

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4764387号
(P4764387)

(45) 発行日 平成23年8月31日 (2011.8.31)

(24) 登録日 平成23年6月17日 (2011.6.17)

(51) Int.Cl.		F I		
G06F 15/78	(2006.01)	G06F 15/78	510P	
G06F 1/04	(2006.01)	G06F 1/04	301C	
G06F 1/32	(2006.01)	G06F 1/00	332Z	

請求項の数 8 (全 11 頁)

(21) 出願番号	特願2007-207488 (P2007-207488)	(73) 特許権者	302062931
(22) 出願日	平成19年8月9日 (2007.8.9)		ルネサスエレクトロニクス株式会社
(65) 公開番号	特開2009-43044 (P2009-43044A)		神奈川県川崎市中原区下沼部 1 7 5 3 番地
(43) 公開日	平成21年2月26日 (2009.2.26)	(74) 代理人	100089071
審査請求日	平成22年7月26日 (2010.7.26)		弁理士 玉村 静世
		(72) 発明者	高木 克泰
			東京都千代田区大手町二丁目6番2号 株
			式会社ルネサステクノロジ内
		(72) 発明者	伊東 久範
			東京都千代田区大手町二丁目6番2号 株
			式会社ルネサステクノロジ内
		審査官	三坂 敏夫

最終頁に続く

(54) 【発明の名称】 半導体装置

(57) 【特許請求の範囲】

【請求項 1】

クロックサイクルに同期動作しアクセスを要求することができる第1回路と、前記第1回路からのアクセス要求に応答して第2回路をアクセス制御する第3回路と、前記第2回路からのアクセス応答があるまで第3回路が第1回路に動作の休止を指示する期間に電流消費動作を行う電流消費回路とを有し、

前記電流消費回路は第1回路に指示された動作の休止期間における消費電流量の低下を抑制するために前記クロックサイクル毎に電流消費動作を行い、

前記電流消費回路は複数個の電流消費ユニットを有し、前記第1回路の動作休止期間に、電流消費動作を行う前記電流消費ユニットの数が可変可能にされる、半導体装置。

10

【請求項 2】

前記電流消費ユニットの数を指定する制御データを保有するフラッシュメモリと、前記フラッシュメモリから出力された前記制御データをデコードして電流消費動作を行う前記電流消費ユニットを選択するための選択信号を生成するデコーダとを有する、請求項1記載の半導体装置。

【請求項 3】

前記デコーダは制御データの全ビットの値が0又は1の何れにおいても電流消費動作を行う前記電流消費ユニットの数をゼロとする、請求項2記載の半導体装置。

【請求項 4】

前記第1回路は命令を実行する中央処理装置であり、前記第2回路は前記第1回路より

20

も動作速度の遅い回路であり、前記第 3 回路はバスステートコントローラであり、

前記第 3 回路は第 1 回路に命令実行動作をストールする指示によって前記動作の休止を指示する、請求項 1 乃至 3 の何れか 1 項に記載の半導体装置。

【請求項 5】

第 1 回路と、前記第 1 回路とは相補的に動作され且つ第 1 回路よりも動作時の消費電流量が大きな第 2 回路と、前記第 2 回路が動作を待ち第 1 回路が動作する期間の消費電流量と前記第 1 回路が動作を待ち第 2 回路が動作する期間の消費電流量との差分を補填するために前者の期間に電流を消費する電流消費回路と、を有する半導体装置。

【請求項 6】

前記電流消費回路は半導体装置全体に分散配置されている、請求項 5 記載の半導体装置

10

【請求項 7】

前記電流消費回路は前記第 2 回路よりも前記第 1 回路寄りに多く配置されている、請求項 6 記載の半導体装置。

【請求項 8】

前記第 1 回路及び第 2 回路はクロック信号のクロックサイクルに同期して動作し、前記電流消費回路は前記クロックサイクル毎に電流消費動作を行う、請求項 7 記載の半導体装置。

【発明の詳細な説明】

【技術分野】

20

【0001】

本発明は、半導体装置における電流消費技術に関し、例えば消費電流に時間的偏り若しくは場所的偏りの大きなデータ処理用又は通信用の半導体装置に適用して有効な技術に関する。

