

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第3606788号
(P3606788)

(45) 発行日 平成17年1月5日(2005.1.5)

(24) 登録日 平成16年10月15日(2004.10.15)

(51) Int. Cl.⁷

F I

G 1 1 C	29/00	G 1 1 C	29/00	6 3 1 B
G 0 6 F	12/14	G 1 1 C	29/00	6 7 5 L
G 0 6 F	12/16	G 0 6 F	12/14	3 2 0 A
G 1 1 C	16/02	G 0 6 F	12/16	3 3 0 A
G 1 1 C	16/06	G 1 1 C	17/00	6 0 1 P

請求項の数 2 (全 7 頁) 最終頁に続く

(21) 出願番号 特願2000-161343 (P2000-161343)
 (22) 出願日 平成12年5月31日 (2000.5.31)
 (65) 公開番号 特開2001-344992 (P2001-344992A)
 (43) 公開日 平成13年12月14日 (2001.12.14)
 審査請求日 平成13年3月29日 (2001.3.29)

前置審査

(73) 特許権者 000005821
 松下電器産業株式会社
 大阪府門真市大字門真1006番地
 (74) 代理人 100077931
 弁理士 前田 弘
 (74) 代理人 100094134
 弁理士 小山 廣毅
 (74) 代理人 100110939
 弁理士 竹内 宏
 (74) 代理人 100110940
 弁理士 嶋田 高久
 (74) 代理人 100113262
 弁理士 竹内 祐二
 (74) 代理人 100115059
 弁理士 今江 克実

最終頁に続く

(54) 【発明の名称】 半導体集積回路および半導体集積回路の検査方法

(57) 【特許請求の範囲】

【請求項1】

複数の機密情報データを格納し、外部から読み出しできないように構成されたROMと、このROMのテストを行うためのテスト回路とを内蔵した半導体集積回路であって、前記ROMは、前記機密情報データに所定の演算を施して得られ、各々が前記複数の機密情報データに対応して設けられた複数のチェック用冗長データを、記憶しており、前記複数の機密情報データは、前記ROMの最下位アドレスから順に格納されており、前記複数のチェック用冗長データは、前記ROMの最上位アドレスから順に格納されており、

前記テスト回路は、

前記ROMから読み出された複数の機密情報データの各々に対し、前記所定の演算に相当する演算を実行するチェック演算回路を有し、このチェック演算回路の演算結果と、前記ROMに記憶された複数のチェック用冗長データとの比較を行い、前記機密情報データ毎に、対応する前記チェック用冗長データとの比較結果を出力する

ことを特徴とする半導体集積回路。

【請求項2】

複数の機密情報データを格納し、外部から読み出しできないように構成されたROMを内蔵した半導体集積回路を検査する方法であって、前記ROMの最下位アドレスから順に格納された前記機密情報データに所定の演算を施して得られ、各々が前記複数の機密情報データに対応して設けられた複数のチェック用冗長

データを、予め、前記ROMの最上位アドレスから順に、記憶させておく前処理と、前記ROMから前記複数の機密情報データを読み出し、読み出した前記複数の機密情報データの各々に対し、前記所定の演算に相当する演算を実行する処理と、前記ROMから前記複数のチェック用冗長データを読み出し、前記演算を実行する処理の結果と、対応する前記チェック用冗長データとを比較し、前記機密情報データ毎に比較結果を出力する処理とを備えた

ことを特徴とする半導体集積回路の検査方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ROMを内蔵した半導体集積回路について、このROMをテストするための技術に属する。

【0002】

【従来の技術】

図4はROMを内蔵した半導体集積回路のテスト回路の従来の構成を示す図である。図4の構成では、テスト回路として、ROM51の入力側と出力側にセレクタ61, 62, 63が設けられている。各セレクタ61, 62, 63は入力Sが“H”のとき、端子Aの入力を選択出力する。

【0003】

ROM51のテストを行うときは、テスト信号TESTとして“H”を与える。これによって、外部端子IN1, IN2への入力データがROM51のアドレス入力ADDおよびリード入力READに供給される。そして、ROM51の出力DOが外部端子OUTから出力される。このように、従来は、ROM51の入出力を外部から直接的に制御可能にすることによって、ROM51のテストを実行していた。

