(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4920680号
(P4920680)
(45)発行日　平成24年4月18日(2012.4.18)　(24)登録日　平成24年2月10日(2012.2.10)

(51)Int.Cl.　F I
G06F 21/02 (2006.01)　G06F 21/02　175

請求項の数 14　(全 10 頁)

(21)出願番号	特願2008-510607 (P2008-510607)
(86)(22)出願日	平成18年3月31日 (2006.3.31)
(65)公表番号	特表2008-541257 (P2008-541257A)
(43)公表日	平成20年11月20日 (2008.11.20)
(86)国際出願番号	PCT/FR2006/000704
(87)国際公開番号	WO2006/120310
(87)国際公開日	平成18年11月16日 (2006.11.16)
審査請求日	平成21年2月6日 (2009.2.6)
(31)優先権主張番号	0504610
(32)優先日	平成17年5月9日 (2005.5.9)
(33)優先権主張国	フランス(FR)

(73)特許権者　598145510
ストミクロエレクトロニクス・ソシエテ・アノニム
フランス・Ｆ－９２１２０・モンルージュ・ブールヴァール・ロメン・ローラン・２９
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】エラー注入によるアタックに対してメモリを保護する装置

(57)【特許請求の範囲】
【請求項１】
メモリ(1)内のデータの読取りの方法において、前記メモリによる読取り命令の受信に続いてトリガされる前記メモリ内のデータ(Data(i,k))の読取りサイクルを含み、前記読取りサイクルは、前記メモリの制御回路の制御の下で実行されるとともに、前記メモリ内の前記データを読取るステップを含む方法であって、
前記データ(Data(i,k))の読取りサイクルが、前記制御回路によって実行される
前記メモリ内の前記データを読み取る段階と、
前記メモリに格納された基準データ(Data(ref,k))を読み取る段階と、
読み取った前記基準データと、前記基準データが前記メモリに格納されるときの前記基準データの値と同一である期待値であって前記制御回路に格納された期待値(REG)とを比較する段階と、
読み取った前記基準データが前記期待値と異なる場合、前記メモリをエラーモードにする段階と
をさらに含むことを特徴とする方法。
【請求項２】
前記メモリ(1)内の読み取るべきデータの読取りの直後に前記基準データ(Data(ref,k))が読み取られる請求項1に記載の方法。
【請求項３】
前記メモリ(1)内の読み取るべきデータの読取りに続くクロックサイクル中に前記基準

データが読み取られる請求項1または2に記載の方法。
【請求項４】
前記メモリ(1)内の読み取るべきデータの読取りと同一のクロックサイクル中に前記基準データが読み取られる請求項1または2に記載の方法。
【請求項５】
前記データ(Data(i,k))が、ワード線(WL(i))およびワード列を選択することによって前記メモリ(1)で読み取られ、前記基準データ(Data(ref,k))が、同一のワード列(Sel(k))および基準ワード線(WL(ref))を選択することによって読み取られる請求項1から4の一項に記載の方法。
【請求項６】
前記メモリ(1)が、行として配列されたワード線(WL(i))と、ビットの列として配列されたビット線(BL(j,k))とに接続されたメモリセル(MC(i,j,k))を含み、前記ワード線が行デコーダ(RDEC)に接続され、前記ビット線がセンス増幅器(SA(j))にリンクされ、前記メモリ内のデータを読み取る前記段階が、
読み取るべきデータの受信アドレスに対応するワード線(WL(i))を選択する段階と、
前記選択したワード線のメモリセル(MC(i,j,k))を読み取る段階と、
読み取った前記メモリセルの内容を前記メモリの出力データバス(DB)に印加する段階と、
前記基準データのアドレスに対応する基準ワード線(WL(ref))を選択する段階と、
前記基準データ(Data(ref,k))が読み取られる、前記選択した基準ワード線の基準メモリセル(MC(ref,j,k))を読み取る段階と、
読み取った前記基準データを期待値と比較する段階と、
読み取った前記基準データが前記期待値と異なる場合、前記メモリをエラーモードにする段階と
を含む請求項1から5に記載の方法。
【請求項７】
前記メモリ(1)がエラーモードでエラー信号(ER)を送る請求項1から6の一項に記載の方法。
【請求項８】
読取りサイクル中に、メモリ内のデータを、前記メモリで受信される前記データの読取りコマンドに続いて読み取る制御回路を備える読取りセキュアメモリ(1)であって、前記制御回路は、
前記データの前記読取りコマンドに続く前記読取りサイクル中に、前記メモリ内の基準データを読み取る手段と、
読み取った前記基準データと、前記基準データが前記メモリに格納されるときの前記基準データの値と同一である期待値であって前記制御回路に格納された期待値(REG)とを比較する手段(XG(j))と、
読み取った前記基準データが前記期待値と異なる場合、エラー信号(ER)を生成する手段(OG)と
を備えることを特徴とするメモリ(1)。
【請求項９】
同一のクロックサイクル中にデータおよび前記基準データを読み取る手段を含む請求項8に記載のメモリ(1)。
【請求項１０】
2つの連続するクロックサイクル中にデータおよび前記基準データを読み取る手段を含む請求項8に記載のメモリ(1)。
【請求項１１】
前記データ(Data(i,k))が、ワード線およびワード列(Sel(k))を選択することによって前記メモリ(1)で読み取られ、前記基準データ(Data(ref,k))が、同一のワード列および基準ワード線(WL(ref))を選択することによって読み取られる請求項8から10の一項に記載の