【背景技術】

【0002】

特許文献 1 にはパワーダウンモードと通常モードの切換え時に負荷電流の変動による電源電圧の変動を抑制する電流消費回路を搭載した半導体装置について記載される。これは、負荷に急激な電流が流れる前に電流消費回路に電流を流し、負荷電流が急激に減少する前に電流消費回路による電流消費を減少させたりして、急激な電流変動を抑制しようとするものである。

30

【0003】

特許文献 2 には電流量変化に起因して起こる電源電圧変動を低減するために、パルス発生回路の動作率（活性率）を検出する動作検出回路と、その検出回路による検出信号により電流を消費させる電流消費回路とから成る過渡電流低減回路を備えた半導体装置について記載される。

【0004】

【特許文献 1】特開 2003 - 258617 号公報

【特許文献 2】特開平 10 - 090370 号公報

【発明の開示】

40

【発明が解決しようとする課題】

【0005】

本発明者は中央処理装置のパイプラインストールによる消費電流量の低下による影響を検討した。中央処理装置が低速モジュールをアクセスしてデータを取得するまでの間に命令実行動作がストールされると消費電流量が大きく低下することに着目した。中央処理装置による消費電流量は大きいから、その休止期間に消費電流量が低下すると、パイプラインストールの前後で電源電圧が変動する可能性がある。この消費電流量の低下を抑制するにはその期間に電流を消費させればよいが、予めその電流量を見積もることは難しい。上記特許文献ではこの点にいて考慮されていない。

【0006】

50

さらに本発明者は電流消費回路について検討した結果、回路の消費電力や漏洩電磁波などから秘密情報を奪うサイドチャネル攻撃に対して、電流量、電流を流すタイミングをコントロール可能な電流消費回路は、消費電力や、漏洩電磁波をかく乱させるのに有用であることを見出した。

【0007】

本発明の目的はクロックサイクルに同期する回路による電力消費状態の相違に起因する電源電圧の変動を容易に抑制することができる半導体装置を提供することにある。

【0008】

本発明の別の目的はサイドチャネル攻撃に対して回路の消費電力や漏洩電磁波を容易に攪乱させることができる半導体装置を提供することにある。

10

【0009】

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】

【0010】

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。

【0011】

すなわち、クロックサイクルに同期動作しアクセスを要求することができる第1回路がアクセス要求に対する応答を待っているとき、電流消費動作を行う電流消費回路を採用する。前記電流消費回路は第1回路に指示された動作の休止期間における消費電流量の低下を抑制するために前記クロックサイクル毎に電流消費動作を行い、電流消費動作を行う複数の電流消費ユニットを有する。前記第1回路の動作休止期間に、電流消費動作を行う前記電流消費ユニットの数は可変可能にされる。

20

【0012】

上記より、電流消費回路により第1回路の動作休止期間に消費電流量が低下するのを抑制することができる。電流消費回路による消費電流量は動作選択される電流消費ユニットの数によって設定されるから、予めその電流量を見積もることは難しい場合にも容易に対応することができる。

【0013】

また、相補的に動作される回路の消費電流量の相違を補填するように電流消費動作を行う電流消費回路を採用することにより、内部の動作状態の相違を消費電流量から推測し難くなる。

30

【発明の効果】

【0014】

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とおりである。

【0015】

すなわち、クロックサイクルに同期する回路による電力消費状態の相違に起因する電源電圧の変動を容易に抑制することができる。

40

【0016】

サイドチャネル攻撃に対して回路の消費電力や漏洩電磁波を容易に攪乱させることができる。

【発明を実施するための最良の形態】

【0017】

1. 実施の形態の概要

先ず、本願において開示される発明の代表的な実施の形態について概要を説明する。代表的な実施の形態についての概要説明で括弧を付して参照する図面中の参照符号はそれが付された構成要素の概念に含まれるものを例示するに過ぎない。