【0004】

【発明が解決しようとする課題】

ところが、従来のように、ROMの入出力を外部から直接的に制御可能にすると、マイクロコード、秘密鍵やパスワードなどのような機密情報データをROMに実装した場合に、その実装した機密情報データが外部から容易に解読されてしまう、という問題が生じる。

【0005】

また、従来のBIST (Built In Self Test) 方式を利用した場合は、データの機密性は上述の例よりも高まるものの、機密情報データの内容を変更した場合に、半導体集積回路内に実装するBIST回路自体の構成も変更する必要がある。このため、開発工数やマスク設計費などが大幅に増大してしまう。

【0006】

前記の問題に鑑み、本発明は、ROMを内蔵した半導体集積回路として、ROMに実装したデータの機密性を保ちつつ、ROMのテストを実行可能にすることを課題とする。

【0007】

【課題を解決するための手段】

前記の課題を解決するために、請求項1の発明が講じた解決手段は、複数の機密情報データを格納し、外部から読み出しできないように構成されたROMと、このROMのテストを行うためのテスト回路とを内蔵した半導体集積回路として、前記ROMは、前記機密情報データに所定の演算を施して得られ、各々が前記複数の機密情報データに対応して設けられた複数のチェック用冗長データを記憶しており、前記複数の機密情報データは、前記ROMの最上位アドレスから順に格納されており、前記複数のチェック用冗長データは、前記ROMの最上位アドレスから順に格納されており、前記テスト回路は、前記ROMから読み出された複数の機密情報データの各々に対し、前記所定の演算に相当する演算を実行するチェック演算回路を有し、このチェック演算回路の演算結果と、前記ROMに記憶された複数のチェック用冗長データとの比較を行い、前記機密情報データ毎に、対応する前記チェック用冗長データとの比較結果を出力するものである。

10

20

30

40

50

【 0 0 0 8 】

請求項 1 の発明によると、ROM から読み出された機密情報データに対し、テスト回路が有するチェック演算回路によって、チェック用冗長データ生成のための所定の演算に相当する演算が実行される。そして、ROM に記憶されたチェック用冗長データと、チェック演算回路の演算結果とが比較される。これにより、機密情報データが半導体集積回路外部に読み出されることなく、データチェックが実現され、機密情報データの機密性を損なうことなく、ROM のテストを実行することができる。しかも、機密情報データは、ROM の最下位アドレスから順に格納されており、チェック用冗長データは、ROM の最上位アドレスから順に格納されているので、コンプリメンタリチェックに適している。

【 0 0 0 9 】

また、請求項 2 の発明が講じた解決手段は、複数の機密情報データを格納し、外部から読み出しできないように構成された ROM を内蔵した半導体集積回路を検査する方法として、前記 ROM の最下位アドレスから順に格納された前記機密情報データに所定の演算を施して得られ、各々が前記複数の機密情報データに対応して設けられた複数のチェック用冗長データを予め前記 ROM の最上位アドレスから順に記憶させておく前処理と、前記 ROM から前記複数の機密情報データを読み出し、読み出した前記複数の機密情報データの各々に対し前記所定の演算に相当する演算を実行する処理と、前記 ROM から前記複数のチェック用冗長データを読み出し、前記演算を実行する処理の結果と、対応する前記チェック用冗長データとを比較し、前記機密情報データ毎に比較結果を出力する処理とを備えたものである。

【 0 0 1 0 】

【 発明の実施の形態 】

以下、本発明の一実施形態について、図面を参照して説明する。

【 0 0 1 1 】

図 1 は本発明の一実施形態に係る半導体集積回路の構成を示すブロック図である。図 1 に示す半導体集積回路は、マイクロコード、秘密鍵やパスワードなどの機密情報データの機密性を損なうことなく、ROM 10 のテストが実現可能に構成されている。

【 0 0 1 2 】

図 1 において、 $(n + 1)$ 個の機密情報データすなわち機密情報データ $(0) \sim (n)$ が、ROM 10 の下位アドレスに実装されている。そして、各機密情報データ $(0) \sim (n)$ について、CRC (Cyclic Redundancy Check: 巡回冗長検査) による冗長コードすなわちチェック用冗長データとしての機密 CRC データ $(0) \sim (n)$ が生成されており、これらは、冗長データ記憶手段としての ROM 10 の上位アドレスに実装されている。