メモリ(1)。
【請求項１２】
行として配列されたワード線(WL(i))と、ビットの列として配列されたビット線(BL(j,k))とに接続されたメモリセル(MC(i,j,k))と、
前記ワード線に接続され、読み取るべきデータの受信アドレスに対応するワード線を選択する行デコーダ(RDEC)と、
前記メモリ内のワード(Data(i,k))の読取りサイクル中に、基準データ(Data(ref,k))を含む基準メモリセル(MC(ref,j,k))が接続される基準ワード線(WL(ref))を選択し、前記選択した基準メモリセルの読取りをトリガする手段(CTL)と、
読み取った前記基準メモリセルの内容をそれぞれの期待値と比較する手段(XG(j))であって、前記基準ワード線のメモリセルの内容がそれぞれの期待値と異なる場合、前記エラー信号がエラー信号出力(ER)上に送られる手段と
を備える請求項8から11の一項に記載のメモリ(1)。
【請求項１３】
前記メモリセルがメモリアレイ(MA)として配設され、前記基準ワード線(WL(ref))が、前記ビット線(BL(j,k))とセンス増幅器(SA(j))との間のリンクと反対側のメモリアレイの1辺上に配置される請求項12に記載のメモリ(1)。
【請求項１４】
読み取るべきデータの受信アドレスに対応するワードを形成するビット線(BL(j,k))のグループを選択する列デコーダ(CDEC)を備え、基準データ(Data(ref,k))が格納される前記基準ワード線（WL(ref)）のメモリセル（MC(ref, j, k)）が、ビット線の各グループに前記基準データを保存する請求項12または13に記載のメモリ(1)。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、エラー注入によるアタックに対する集積回路の保護に関し、詳細には、スマートカード内に存在する集積回路の保護に関する。
【０００２】
より詳細には、本発明は、メモリの読取りをセキュアにする方法に関する。
【０００３】
具体的には、本発明は、専らではないがROM、EEPROM、フラッシュメモリなどの不揮発性メモリに適用される。
【背景技術】
【０００４】
近年、セキュアなマイクロプロセッサ集積回路(マイクロプロセッサ、マイクロコントローラ、マイクロプロセッサメモリ、コプロセッサ集積回路など)をハッキングする技法がかなり発展してきている。現在、最先端のハッキング方法は、例えば認証操作や暗号アルゴリズムを実行する操作などの、いわゆる敏感な操作(sensitive operation)の実行中に、集積回路の決定した地点でエラーを注入するものである。障害注入によるアタックとも呼ばれる、そのようなエラー注入によるアタックは、数学的モデルと共に、ハードワイヤード論理暗号アルゴリズムおよび/またはそれが使用する秘密鍵の構成を推定することを可能にする。グリッチを集積回路の供給電圧に導入すること、集積回路のクロック信号にグリッチを導入すること、集積回路を放射またはレーザビームに露出することなどにより、様々な方式でエラー注入を行うことができる。
【０００５】
米国特許出願第２００４／０５２１１０号に開示されている知られている一方法は、例えば集積回路を開始するとき、または集積回路の動作中に、メモリの内容に関する完全性チェックを実施するものである。しかし、こうしたチェックは、メモリの内容を変更せず、データがメモリで読み取られる瞬間に、すなわちメモリ読取り経路上でデータを変更することを目的とするアタックを検出しない。