【0018】

50

〔 1 〕半導体装置はクロックサイクルに同期動作しアクセスを要求することができる第 1 回路 (2) と、前記第 1 回路からのアクセス要求に応答して第 2 回路 (5) をアクセス制御する第 3 回路 (4) と、前記第 2 回路からのアクセス応答があるまで第 3 回路が第 1 回路に動作の休止を指示する期間に電流消費動作を行う電流消費回路 (2 0) とを有する。前記電流消費回路は第 1 回路に指示された動作の休止期間における消費電流量の低下を抑制するために前記クロックサイクル毎に電流消費動作を行う。前記電流消費回路は複数個の電流消費ユニット (2 1) を有し、前記第 1 回路の動作休止期間に、電流消費動作を行う前記電流消費ユニットの数が可変可能にされる。

【 0 0 1 9 】

上記より、電流消費回路により第 1 回路の動作休止期間に消費電流量が低下するのを抑制することができる。電流消費回路による消費電流量は動作選択される電流消費ユニットの数によって設定されるから、予めその電流量を見積もることは難しい場合にも容易に対応することができる。

【 0 0 2 0 】

〔 2 〕項 1 の半導体装置は更に、前記電流消費ユニットの数を指定する制御データ (C D A T) を保有するフラッシュメモリ (6) と、前記フラッシュメモリから出力された前記制御データをデコードして電流消費動作を行う前記電流消費ユニットを選択するための選択信号を生成するデコーダ (2 2) とを有する。動作選択すべき電流消費ユニットの数に応じてフラッシュメモリから読み出す制御データを決めればよい。例えば半導体装置のリセット指示解除後の初期化動作においてフラッシュメモリから初期値をデコーダに供給すればよい。

【 0 0 2 1 】

〔 3 〕項 2 の半導体装置において前記デコーダは制御データの全ビットの値が 0 又は 1 の何れにおいても電流消費動作を行う前記電流消費ユニットの数をゼロとする。フラッシュメモリの初期状態において制御データは全ビット 0 又は 1 の何れかになるかが不定の異場合に、意に反して過大な電流が流れることを防止することができる。

【 0 0 2 2 】

〔 4 〕以上の半導体装置において、前記第 1 回路は命令を実行する中央処理装置であり、前記第 2 回路は前記第 1 回路よりも動作速度の遅い回路であり、前記第 3 回路はバスステートコントローラである。前記第 3 回路は第 1 回路に命令実行動作をストールする指示によって前記動作の休止を指示する。半導体装置は例えばマイクロコンピュータである。

【 0 0 2 3 】

〔 5 〕本発明の別の観点による半導体装置は、第 1 回路 (7 1) と、前記第 1 回路とは相補的に動作され且つ第 1 回路よりも動作時の消費電流量が大きな第 2 回路 (7 2) と、前記第 2 回路が動作を待ち第 1 回路が動作する期間の消費電流量と前記第 1 回路が動作を待ち第 2 回路が動作する期間の消費電流量との差分を補填するために前者の期間に電流を消費する電流消費回路 (8 1 , 8 2) とを有する。

【 0 0 2 4 】

これにより、内部の動作状態の相違を消費電流量から推測し難くなり、サイドチャネル攻撃に対して回路の消費電力や漏洩電磁波を容易に攪乱させることができる。

【 0 0 2 5 】

〔 6 〕項 5 の半導体装置において、前記電流消費回路は半導体装置全体に分散配置、若しくは満遍なく配置されている。また、前記電流消費回路は前記第 2 回路よりも前記第 1 回路寄りに多く配置されている。これにより、回路配置の点からも消費電流量の相違を把握することを難しくすることができる。

【 0 0 2 6 】

〔 7 〕項 6 の半導体装置において前記第 1 回路及び第 2 回路はクロック信号のクロックサイクルに同期して動作し、前記電流消費回路は前記クロックサイクル毎に電流消費動作を行う。クロック同期という動作形態の点からも消費電流量の相違を把握することを難しくすることができる。

10

20

30

40

50

【 0 0 2 7 】

２．実施の形態の詳細

《中央処理装置のストール時における消費電流量の低下の抑制》

図１には本発明の一例に係るマイクロコンピュータ１が例示される。同図に示されるマイクロコンピュータ１は、特に制限されないが、単結晶シリコン等の半導体基板に公知の相補型ＭＯＳ集積回路製造技術によって形成される。