【 0 0 1 3 】

ROM 10 のアドレス空間において、機密情報データ $(0) \sim (n)$ は、最下位アドレスから順に格納されており、機密 CRC データ $(0) \sim (n)$ は、最上位アドレスから順に格納されている。例えば、ROM 10 の最下位アドレスに格納された機密情報データ (0) に対する機密 CRC データ (0) は、ROM 10 の最上位アドレスに格納されている。このようなアドレス配置は、ROM 10 のコンプリメンタリチェックに適している。

【 0 0 1 4 】

また、図 1 において、セレクタ 21, 22、アドレスデコーダ (ADEC) 23、フリップフロップ (FF) 24、チェック演算回路 (CRC) 25 および比較回路 (COMP) 26 によって、テスト回路が構成されている。また、論理回路ブロック (LOGIC) 30 は通常モードで用いられる回路ブロックである。

【 0 0 1 5 】

各セレクタ 21, 22 は、入力 S が “H” (ハイレベル) になると、入力端子 A の入力を選択出力する。アドレスデコーダ 23 はテスト時に入力されるアドレス信号をデコードし、チェック演算回路 25 や比較回路 26 を制御する。チェック演算回路 25 は ROM 10 から読み出された機密情報データに対し、機密 CRC データ生成の際の所定の演算に相当する演算を実行する。比較回路 26 は、チェック演算回路 25 の出力と、ROM 10 から

10

20

30

40

50

読み出された機密CRCデータとを比較する。なお、CLKは、各回路ブロックの同期用クロック信号である。

【0016】

通常動作時は、テスト信号TESTは“L”（ロウレベル）になり、セクタ21, 22は入力端子Bの入力を選択する。すなわち、外部端子INA, INBからの入力データがROM10に与えられる。これらの入力データは、半導体集積回路内の別のブロックから供給される。また、ROM10の出力DOは、論理回路ブロック30に供給される。

【0017】

一方、テスト時は、テスト信号TESTは“H”になり、セクタ21, 22は入力端子Aの入力を選択する。すなわち、外部端子IN1, IN2からの入力データが、ROM10のアドレス入力ADDおよびリード入力READに供給される。

10

【0018】

また、外部端子IN1からの入力データは、アドレスデコーダ23にも入力される。アドレスデコーダ23は、外部端子IN1からの入力データが、機密情報データが格納されているアドレス(address(0)~(n))を示すときは、出力AOUT1をイネーブル(“H”)にする。出力AOUT1が“H”になると、ROM10の出力DOの先にあるチェック演算回路25が1クロック遅れて動作を開始する。また、外部端子IN1からの入力データが、機密CRCデータが格納されているアドレス(address(n+1)~(2n+1))を示すときは、アドレスデコーダ23は、出力AOUT2をイネーブル(“H”)にする。出力AOUT2が“H”になると、比較回路26は、チェック演算回路25の演算結果(IN1)と、ROM10から読み出された機密CRCデータ(IN2)との比較を実行する。そして、比較結果が一致したとき、出力信号RESULTをアサート(“H”)する。

20

【0019】

図2は図1に示す半導体集積回路のテスト時の動作を示すタイミングチャートである。

【0020】

まず、ROM10のテストを行うモードにするために、テスト信号TESTを“H”にする。次に、外部端子IN1から、ROM10において機密情報データ(0)が格納されたアドレスaddress(0)を示す信号を入力するとともに、外部端子IN2から、ROM10のリード入力READがイネーブルになるように“H”を入力する。すると、次のクロック信号CLKの立ち上がりで、ROM10の出力DOとして機密情報データ(0)が読み出される。

30

【0021】

また、アドレスデコーダ23は、アドレスaddress(0)を示す信号が入力されたので、出力AOUT1として“H”を出力する。この信号“H”は、フリップフロップ24で1クロックラッチされた後、チェック演算回路25にイネーブル入力enとして供給される。これにより、チェック演算回路25は、ROM10から出力された機密情報データ(0)に対するCRC演算を開始する。