【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、読取りサイクル中にデータを変更することを目的とするアタックに対してメモリを保護することを目的とする。この目的は、メモリが読み取られるごとに、その完全性がチェックされる基準データの第2読取りを設けることによって達成される。
【課題を解決するための手段】
【０００７】
より具体的には、本発明は、メモリ内のデータの読取りの方法であって、メモリによる読取り順序の受領に続いてトリガされるメモリ内のデータの読取りサイクルを含み、メモリ内のデータの読取りステップを含む方法を提供する。本発明によれば、メモリ内のデータの読取りサイクルはさらに、
メモリに格納された基準データを読み取るステップと、
読み取った基準データを期待値と比較するステップと、
読み取ったデータが期待値と異なる場合、メモリをエラーモードに入れるステップとを含む。
【０００８】
本発明の一実施形態によれば、メモリ内の読み取るべきデータの読取りの直後に基準データが読み取られる。
【０００９】
本発明の一実施形態によれば、メモリ内の読み取るべきデータの読取りに続くクロックサイクル中に基準データが読み取られる。
【００１０】
本発明の一実施形態によれば、メモリ内の読み取るべきデータの読取りと同一のクロックサイクル中に基準データが読み取られる。
【００１１】
本発明の一実施形態によれば、メモリは、行として配列されたワード線と、ビットの列として配列されたビット線とに接続されたメモリセルを含み、ワード線が行デコーダに接続され、ビット線がセンス増幅器にリンクされ、メモリ内のデータを読み取る段階は、
読み取るべきデータの受信アドレスに対応するワード線を選択するステップと、
選択したワード線のメモリセルを読み取るステップと、
読み取ったメモリセルの内容をメモリの出力データバスに印加するステップと、
基準データのアドレスに対応する基準ワード線を選択するステップと、
基準データが読み取られる、選択した基準ワード線の基準メモリセルを読み取るステップと、
読み取った基準データを期待値と比較するステップと、
読み取った基準データが期待値と異なる場合、メモリをエラーモードにするステップとを含む。
【００１２】
本発明の一実施形態によれば、メモリは、エラーモードでエラー信号を送る。
【００１３】
本発明はまた、メモリで受領されるデータの読取りコマンドに続いて、読取りサイクル中にメモリ内のデータを読み取る手段を備える読取りセキュアメモリに関する。本発明によれば、メモリは、
データの読取りコマンドに続いて読取りサイクル中に、メモリ内の基準データを読み取る手段と、
読み取った基準データを期待値と比較する手段と、
読み取った基準データが期待値と異なる場合、エラー信号を生成する手段とを備える。
【００１４】
本発明の一実施形態によれば、メモリが、同一のクロックサイクル中にデータおよび基