マイクロコンピュータ１はその実装基板（図示せず）に搭載された外部電源回路としての外部電圧レギュレータ（ＶＰＲＥＧＵ）１０から動作電源電圧ＶＣＣが供給される。

【 0 0 2 8 】

マイクロコンピュータ１はクロック信号ＣＬＫに同期動作され、命令を実行する中央処理装置（ＣＰＵ）２を有する。中央処理装置２はフェッチした命令を解釈して実行するとき、演算等に必要なオペランドをフェッチしたり、次に実行する命令をフェッチしたりするためにアクセスを要求する。中央処理装置２が発行するアクセス要求が高速アクセスモジュール（ＨＳＭＤＬ）３に対するものであれば、高速アクセスモジュール３はそれに対応してデータ等を中央処理装置２に返す。高速アクセスモジュール３は例えば内部ＲＡＭ（ランダム・アクセス・メモリ）等である。中央処理装置２及び高速アクセスモジュールは、特に制限されないが、クロック信号ＣＬＫのサイクル単位で動作を行う。例えば中央処理装置２は命令をパイプラインで実行し、見掛け上１命令をクロック信号ＣＬＫの１サイクルで実行する能力を有する。但し、演算ステージにおいて演算に必要なデータが揃っていないような場合には、データが揃うまでパイプラインがストールされる。また、プリフェッチキューに実行可能な命令が溜まっていないような場合にもパイプラインストールを生ずる。パイプラインストールが生ずると、各パイプラインステージはＮＯＰ（ノン・オペレーション）とされ、その期間、ＣＰＵ２は命令実行動作を休止する。パイプラインストールは、あるパイプラインステージの処理に、それより前のパイプラインのステージによる処理結果が必要とされるときに、必要な処理結果が揃っていないときに発生することになる。

【 0 0 2 9 】

中央処理装置２が発行するアクセス要求は、バスステートコントローラ（ＢＳＣ）４にも供給される。バスステートコントローラ４にはフラッシュメモリ（ＦＬＡＳＨ）６及びその他の低速アクセスモジュール（ＬＳＭＤＬ）５が接続される。バスステートコントローラ４は中央処理装置２からのアクセス要求がフラッシュメモリ６又はその他の低速アクセスモジュール５（フラッシュメモリ６及びその他の低速アクセスモジュール５を単に低速アクセスモジュール５，６とも称する）に対するものであるとき、低速アクセスモジュール５，６の動作速度等に合わせて低速アクセスモジュール５，６をアクセス制御する。そのアクセス要求がリードアクセスであれば、その応答結果であるリードデータが低速アクセスモジュール５，６からバスステートコントローラ４に与えられ、バスステートコントローラ４はそのデータをアクセス要求元である中央処理装置２に返す。

【 0 0 3 0 】

バスステートコントローラ４は中央処理装置２からのアクセス要求に対する応答を中央処理装置２に返すまでの間、ストール信号ＳＴＬを中央処理装置２に出力する。ストール信号ＳＴＬがアサートされると、中央処理装置２はそれ以降パイプラインの各ステージをノンオペレーションとすることにより、それがネゲートされるまで命令実行動作をストール、即ち命令実行動作を休止する。

【 0 0 3 1 】

マイクロコンピュータ１は、ストール信号ＳＴＬを入力することにより、前記命令実行動作のストール期間に呼応して電流消費動作を行う電流消費回路２０を有する。電流消費回路２０は複数の電流消費ユニット（ＣＬＤＵ）２１＿１～２１＿ｉを有する。前記電流消費動作を行う前記電流消費ユニットの数は電流消費制御回路（ＣＬＤＣＮＴ）２２からの指示に従って可変可能にされる。そのための制御データＣＤＡＴはフラッシュメモリ６が保有する。例えばリセット信号ＲＥＳによるリセット指示が解除されたとき、フラッシ

メモリ 6 から電流消費制御回路 22 に制御データ C D A T がイニシャルロードされ、それを電流消費制御回路 22 がデコードすることによって電流消費動作を行う電流消費ユニット 21 を選択する選択信号としてのイネーブル信号 E N B __ 1 ~ E N B __ i を生成する。

