指示する。時刻t 0から始まる1クロックサイクル（CYC 1）で前記リードサイクルのアドレス（H' 000100 = EEPROM 6Aのアドレス）がアドレスバスNEABUSに出力され、時刻t 1から始まる1クロックサイクル（CYC 2）で前記ライトサイクルのアドレス（H' FFFA10 = RAM 7Aのアドレス）がアドレスバスNEABUSに出力される。これと共に、暗号化されたアドレス情報がアドレスバスABUSに出力されるが、同図では便宜上、アドレス情報に対する暗号化及び復号については着目していない。

【0032】

BSC 4はリードサイクルのアドレス（H' 000100 = EEPROM 6Aのアドレス）に応答してモジュール選択信号13_1をローレベルにアサートし、これを受けてECRP 5はEEPROMグループ6に対する暗号鍵更新制御信号14_1をハイレベルにアサートする。暗号鍵更新制御信号14_1によって更新が指示される暗号鍵生成回路EK 1_s、EK 1_mが生成する暗号鍵はH' 55とされている。暗号鍵生成回路は前記データバスDBUS上におけるデータ出力又はデータバスからのデータ入力のクロックサイクルの開始タイミング（＝アドレスバスに対するアドレス出力のクロックサイクルの終了タイミング）に同期して前記暗号鍵の同期的更新動作を行なうから、暗号鍵生成回路EK 1_s、EK 1_mの暗号鍵はクロックサイクルCYC 2が始まる時刻t 1にH' 55からH' AAに同期的に更新される。時刻t 1から始まるクロックサイクルCYC 2において、EEPROM 6Aはメモリアレイから読み出した元データH' 66を暗号鍵H' AAを用いてデータH' CCに暗号化し、これをデータバスDBUSに出力し、一方、CPU 2はデータバスDBUSからH' CCの暗号化データを取り込み、これを暗号鍵H' AAで復号して、元データH' 66を再生して取り込む。この動作中、アクセス対象とされていないRAMグループ7の暗号鍵に関する暗号鍵生成回路EK 2_s、EK 2_mは暗号鍵の更新動作が抑止されている。図示はしないがMRONグループの暗号鍵に関する暗号鍵生成回路EK 3_s、EK 3_mも同様に更新動作が抑止されている。

【0033】

時刻t 1から始まるライトサイクルでは、BSC 4は当該ライトサイクルのアドレス（H' FFFA10 = RAM 7Aのアドレス）に応答してモジュール選択信号13_2をローレベルにアサートし、これを受けてECRP 5はRAMグループ7に対する暗号鍵更新制御信号14_2をハイレベルにアサートする。暗号鍵更新制御信号14_2によって更新が指示される暗号鍵生成回路EK 2_s、EK 2_mが生成する暗号鍵はH' 2Aとされている。暗号鍵生成回路EK 2_s、EK 2_mの暗号鍵はクロックサイクルCYC 3が始まる時刻t 2にH' 2AからH' B5に同期的に更新される。時刻t 2から始まるクロックサイクルCYC 3において、CPU 2は書込みアクセスの元データH' 88を暗号鍵H' B5を用いてデータH' 3Dに暗号化し、これをデータバスDBUSに出力し、一方、書込み動作されるRAM 7AはデータバスDBUSからH' 3Dの暗号化データを取り込み、これを暗号鍵H' B5で復号して、元データH' 88を再生してメモリアレイに書込む。この動作中、アクセス対象とされていないEEPROMグループ6の暗号鍵に関する暗号鍵生成回路EK 1_s、EK 1_mは暗号鍵の更新動作が抑止されている。図示はしないがMRONグループの暗号鍵に関する暗号鍵生成回路EK 3_s、EK 3_mも同様に更新動作が抑止されている。

【0034】

《アドレスバスの暗号化復号機能》

図 5 には I C カードマイコンにおけるアドレスバスの暗号化復号機能の詳細が例示される。図 5 ではバスマスタとして C P U 2 のみ代表的に示される。図 5 において暗号化復号回路 2 1、3 1 ~ 3 3 において暗号鍵を用いた暗号化及び復号にはアドレスの各ビットに排他的論理和ゲート (E O R) を用いる。特に図示はしないは、アドレスバス A B U S に出力端子が結合された E O R はトライステート出力が可能にされ、出力動作が指示されていないときは高出力インピーダンス状態 (H i Z) にされる。アドレスの暗号化にもデータと同じ暗号鍵生成回路 E K 1 __m ~ E K 3 __m を用いる。したがって暗号鍵の更新制御はデータの場合と同じである。但し、暗号鍵の更新タイミングはデータサイクルの開始タイミング (アドレスサイクルの周力タイミング) であるから、アドレスを暗号化するとき用いる暗号鍵は更新前の暗号鍵とされる。