【0022】

チェック演算回路25がCRC演算を完了する1サイクル前に、外部端子IN1への入力データを、address(0)~(n)以外の値に変更するとともに、外部端子IN2への入力データをネゲート(“L”)にする。すると、アドレスデコーダ23の出力AOUT1もネゲートされ、さらに1サイクル遅れてチェック演算回路25のイネーブル入力enもネゲートされる。これにより、チェック演算回路25の演算結果が出力OUTに保持される。

40

【0023】

次に、外部端子IN1から、機密情報データ(0)に対応する機密CRCデータ(0)が格納されたアドレスaddress(2n+1)を示す信号を入力するとともに、外部端子IN2から、ROM10のリード信号READがイネーブルになるように“H”を入力する。

【0024】

アドレスデコーダ23は、アドレスaddress(2n+1)を示す信号が入力されたので、出力AOUT1として“L”を入力するとともに、出力AOUT2として“H”を出力する。比

50

較回路26は、チェック演算回路25の出力OUTと、ROM10の出力DOすなわち機密CRCデータ(0)との比較を実行する。そして、この比較の結果、両者が一致しているときは、信号RESULTをアサートし(“H”)、不一致のときは“L”にする。

【0025】

また、出力AOUT2が“H”の間、1サイクル期間は信号COMP enがアサートされ、RESULT信号の出力とともにネゲートされる。また、信号COMP enの立ち下がりによって、チェック演算回路25は初期化される。

【0026】

以上のような動作によって、機密情報データ(0)のテストが完了する。

【0027】

同様の動作を、アドレスaddress(1), address(2n)、アドレスaddress(2), address(2n-1)、...、アドレスaddress(n), address(n+1)を指定しながら実行し、信号RESULTを外部からモニターする。この結果から、ROM10に、製造上の問題などに起因して異常が生じているか否かを判定することができる。

【0028】

なお、図1の構成では、機密CRCデータを、機密情報データとは別のアドレスに格納するものとしたが、機密情報データと同一アドレスに格納してもかまわない。例えば図3に示すように、機密情報データの上位側のビット位置に、対応する機密CRCデータをマッピングするようにしてもよい。

【0029】

また、ここでは、機密CRCデータを、機密情報データが実装されたROM自体に実装するものとしたが、機密情報データが実装されたROMとは別の、半導体集積回路に内蔵されたROMなどの記憶手段に、機密CRCデータを実装してもかまわない。

【0030】

また、本発明によると、機密情報データの内容を変更する場合には、その変更に応じて、機密CRCデータを変更するだけでよい。したがって、テスト回路の構成の変更は不要であり、このため、開発工数やマスク設計費などを大幅に削減することができる。

【0031】

また、CRCによる冗長コード以外のデータを、機密情報データのチェックに利用してもかまわない。ただし、この場合は、そのチェック用データを生成するための所定の演算に相当する演算を実行するチェック演算回路を、テスト回路内に設ける必要がある。

【0032】

なお、本実施形態では、同期ROMを例にとって説明を行ったが、非同期ROMであっても、同様の実施が容易に実現可能である。

【0033】

【発明の効果】

以上のように本発明によると、機密情報データを格納するROMを内蔵した半導体集積回路において、ROMのテストを、そのROM内部の機密情報データの機密性を損なうことなく、実現することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る半導体集積回路の構成を示すブロック図である。