【 0 0 3 2 】

電流消費ユニットは、その配置個所に制限はなく、半導体装置全体にまんべんなく自由に配置することが可能である。

【 0 0 3 3 】

図 2 には電流消費ユニット 21 __ i の具体例が示される。電流消費ユニット 21 __ i は例えば複数個の単位回路 30 __ 1 ~ 30 __ j を有する。各単位回路 30 __ 1 ~ 30 __ j にはストール信号 S T L、対応するイネーブル信号 E N B __ i、及びクロック信号 C L K が供給される。

【 0 0 3 4 】

単位回路 30 __ 1 は直列接続された複数個のロードセル (L D C) 40 を有し、その最終段のロードセル 4 の出力に D 型ラッチ回路 (L A T) 41 のデータ入力端子が接続される。ラッチ回路 41 のデータ出力端子はナンドゲート (N A N D) 42 とノアゲート (N O R) 43 の夫々の一方の入力端子に帰還結合され、夫々の出力はセクタ 44 で選択され、選択された出力が初段のロードセル 40 の入力端子に結合される。前記ストール信号 S T L と対応するイネーブル信号 E N B __ i はアンドゲート 45 で論理積が採られ、その論理積信号が前記ナンドゲート 42 の他方の入力端子に供給され、前記論理積信号の反転信号が前記ノアゲート 43 の他方の入力端子に供給される。セクタ 44 は選択信号 i v s が 1 のときノアゲート 43 の出力を選択し、選択信号 i v s が 0 のときナンドゲート 42 の出力を選択する。アンドゲート 45 の初期出力は 0 であるから、ナンドゲート 42 の初期出力は 1、ノアゲート 43 の初期出力は 0 になる。セクタ 44 によってナンドゲート 42 の出力が選択されている状態では、ラッチ回路 41 のラッチ動作によってセクタ 44 の出力がナンドゲート 42 に帰還入力されると、その度にナンドゲート 42 の出力が反転される。セクタ 44 によってノアゲート 43 の出力が選択されている状態では、ラッチ回路 41 のラッチ動作によってセクタ 44 の出力がノアゲート 43 に帰還入力されると、その度にノアゲート 43 の出力が反転される。従ってセクタ 44 の出力は図 3 に例示されるようにクロック信号 C L K の 2 倍の周期でクロック変化される。選択信号 i v s = 1 のときのクロック変化と、i v s = 0 のときのクロック変化は位相が 180 度ずれている。

【 0 0 3 5 】

ロードセル 4 は図 4 に例示されるように入力 A を直列 2 段にインバータ 50, 51 を通して出力 Y とする。入力 A のインバータ 50 による反転信号は遅延回路 (D L Y) 54 で遅延され、遅延回路 54 の出力と、入力 A のインバータ 50、52 による非反転信号とをアンドゲート 56 に受け、その出力で n チャンネル型の駆動 M O S トランジスタ 57 をスイッチ制御する。アンドゲート 56 の出力 e n は、図 5 に例示されるように、入力 A のクロックデューティよりも小さなデューティのクロック波形とされ、出力 e n が 1 にされる期間に駆動 M O S トランジスタ 57 がオン動作され、電流 I d を流す。

【 0 0 3 6 】

ロードセルの入力 A に供給されるパルス波形は図 3 の i v s = 1 の時の波形又は i v s = 0 の時の波形であり、一つの単位回路 30 が電流を流す動作はクロック信号 C L K の 2 サイクルに 1 度となる。クロック信号 C L K は中央処理装置 2 の動作サイクルであるから、そのサイクル毎に電流を流す動作を行うように、半分の単位回路 30 は i v s = 1 にされ、残り半分の単位回路 30 は i v s = 0 にされる。これにより、一つの電流消費ユニット 21 __ i はクロック信号 C L K のサイクル毎に同じ電流を流すことができる。特に図示はしないがその他の電流消費ユニットも同様に構成される。