10

【0035】

図 6 には図 5 の回路におけるアドレスの暗号化復号動作のタイミングチャートが例示される。上記同様に図 6 の場合も、バスマスタは内部クロック信号 C L K に同期してアドレス A B U S にアドレス信号を出力したとき次のクロックサイクルで、書込みデータをデータバス D B U S に出力し、又はデータバス D B U S から読出しデータを取り込む制御を行うようになっている。例えば C P U 2 が時刻 t 0 にリードアクセスを指示し、時刻 t 1 にライトアクセスを指示し、時刻 t 2 にリードアクセスを指示する。時刻 t 0 から始まる 1 クロックサイクル (C Y C 1) で前記リードサイクルのアドレス情報 A D R S (H ' 0 0 0 1 0 0 = E E P R O M 6 A のアドレス) が暗号化復号回路 2 1 と B S C 4 に出力され、時刻 t 1 から始まる 1 クロックサイクル (C Y C 2) で次のライトサイクルのアドレス情報 A D R S (H ' F F F A 1 0 = R A M 7 A のアドレス) が暗号化復号回路 2 1 と B S C 4 に出力され、時刻 t 2 から始まる 1 クロックサイクル (C Y C 3) で其の次のリードサイクルのアドレス情報 A D R S (H ' 0 0 0 1 1 0 = E E P R O M 6 A のアドレス) が暗号化復号回路 2 1 と B S C 4 に出力される。

20

【0036】

B S C 4 は最初のリードサイクルのアドレス情報 (H ' 0 0 0 1 0 0 = E E P R O M 6 A のアドレス) に応答してモジュール選択信号 1 3 __1 をローレベルにアサートし、これを受けて E C R P 5 は E E P R O M グループ 6 に対する暗号鍵更新制御信号 1 4 __1 をハイレベルにアサートする。暗号鍵更新制御信号 1 4 __1 によって更新が指示される暗号鍵生成回路 E K 1 __s、E K 1 __m が生成する暗号鍵は H ' 5 5 とされている。暗号鍵生成回路 E K 1 __s、E K 1 __m は前記データバス D B U S 上におけるデータ出力又はデータバスからのデータ入力のクロックサイクルの開始タイミング (= アドレスバスに対するアドレス出力のクロックサイクルの終了タイミング) に同期して前記暗号鍵の同期的更新動作を行なうから、暗号鍵生成回路 E K 1 __s、E K 1 __m の暗号鍵はクロックサイクル C Y C 2 が始まる時刻 t 1 に H ' 5 5 から H ' A A に同期的に更新される。アドレスに対する暗号化はアドレス出力サイクル C Y C 1 の最初に行われなければならないから、C P U 2 は時刻 t 0 から始まるクロックサイクル C Y C 1 において、アクセスアドレスの元アドレス情報 H ' 0 0 0 1 0 0 を暗号鍵 H ' 5 5 を用いてアドレス情報 H ' 5 5 5 4 5 5 に暗号化し、これをアドレスバス A B U S に出力し、一方、E E P R O M 6 A はアドレスバス A B U S から暗号化アドレス情報 H ' 5 5 5 4 5 5 を取り込み、これを暗号鍵 H ' 5 5 で復号して、元のアドレス情報 H ' 0 0 0 1 0 0 を再生して取り込み、取り込んだアドレスに基づいて E E P R O M 6 A からデータを読み出し、読出されたデータは C P U 2 に取り込まれる。この動作中、アクセス対象とされていない R A M グループ 7 及び M R O M グループ 8 の暗号鍵に関する暗号鍵生成回路 E K 2 __s、E K 2 __m、E K 3 __s、E K 3 __m は暗号鍵の更新動作が抑止されている。