【図2】図1に示す半導体集積回路のテスト時の動作を示すタイミングチャートである。

【図3】ROMにおけるデータ格納の他の例を示す図である。

【図4】従来構成の例を示す図である。

【符号の説明】

10, 10A ROM

25 チェック演算回路

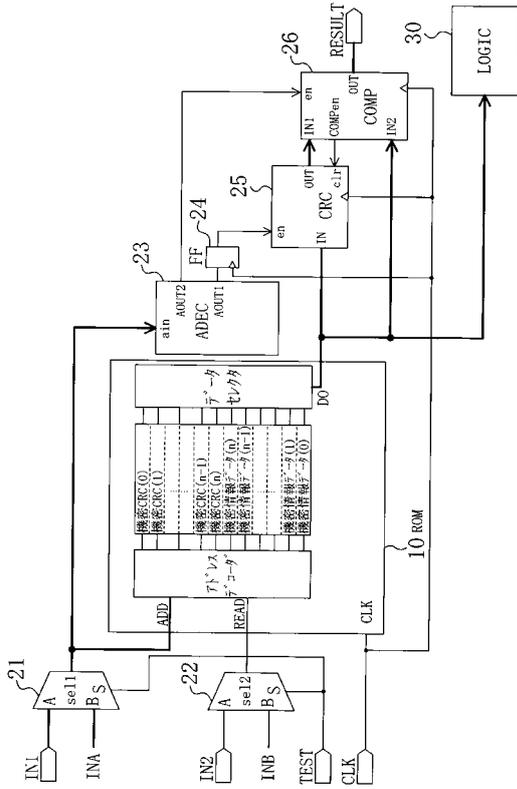
10

20

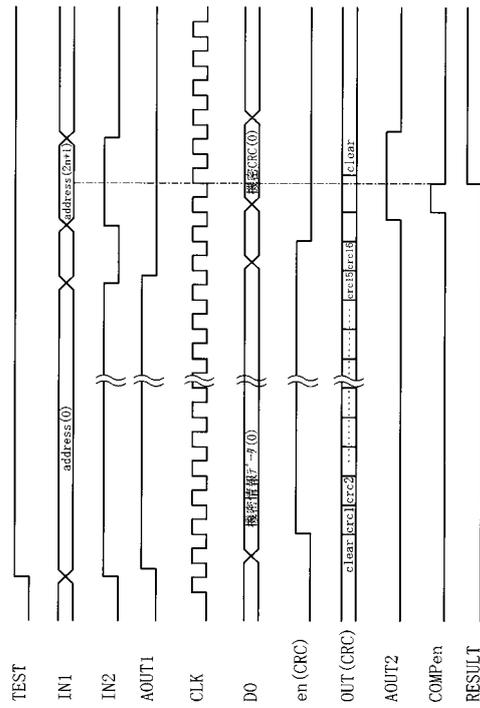
30

40

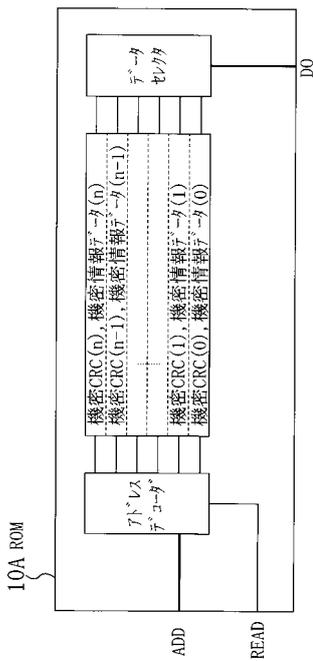
【 図 1 】



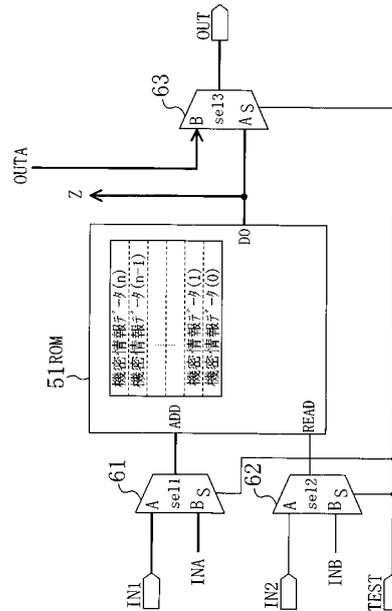
【 図 2 】



【 図 3 】



【 図 4 】



フロントページの続き

(51) Int.Cl.⁷

F I

G 1 1 C 17/00 6 3 9 Z

(74)代理人 100115691

弁理士 藤田 篤史

(74)代理人 100117581

弁理士 二宮 克也

(74)代理人 100117710

弁理士 原田 智雄

(74)代理人 100121728

弁理士 井関 勝守

(72)発明者 藤原 睦

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

審査官 長島 孝志

(56)参考文献 特開昭 5 7 - 0 0 6 4 9 1 (J P , A)

特開平 1 1 - 1 7 5 4 0 3 (J P , A)

特開昭 6 0 - 0 3 0 0 0 0 (J P , A)

(58)調査した分野(Int.Cl.⁷, D B名)

G11C 29/00

G11C 16/00-16/34

G06F 12/14-12/16