【 0 0 3 7 】

図 6 には前記電流消費制御回路 (C L D C N T) 22 のデコード論理 (D E C) が例示

される。ここでは制御データを3ビットとし、6本のイネーブル信号 $ENB_1 \sim ENB_6$ を生成するものとし、便宜上1本のイネーブル信号毎に2個の電流消費ユニットを割り当てたものとする内容になっている。特に制御データ $CDA T$ の値が全ビットの値が0又は1の何れにおいても電流消費動作を行う電流消費ユニットの数をゼロとするデコード論理を備える。上記制御により、動作させるモジュール数を任意に選択することが可能であるから、状況に応じて必要な電流消費を発生することが可能となる。

【0038】

以上説明したマイクロコンピュータによれば以下の作用効果を得る。

(1) 電流消費回路20により中央処理装置2の動作休止期間に消費電流量が低下するのを抑制することができる。電流消費回路20による消費電流量は動作選択される電流消費ユニット21の数によって設定されるから、予めその電流量を見積もることは難しい場合にも容易に対応することができる。

10

(2) 図3の電流波形で例示されるように、中央処理装置2のクロック同期動作と同様に中央処理装置2の動作クロックサイクル毎に電流を流すことができる。

(3) 図2に例示されるように電流消費ユニット21には順序回路としてラッチ回路41が配置されているので、自動配置配線において電流消費ユニット21もイベントドリブンのようなタイミング検証の対象にすることができ、人手の介在を極力減らすことが可能である。

(4) 前記電流消費制御回路22は制御データの全ビットの値が0又は1の何れにおいても電流消費動作を行う前記電流消費ユニットの数をゼロとする。フラッシュメモリ6の初期状態において制御データ $CDA T$ は全ビット0又は1の何れかになるかが不定の場合に、意に反して過大な電流が流れることを防止することができる。

20

【0039】

《耐タンパー性向上のための消費電流量低下の抑制》

次に、耐タンパー性が要求される回路、例えば RSA 暗号回路等に電流消費回路を適用して、耐タンパー性を向上させる例について説明する。

【0040】

例えばバイナリー(Binary)法によるべき乗剰余演算回路を用いた暗号回路での例を挙げる。べき乗剰余演算回路アルゴリズムは例えば、

Input: $Z, N, E = (e_{k-1}, \dots, e_1, e_0)_2$

30

Output: $Z = XE \bmod N$

1: $Z := 1;$

2: for $i = k-1$ downto 0

3: $Z := Z * Z \bmod N;$

4: if $(e_i == 1)$ then

5: $Z := Z * X \bmod N;$

6: endif

7: end for

のように記述される。

【0041】

40

図7には上記アルゴリズムを使用した回路の全体図が例示される。上記アルゴリズムの“4:”の記述行において e_i の値によって処理が分岐している。この回路規模を図中のブロックの大きさで現したのが、図7に記載された「第1回路71」($e_i == 0$ の処理)、「第2回路72」($e_i == 1$ の処理)である。第1回路71と第2回路72は相補的に動作される。

【0042】

第1回路71と第2回路72には回路規模に差があるため、図8に例示されるように、 e_i の値によって消費電力が異なる。第2回路72の方が消費電流量が多い。また、これら回路をチップ上にレイアウトした時の配置を図9とすると、その輻射電磁波は図10に示すように偏りとその強さの差も見えてしまう。これらの消費電力と輻射電磁波の差からサ

50

イドチャネル攻撃を受けやすくなっている。

【 0 0 4 3 】

そこで図 1 1 のように前記電流消費ユニット 2 1 を有する複数の電流消費回路 8 1 , 8 2 を電流差分を埋めるように半導体装置のチップ (Chip) 全体に配置する。これにより図 1 2 に例示されるように電流消費の差が見えなくなり、図 1 3 に示すように輻射電磁波をかく乱することも可能になる。

【 0 0 4 4 】

また、電流消費回路 8 1 , 8 2 を構成する電流消費ユニット 2 1 を標準の M O S を使用してセル化すると、レイアウト的に標準セルと見分けがつかないので、配置されていることも見破りづらく、配置も自由にできるので攪乱源として見破られにくい。

10

【 0 0 4 5 】

上記により、回路の消費電力や漏洩電磁波などから秘密情報を奪うサイドチャネル攻撃に対して、電流量、電流を流すタイミングをコントロール可能な電流消費回路を用いることにより、消費電力や、漏洩電磁波をかく乱させることが可能になる。