30

40

【0037】

次のクロックサイクル C Y C 2 では、アドレス情報 (H ' F F F A 1 0 = R A M 7 A のアドレス) に応答してモジュール選択信号 1 3 __2 をローレベルにアサートし、これを受けて E C R P 5 は R A M グループ 7 に対する暗号鍵更新制御信号 1 4 __2 をハイレベルにアサートする。暗号鍵更新制御信号 1 4 __2 によって更新が指示される暗号鍵生成回路 E

50

K 2 __ s、E K 2 __ mが生成する暗号鍵は時刻 t 1 において H ' 2 A とされている。暗号鍵生成回路 E K 2 __ s、E K 2 __ m はクロックサイクル C Y C 3 が始まる時刻 t 2 に H ' 2 A から H ' B 5 に同期的に更新される。アドレスに対する暗号化はアドレス出力サイクル C Y C 2 の最初に行われなければならないから、C P U 2 は時刻 t 1 から始まるクロックサイクル C Y C 2 において、アクセスアドレスの元アドレス情報 H ' F F F A 1 0 を暗号鍵 H ' 2 A を用いてアドレス情報 H ' D 5 D 0 3 A に暗号化し、これをアドレスバス A B U S に出力し、一方、R A M 7 A はアドレスバス A B U S から暗号化アドレス情報 H ' D 5 D 0 3 A を取り込み、これを暗号鍵 H ' 2 A で復号して、元のアドレス情報 H ' F F F A 1 0 を再生して取り込み、取り込んだアドレスに基づいて R A M 7 A にデータが書込まれる。この動作中、アクセス対象とされていない E E P R O M グループ 6 及び M R O M グループ 8 の暗号鍵に関する暗号鍵生成回路 E K 1 __ s、E K 1 __ m、E K 3 __ s、E K 3 __ m は暗号鍵の更新動作が抑止されている。

10

【0038】

その次のクロックサイクル C Y C 3 では、アドレス情報 (H ' 0 0 0 1 1 0 = E E P R O M 6 A のアドレス) に応答してモジュール選択信号 1 3 __ 1 をローレベルにアサートし、これを受けて E C R P 5 は E E P R O M グループ 6 に対する暗号鍵更新制御信号 1 4 __ 1 をハイレベルにアサートする。暗号鍵更新制御信号 1 4 __ 1 によって更新が指示される暗号鍵生成回路 E K 1 __ s、E K 1 __ m が生成する暗号鍵は時刻 t 2 において H ' A A とされている。暗号鍵生成回路 E K 1 __ s、E K 1 __ m はクロックサイクル C Y C 4 が始まる時刻 t 3 に H ' A A から H ' 6 7 に同期的に更新される。アドレスに対する暗号化はアドレス出力サイクル C Y C 3 の最初に行われなければならないから、C P U 2 は時刻 t 2 から始まるクロックサイクル C Y C 3 において、アクセスアドレスの元アドレス情報 H ' 0 0 0 1 1 0 を暗号鍵 H ' A A を用いてアドレス情報 H ' B 5 B 4 A 5 に暗号化し、これをアドレスバス A B U S に出力し、一方、E E P R O M 6 A はアドレスバス A B U S から暗号化アドレス情報 H ' B 5 B 4 A 5 を取り込み、これを暗号鍵 H ' A A で復号して、元のアドレス情報 H ' 0 0 0 1 1 0 を再生して取り込み、取り込んだアドレスに基づいて E E P R O M 6 A からデータを読み出し、読出されたデータは C P U 2 に取り込まれる。この動作中、アクセス対象とされていない R A M グループ 7 及び M R O M グループ 8 の暗号鍵に関する暗号鍵生成回路 E K 2 __ s、E K 2 __ m、E K 3 __ s、E K 3 __ m は暗号鍵の更新動作が抑止されている。尚、図 6 のアドレスの暗号化復号動作を行うとき図 2 におけるデータバスに対する暗号化復号機能を併用し、アドレスバスおよびデータバス双方に対して暗号化復号処理を行なうことは当然である。

20

30

【0039】

上記 I C カードマイコン 1 によれば以下の作用効果を得る。

【0040】

(1) バススレーブのグループ (6, 7, 8) 毎にバスマスタ及びバススレーブにおける暗号鍵の生成と更新をグループ化したから、バスアクセス動作において動作される暗号鍵生成回路はアクセス主体のバスマスタとアクセス対象とされるバススレーブを含むバススレーブのグループとに限定される。このように動作すべき暗号鍵生成回路を限定することにより、暗号鍵の更新動作等に伴う消費電力を低減することが可能になる。