準データを読み取る手段を含む。
【００１５】
本発明の一実施形態によれば、メモリが、2つの連続するクロックサイクル中にデータおよび基準データを読み取る手段を含む。
【００１６】
本発明の一実施形態によれば、メモリは、
行として配列されたワード線と、ビットの列として配列されたビット線とに接続されたメモリセルと、
ワード線に接続され、読み取るべきデータの受信アドレスに対応するワード線を選択する行デコーダと、
メモリ内のワードの読み取りサイクル中に、基準データを含む基準メモリセルが接続される基準ワード線を選択し、選択したメモリセルの読取りをトリガする手段と、
読み取った基準メモリセルの内容をそれぞれの期待値と比較する手段であって、基準ワード線のメモリセルの内容がそれぞれの期待値と異なる場合、エラー信号がエラー信号出力上に送られる手段とを備える。
【００１７】
本発明の一実施形態によれば、メモリセルがメモリアレイとして配設され、基準ワード線が、ビット線とセンス増幅器との間のリンクと反対側のメモリアレイの1辺上に配置される。
【００１８】
本発明の一実施形態によれば、メモリは、読み取るべきデータの受信アドレスに対応するワードを形成するビット線のグループを選択する列デコーダを備え、基準データが格納される基準ワード線のメモリセルが、ビット線の各グループに基準データを保存する。
【００１９】
限定はしないが添付の図に関連して与えられる本発明の以下の説明で、本発明の上記およびその他の目的、特徴、および利点をより詳細に説明する。
【発明を実施するための最良の形態】
【００２０】
図1は、メモリアレイMA、ワード線デコーダRDEC、列デコーダCDEC、および制御回路CTLを備えるメモリ1を表す。メモリアレイMAは、行として配設されたワード線WL(i)と、列として配設されたビット線BL(j,k)とに接続されたメモリセルMC(i,j,k)を備える。ワード線WL(i)は、行デコーダRDECによって制御される。各ビット線BL(j,k)は、kランクワード列選択トランジスタTS(k)を介してセンス増幅器SA(j)(jは0からm-1の間の整数)と、多重化バスMBとにリンクされる。
【００２１】
選択トランジスタTS(k)は、列デコーダCDECによって送られる信号SEL(k)で駆動される。入力で多重化バスMBに接続され、出力でメモリの出力バスDBに接続されるセンス増幅器SA(j)により、ワード線WL(i)で選択されたmビットのワードを読み取ることが可能となり、こうしたビットの値をバスDBのそれぞれの線上に印加することが可能となる。
【００２２】
制御回路CTLは、入力で、読取りアドレスAD、ならびにメモリを活動化させることを可能にするクロックCLKおよびチップ選択CS信号を受け取り、出力で、センス増幅器をトリガする信号RDと、行デコーダRDECおよび列デコーダCDECにそれぞれ印加されるアドレスADHおよびADLとを送達する。通常、行デコーダに印加されるアドレスADHは、メモリの入力で印加されるアドレスADの最上位ビットをグループ化し、列デコーダに印加されるアドレスADLは最下位ビットをグループ化する。アドレスADHおよびADLを使用して、行デコーダおよび列デコーダは、ランクiのワード線およびランクkのワード列を選択して、いくつかのビット線BL(j,k)をグループ化する。制御回路は、メモリの出力で、メモリがビジーであるか、それとも別の読取りコマンドを受け取る準備ができているかを外部回路に示す信号RB(Ready/Busy)を発行する。

【００２３】
本発明によれば、メモリアレイMAのワード線WL(ref)に接続されたメモリセルのグループMC(ref,j,k)が、メモリ内のワードを読み取る各段階で読み取られる基準ワードを格納するために予約される。制御回路CTLは、読み取られた基準ワードを取り出して、それを制御回路で保存された期待値と比較するように設計される。基準ワードが期待値を有さない場合、制御回路は、例えばその目的で設けられたメモリの出力ER上にエラー信号を送ることにより、メモリをエラーモードにする。
【００２４】
図2は、データバスDB上に現れる、読み取られた基準ワードと、例えば制御回路CTLの内部のレジスタREGに保存される基準値との間でビットごとの比較を実施することを可能にする比較回路の一実施形態を表す。比較回路は、読み取られた基準ワードとこの基準ワードの期待値との間に少なくとも1つのビットに関する違いが検出された場合に、出力ERで信号on 1を生成するように設計される。この目的で、比較回路は、1組の排他的論理和ゲートXG(j)(jは0からm-1の間の整数)を備える。各ゲートXG(j)は、レジスタREGのセルにそれぞれ接続された第1入力と、バスDBの対応する線にそれぞれ接続された第2入力とを備える。各ゲートXG(j)の出力は、ORゲートOGの入力にそれぞれ接続され、ORゲートOGの出力は、比較回路の出力ERに接続される。基準値を含むレジスタ内のビットのすべてが、バスDB上に現れるワード線WL(ref)で読み取られた基準ワードのそれぞれのビットと同一である場合、ゲートXG(j)の出力はon 0である。ORゲートOGの出力ERもon 0である。しかし、レジスタREG内のビットのうちの少なくとも1つがデータバスDBの対応する線上で読み取られたビットと異なる場合、対応するゲートXG(j)は信号on 1を発行し、ORゲートOGの出力ERは1に変化する。
【００２５】
好ましくは、基準ワードを格納するために選ばれるワード線WL(ref)は、メモリアレイMA内の、センス増幅器SA(j)がビット線BL(j,k)に接続される地点の反対側に位置する。このようにして、グリッチが印加される読取り経路のエリアとは無関係に、読み取られた基準データもグリッチを受け、したがって期待値とは異なるものとなる。
【００２６】
図3に、制御回路CTLで実施される本発明による方法を示す。この方法は、メモリに印加される信号CSが1に変化するときに活動化される(ステップ11)。この信号の送信により、メモリのアドレス入力バスAD上で印加されるアドレスのメモリ内のデータを読み取る段階がトリガされる(ステップ12)。同時に、制御回路は、信号RBを送ることによってメモリをビジー状態にする(ステップ13)。
【００２７】
次のステップ14では、制御回路は、アドレスバスAD上で受け取ったアドレスに対応するアドレスADHおよびADLを行RDECデコーダおよび列CDECデコーダに送り、その結果、ワード線WL(i)と、kランクワード列のビット線BL(j,k)のグループとに属するメモリセルMC(i,j,k)が選択される。
【００２８】
次のステップ15では、制御回路は読取りをトリガする信号RDを送り、それがセンス増幅器SA(j)に印加される。次いで、読み取ったワードが、センス増幅器SA(j)によってデータバスDB上に印加される。メモリ内のワードの読取りに続いて、制御回路は、メモリに格納された基準ワードのアドレスを行デコーダRDECに送る(ステップ16)。
【００２９】
基準ワードにアクセスするために選択されるランクkワード列は、グリッチが印加されたデータ読取り経路のビット線BL(j,k)とは無関係にグリッチを検出することができるように、ステップ14で選択されたものであることが好ましい。この場合、基準ワード線WL(ref)のメモリセルに格納されたワードのすべてが同一であり、レジスタREGに格納された値を有する。
【００３０】