【 0 0 4 6 】

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。

【 0 0 4 7 】

中央処理装置のストール時における消費電流量の低下の抑制を一例として説明した構成はマイクロコンピュータだけでなく、画像処理、音声処理、暗号化復号処理等の各種アクセラレータにも適用することができる。本発明は高速通信モジュールが通信する際に消費する電流と、停止時の電流変動を抑える場合にも適用することができる。

20

【図面の簡単な説明】

【 0 0 4 8 】

【図 1】図 1 は本発明の一例に係るマイクロコンピュータのブロック図である。

【図 2】図 2 は電流消費ユニットの具体例を例示する論理回路図である。

【図 3】図 3 は電流消費ユニットの動作タイミングを例示するタイミングチャートである。

。

【図 4】図 4 はロードセルの具体例を例示する論理回路図である。

30

【図 5】図 5 はロードセルの動作タイミングを例示するタイミングチャートである。

【図 6】図 6 は電流消費制御回路のデコード論理を例示する説明図である。

【図 7】図 7 はべき剰余演算回路アルゴリズムを使用する回路を全体的に示したブロック図である。

【図 8】第 1 回路と第 2 回路における e_i の値によって相違される消費電力を示す説明図である。

【図 9】図 7 の回路をチップ上にレイアウトした時の配置を例示する平面図である。

【図 10】図 9 のレイアウトにおける輻射電磁波の分布を例示する平面図である。

【図 11】電流消費回路を半導体装置のチップに配置した状態を例示する平面図である。

【図 12】電流消費回路の配置によって第 1 回路と第 2 回路の相補動作によって電流消費の差が見えなくなる様子を例示する説明図である。

40

【図 13】電流消費回路によって輻射電磁波をかく乱する様子を例示する平面図である。

【符号の説明】

【 0 0 4 9 】

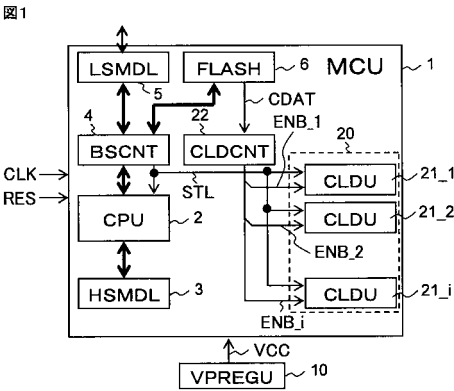
- 1 マイクロコンピュータ (MCU)
- 10 外部電圧レギュレータ (VREGU)
- CLK クロック信号
- 2 中央処理装置 (CPU)
- 3 高速アクセスモジュール (HSMDL)
- 4 バスステートコントローラ (BSC)

50

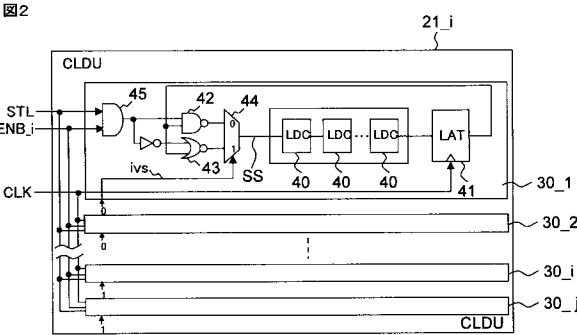
- 6 フラッシュメモリ (F L A S H)
- 5 低速アクセスモジュール (L S M D L)
- STL ストール信号
- 20 電流消費回路
- 21_1 ~ 21_i 電流消費ユニット (C L D U)
- 22 電流消費制御回路 (C L D C N T)
- C D A T 制御データ
- ENB_1 ~ ENB_i イネーブル信号
- 30_1 ~ 30_j 単位回路
- 40 ロードセル (L D C)
- ivs セレクタ選択信号
- 71 第1回路
- 72 第2回路