40

【0041】

(2) また、バススレーブはその数より少ない数にグループ化されグループ毎に暗号鍵を割り当て、全てのバススレーブ毎に個別の暗号鍵を割り当てるものではないから、一つのバスマスタが保有すべき第 2 の暗号鍵生成回路の数はバススレーブの数よりも少なくなり、チップ面積の増大が過大なることはない。低消費電力とチップ面積増大のトレードオフを考慮すると、グループ化は例えば 10 グループ以下にするのがよい。チップ面積はグループ化数に比例して増えるが、消費電力はグループ化数が 10 程度までは漸次減少するがそれ以上では電力消費の低減率が収束してしまうからである。グループ化数が 10 程度を超えると暗号鍵生成回路の数が増える分だけ逆にそれぞれの記憶段等で消費される電力の増大を無視できなくなるからである。

50

【0042】

(3) 図1の例では暗号化復号回路をバスマスタ及びバススレーブのそれぞれのモジュールに設けたが、グループ単位で設ける構成と比較すると、後者の方がチップ面積は低減するが、暗号化前及び復号後の情報伝達距離が長くなり、不正アクセスの攻撃を受け易くなる。前者は内部バス上における機密保護を万全にするという観点において優れている。

【0043】

(4) 図1の例では暗号鍵生成回路をバスマスタ及びバススレーブのそれぞれのモジュールに設けたが、グループ単位で設ける構成と比較すると、後者の方がチップ面積は低減するが暗号鍵を伝達する配線の引き回しが長くなり、暗号鍵それ自体に対する不正アクセスの攻撃を受け易くなる。前者は内部バス上における機密保護を万全にするという観点において優れている。

10

【0044】

図7には暗号鍵生成回路の一例が示される。代表的に示された暗号鍵生成回路EK1__mは初段への帰還経路に乱数発生器(RNG)40の出力と論理演算を行う論理ゲートEOR1を備えたリニアフィードバックシフトレジスタ(LFSR)としてのリングカウンタ41を有し、前記リングカウンタ41の計数値が暗号鍵Kecとされる。論理ゲートEOR1として例えば排他的論理和回路を採用する。リングカウンタ41は例えば直列接続された4個のフリップフロップFFを備え、4個のフリップフロップFFからの並列出力が暗号鍵Kecとされる。例えばデータバスDBUSのビット数が32ビットであるとき、データビット4ビット毎に暗号鍵Kecを用いて暗号化及び復号を行えばよい。乱数発生器40は例えば真正乱数発生器とすればよい。リングカウンタ41のシフト動作はクロック信号CLKに同期される。リセット信号RSTがイネーブルにされることによって暗号鍵Kecが初期化される。更に高い乱数性が必要になる場合はLFSRの段数を増やせばよい。その他の暗号鍵生成回路も同様に構成してよい。

20

【0045】

図8には暗号鍵生成回路の別の例が示される。同図に示される暗号鍵生成回路EK1__mは真正乱数発生器に代えて、セレクトASEL1と排他的論理ゲートEOR2を用いた擬似乱数発生を採用する。排他的論理和ゲートEOR2は例えばデータバスDBUSを入力する。セレクトASEL1は論理値1又排他的論理和ゲートEOR2の出力を選択信号Sseに従って選択する。選択信号Sseは例えばデータバスの適宜の1ビット等のような任意性のあるデータビットであればよい。その他の暗号鍵生成回路も同様に構成してよい。

30

【0046】

図9には暗号鍵生成回路に対するリセット動作の同期制御形態が例示される。バスマスタとバススレーブ間において相互に同じ暗号鍵を同期的に生成すべき暗号鍵生成回路同士を同じリセット信号でリセットすればよい。図9に代表的に示された例では、EEPROMグループ6の暗号鍵生成回路EK1__sとEEPROMグループ6をアクセス可能なバスマスタ(CPU2)が備える暗号鍵生成回路EK1__mとを同じリセット信号RST1でリセット可能とし、また、RAMグループ7の暗号鍵生成回路EK2__sとRAMグループ7をアクセス可能なバスマスタ(CPU2, DMAC12)が備える暗号鍵生成回路EK2__mとを同じリセット信号RST2でリセット可能とする。この例では何れの暗号鍵生成回路も初期値は共通化される。