次のステップ17では、トリガ信号RDが再び送られる。次いで、センス増幅器が、読み取った基準データをデータバスに印加する。次のステップ18では、制御回路が、読み取った基準ワードをレジスタREGに保存された基準値と比較し、違いが検出された場合、制御回路CTLは、エラー信号出力ERに対して印加する信号を1にする。

【００３１】

図4Aに、ワード線WL(i)上に位置する、メモリのkランクワード列中のワードを読み取る古典的シーケンスをタイミング図の形式で示す。この図は、クロック信号CLK、メモリを活動化させる信号CS、アドレス信号AD、ワード線選択信号WL(i)、kランクワード列選択信号SEL(k)、センス増幅器SA(j)の出力で読み取られたデータの信号Data、およびバスDB上のデータ信号を示す。

【００３２】

クロックサイクルCLK中、メモリを活動化させる信号CSはon 1であるのに対して、読取りアドレスはバスAD上に存在する。読取りアドレスは行RDECデコーダおよび列CDECデコーダによって処理され、ワード線および列を選択するどの信号WL(i)およびSEL(k)を同一のクロックサイクル中に1に変更すべきかが判定される。信号WL(i)およびSEL(k)が1に変更されるとすぐに、対応するメモリセルがセンス増幅器SA(j)によって読み取られる。次のクロックサイクル時に、読み取られたデータData(i,k)がデータバスDBに送られる。グリッチPが読取り経路、すなわちビット線BL(j,k)またはセンス増幅器に印加される場合、データバスDBに送られるデータData(i,k)は偽である。

【００３３】

そのようなグリッチを検出するために、メモリを選択するための信号CSと、kランクワード列を選択するためのSEL(k)が、図4Bに示されるように2クロックサイクルの間、on 1に維持される。古典的読取り手続き(図4A)と同様に、読み取るべきワード線を選択する信号WL(i)が、第1クロックサイクル中、on 1に位置される。第2クロックサイクル中、基準ワード線を読み取る信号WL(ref)が1にされ、線WL(ref)およびkランクワード列のメモリセルに格納された基準ワードData(ref,k)が読み取られる(信号SEL(k) on 1)。その結果は、センス増幅器SA(j)の出力で、データData(i,k)が第1クロックサイクルの終りで現れ、基準ワード線で読み取られた基準データData(ref,k)が第2クロックサイクルの終りで現れることである。読み取られた基準データの値が期待値と異なる場合、出力ERに対して印加されるエラー信号が1に変化する。

【００３４】

有利には、制御回路CTLは、読み取るべきデータを読み取り、メモリ1に印加されるクロック信号CLKの単一サイクルで基準データを読み取る。この目的で、制御回路は、クロック信号CLKを使用して、読取り操作を順序付けるために内部クロック信号を生成し、読取り操作の周波数はクロック信号CLKの2倍に等しい。

【００３５】

本発明による方法の様々な代替実施形態が、特にエラー信号の処理に関する限りは可能であることを当業者は理解されよう。具体的には、メモリの外部の環境にエラーを示す必要はない。したがって、敏感なデータをメモリから消去するなど、適切などんな方策も取ることができる。外部環境に対してエラーが示される場合、メモリにアクセスする処理装置を初期化し、または本発明によるメモリを組み込む集積回路を完全にサービス休止にするなど、適切などんな方策も取ることができる。