10

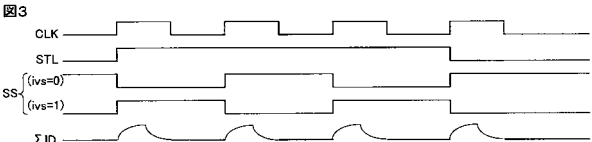
【 図 1 】



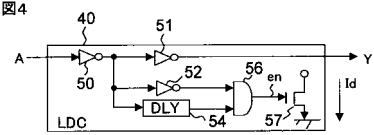
【 図 2 】



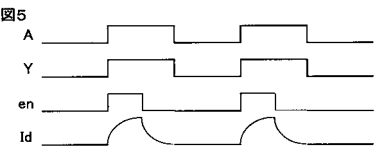
【 図 3 】



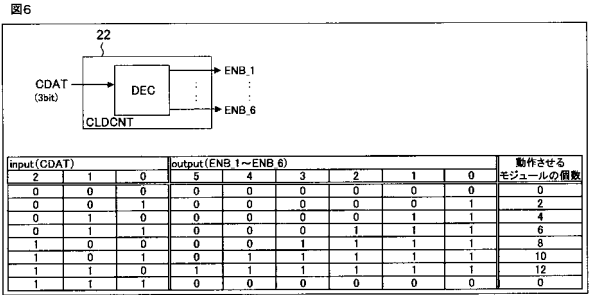
【 図 4 】



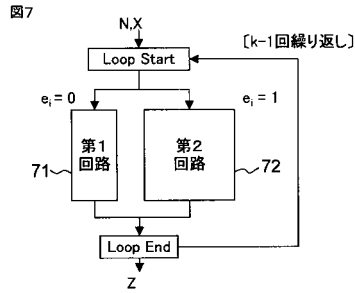
【 図 5 】



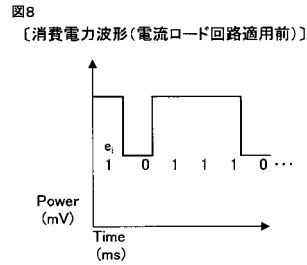
【 図 6 】



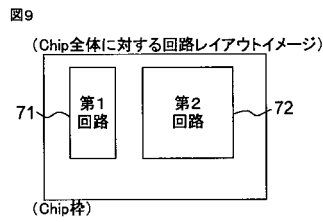
【図 7】



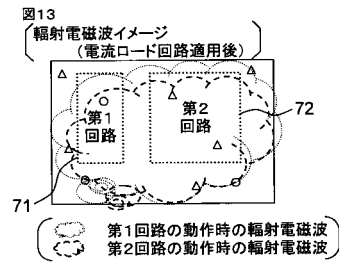
【図 8】



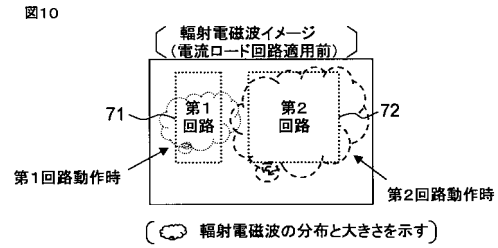
【図 9】



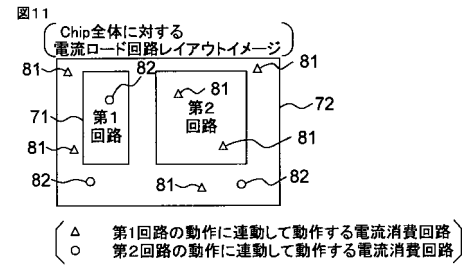
【図 13】



【図 10】

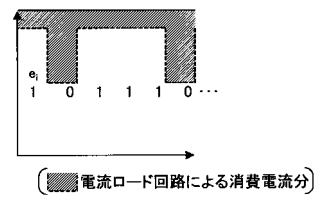


【図 11】



【図 12】

図12
〔消費電力波形(電流ロード回路適用後)〕



フロントページの続き

(56)参考文献 特開2003-258617(JP,A)
特開2003-142999(JP,A)
特開2000-305668(JP,A)

(58)調査した分野(Int.Cl., DB名)

G 0 6 F	1 5 / 7 8
G 0 6 F	1 / 0 4
G 0 6 F	1 / 3 2