40

【0047】

図10には暗号鍵生成回路に対するリセット動作の別の同期制御形態が例示される。バスマスタとバススレーブ間において相互に同じ暗号鍵を同期的に生成すべき暗号鍵生成回路同士を同じ書込み信号を用いて同じ値にプリセット可能とするものである。図10に代表的に示された例では、EEPROMグループ6の暗号鍵生成回路EK1__sのLFSRとEEPROMグループ6をアクセス可能なバスマスタ(CPU2)が備える暗号鍵生成回路EK1__mのLFSRとを同じ書込み信号WS1で初期化データをプリセット可能と

50

し、また、RAMグループ7の暗号鍵生成回路EK2__sのLFSRとRAMグループ7をアクセス可能なバスマスタ(CPU2, DMA C12)が備える暗号鍵生成回路EK2__mのLFSRと同じ書込み信号WS2で初期化データをプリセット可能とする。プリセットすべき初期化データ及び書込み信号は暗号鍵初期化回路(ITC)43が出力する。初期化データの転送路は例えば専用バス44で構成する。暗号鍵初期化回路43は例えばSYSC3が備え、パワーオンリセット若しくはシステムリセットに応答して初期化データのプリセット動作を制御する。図10の構成に適用する前記LFSRは図7及び図8のLFSR41に対して書込み信号がイネーブルにされたときフリップフロップFFのデータ入力端子にプリセットデータが並列に入力されるように構成される。

【0048】

10

以上本発明者によってなされた発明を実施形態に基づいて具体的に説明したが、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

【0049】

例えば、上記説明では暗号化復号回路をバスマスタ及びバススレーブのそれぞれのモジュールに設けたが、グループ単位で設ける構成を採用することも可能である。また、暗号鍵生成回路についてもバスマスタ及びバススレーブのそれぞれのモジュールに設けたが、グループ単位で設ける構成を採用することも可能である。更に、バス暗号化はアドレスバスとデータバスの双方に対して行う場合に限定されず、何れか一方のバス情報に対してだけ暗号化を行うようにしてもよい。アドレス情報に対する暗号化を行わない場合には非暗号化アドレスバスは不要であり、バスコントローラはアドレスバスからアドレス信号を入力してモジュール選択信号を生成すればよい。データバス情報の暗号化復号に用いる暗号鍵とアドレスバス情報の暗号化復号に用いる暗号鍵とを別々にすることも可能である。バスマスタはCPUとDMACに限定されず、その他のアドレッシング機能を有するコントローラであってもよい。バススレーブは揮発性メモリ及び不揮発性メモリに限定されず、入出力インタフェース回路等であってもよい。その他、暗号鍵の生成論理や、バス暗号化の論理ゲートは適宜変更可能である。