【００３６】

さらに、メモリのアドレスバスに対して印加されるアドレスに対応するデータが読み取られる前に、基準データを読み取ることもできる。

【００３７】

さらに、メモリセルが行および列として配列され、行を選択し、選択した行の1つを読み取り、またはいくつかのメモリセルを同時に読み取ることによって読取りが実施される任意のタイプのメモリに本発明を適用することができる。明らかに、行と列の概念は逆転させることができる。

【図面の簡単な説明】

【００３８】

【図１】本発明によるメモリのアーキテクチャをダイアグラムで表す図である。

【図２】図1で現れるメモリの回路を表す図である。

【図３】本発明による方法を示すフローチャートである。

【図４Ａ】古典的メモリを読み取るサイクルを示すタイミング図である。

【図４Ｂ】本発明によるメモリを読み取るサイクルを示すタイミング図である。

【符号の説明】

【００３９】

１　メモリ

BL(j,k) ビット線

CDEC 列デコーダ

CTL 制御回路

DB バス

ER 出力

MA メモリアレイ

MB 多重化バス

MC(i,j,k) メモリセル

OG　ORゲート

REG レジスタ

RDEC ワード線デコーダ

SA(j) センス増幅器

TS(k)　kランクワード列選択トランジスタ

WL(i) ワード線

XG(j) 排他的論理和ゲート

【図１】

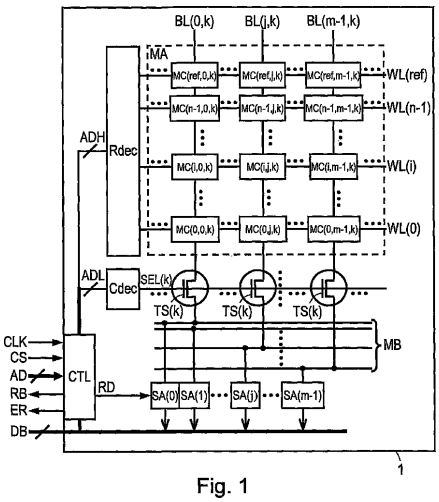

Fig. 1

【図２】

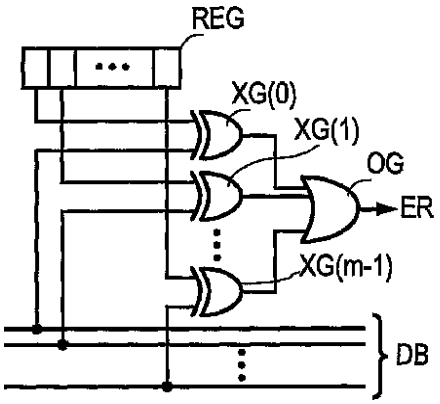

Fig. 2

【図３】

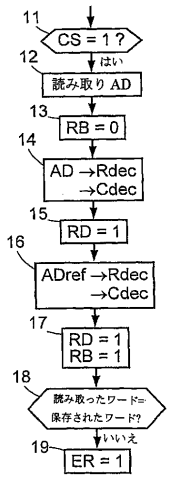

Fig. 3

【図４Ａ】

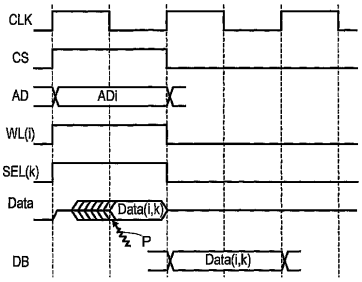

Fig. 4A

【図４Ｂ】

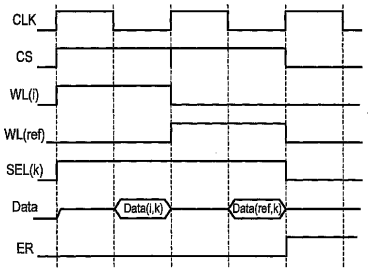

Fig. 4B

フロントページの続き

(72)発明者　シルヴィ・ウィダール
フランス・Ｆ－８３９１０・プルリエール・ル・カドゥ・１２

審査官　児玉　崇晶

(56)参考文献　特開２００５－０４４１８５（ＪＰ，Ａ）
特開２０００－２６０１１８（ＪＰ，Ａ）
特開昭６２－２８２３９２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/02