20

【図面の簡単な説明】

【0050】

【図1】本発明に係る半導体集積回路の一例であるICカードマイコンのブロック図である。

30

【図2】ICカードマイコンにおけるデータバスの暗号化復号機能の詳細を例示するブロック図である。

【図3】バスの暗号化復号論理の一例を示す論理回路図である。

【図4】図2の回路におけるデータの暗号化復号動作のタイミングチャートである。

【図5】ICカードマイコンにおけるアドレスバスの暗号化復号機能の詳細を例示するブロック図である。

【図6】図5の回路におけるアドレスの暗号化復号動作のタイミングチャートである。

【図7】暗号鍵生成回路の一例を示す論理回路図である。

【図8】暗号鍵生成回路の別の例を示す論理回路図である。

40

【図9】暗号鍵生成回路に対するリセット動作の同期制御形態を例示するブロック図である。

【図10】暗号鍵生成回路に対するリセット動作の別の同期制御形態を例示するブロック図である。

【符号の説明】

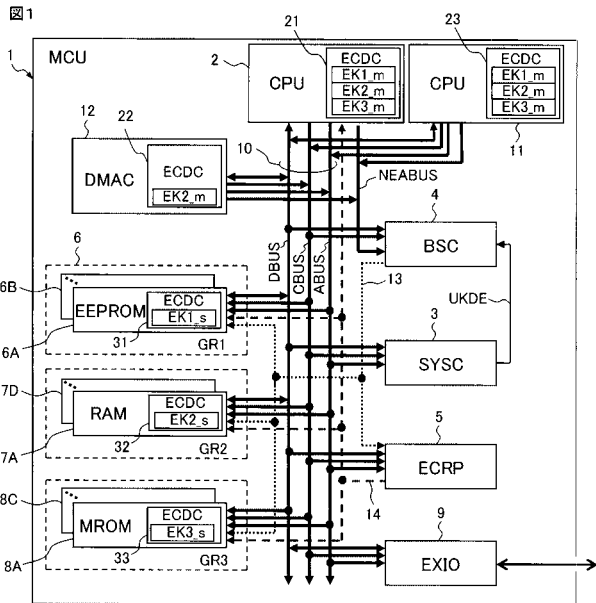
【0051】

- 1 ICカードマイコン
- 2、11 CPU
- 3 システムコントローラ(SYSC)
- DBUS データバス

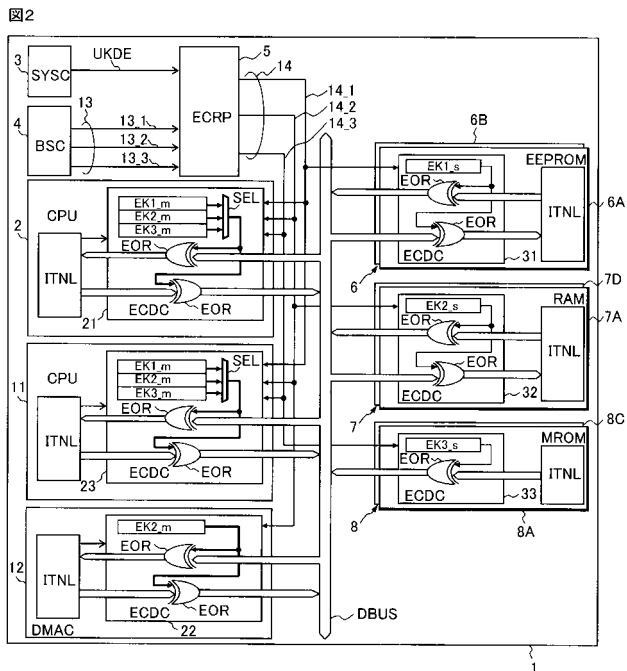
50

- A B U S アドレスバス
 C B U S コントロールバス
 N E A B U S 非暗号化アドレス
 5 暗号鍵制御回路 (E C R P)
 6 A ~ 6 B エレクトリカリ・イレーザブル・アンド・プログラマブルROM (E E P R O M)
 7 A ~ 7 D ランダムアクセスメモリ (R A M)
 8 A ~ 8 C マスクROM (M R O M)
 6 EPROMグループ (G R 1)
 7 RAMグループ (G R 2)
 8 MROMグループ (G R 3)
 1 0 内部バス
 1 2 ダイレクトメモリアクセスコントローラ (D M A C)
 1 3 モジュール選択信号
 1 4 暗号鍵更新制御信号
 2 1 ~ 2 3 バスマスタの暗号化復号回路 (E C D C)
 3 1 ~ 3 3 バススレーブの暗号化復号回路
 E K 1 _ s ~ E K 3 _ s バススレーブの暗号鍵生成回路 (第 1 の暗号鍵生成回路)
 E K 1 _ m ~ E K 3 _ m バスマスタの暗号鍵生成回路 (第 2 の暗号鍵生成回路)

【図 1】

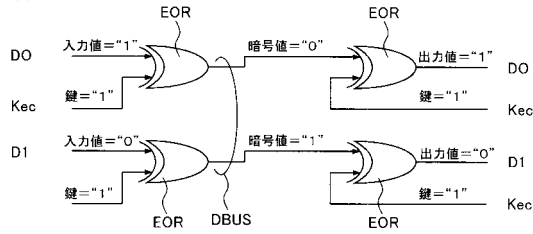


【図 2】



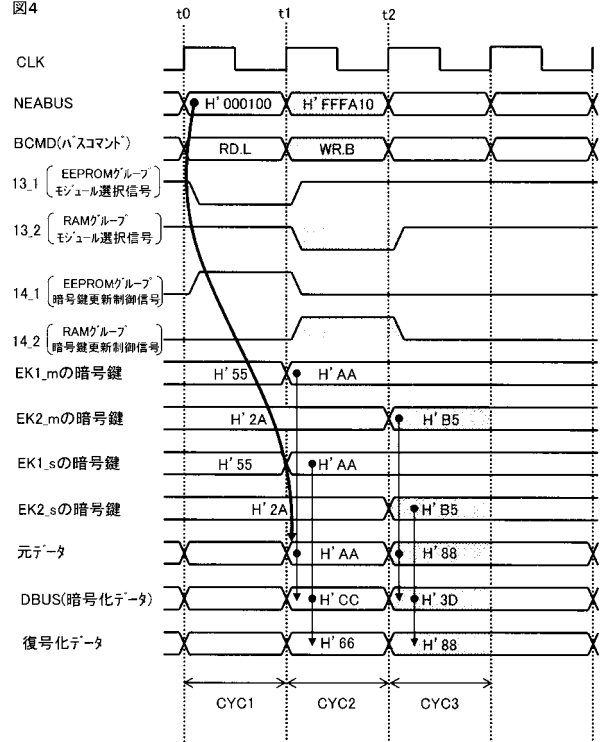
【図 3】

図3



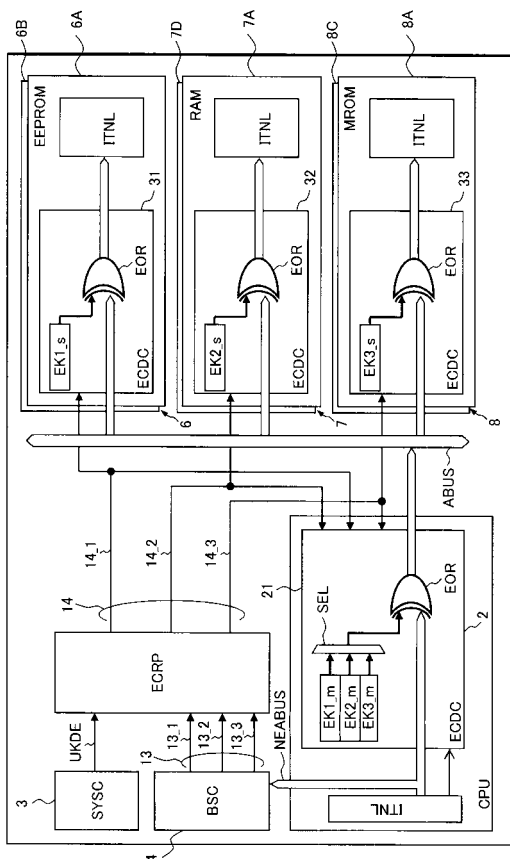
【図 4】

図4



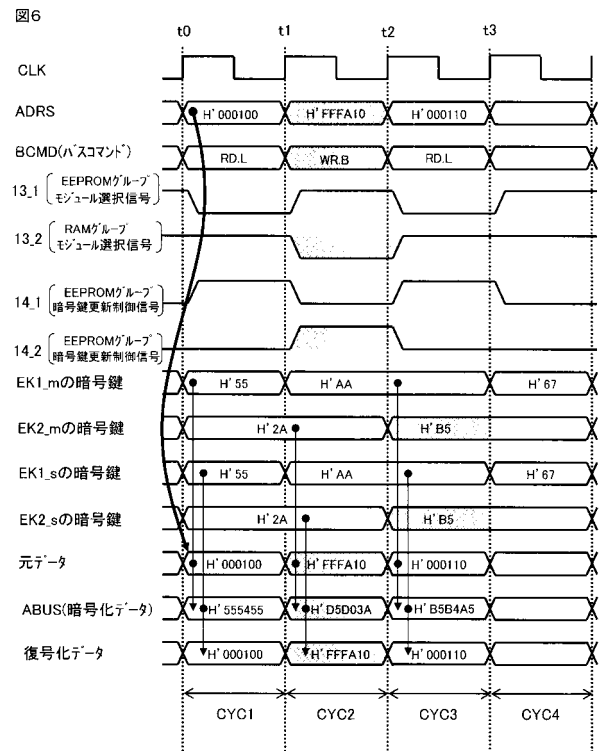
【図 5】

図5



【図 6】

図6



フロントページの続き

(72)発明者 豊嶋 誠

東京都千代田区丸の内二丁目4番1号 株式会社ルネサステクノロジ内

Fターム(参考) 5B017 AA07 BA07 CA14

5J104 AA16 AA32 AA34 EA04 EA15 EA16 JA03 NA02 NA27 NA37
NA39