(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2004-327036
(P2004-327036A)
(43)公開日　平成16年11月18日(2004.11.18)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11C 29/00	G11C 29/00	673Z	2G132
GO1R 31/28	GO1R 31/28	B	5L106
	GO1R 31/28	V	

審査請求 未請求　請求項の数 5　OL　（全 8 頁）

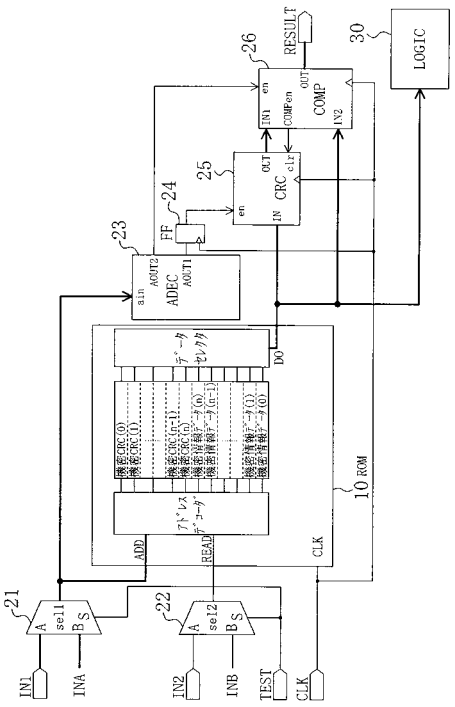
(21)出願番号　特願2004-230465(P2004-230465)
(22)出願日　平成16年8月6日(2004.8.6)
(62)分割の表示　特願2000-161343(P2000-161343)の分割
原出願日　平成12年5月31日(2000.5.31)

(71)出願人　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)【要約】
【課題】　ROMを内蔵した半導体集積回路について、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。
【解決手段】　機密情報データを格納するROM１０に、データチェック用の機密ＣＲＣデータが格納されている。チェック演算回路２５は、ROM１０から読み出された機密情報データに対し、機密ＣＲＣデータ生成のため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の演算結果と、ROM１０から読み出された機密ＣＲＣデータとの比較を行う。
【選択図】　図１



【特許請求の範囲】
【請求項１】
機密情報データを格納する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、
前記機密情報データに所定の演算を施して得たチェック用冗長データを、記憶する冗長データ記憶手段を備え、
前記テスト回路は、
前記ＲＯＭから読み出された機密情報データに対し、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、前記冗長データ記憶手段に記憶されたチェック用冗長データとの比較を行う
ことを特徴とする半導体集積回路。
【請求項２】
請求項１記載の半導体集積回路において、
前記冗長データ記憶手段は、前記ＲＯＭである
ことを特徴とする半導体集積回路。
【請求項３】
請求項２記載の半導体集積回路において、
前記チェック用冗長データは、前記ＲＯＭにおいて、前記機密情報データと異なるアドレスに格納されている
ことを特徴とする半導体集積回路。
【請求項４】
請求項２記載の半導体集積回路において、
前記チェック用冗長データは、前記ＲＯＭにおいて、前記機密情報データと同一アドレスに格納されている
ことを特徴とする半導体集積回路。
【請求項５】
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を検査する方法であって、
前記機密情報データに所定の演算を施して得たチェック用冗長データを、予め、当該半導体集積回路の冗長データ記憶手段に、記憶させておく前処理と、
前記ＲＯＭから機密情報データを読み出し、読み出した機密データに対し、前記所定の演算に相当する演算を実行する処理と、
前記冗長データ記憶手段からチェック用冗長データを読み出し、前記演算処理の結果と、読み出したチェック用冗長データとを比較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】
【技術分野】
【０００１】
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。
【背景技術】
【０００２】
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。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
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。
【課題を解決するための手段】
【０００７】
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、機密情報データを格納する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、前記機密情報データに所定の演算を施して得たチェック用冗長データを記憶する冗長データ記憶手段を備え、前記テスト回路は、前記ＲＯＭから読み出された機密情報データに対し、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、前記冗長データ記憶手段に記憶されたチェック用冗長データとの比較を行うものである。
【０００８】
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、冗長データ記憶手段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。
【０００９】
そして、請求項２の発明では、前記請求項１の半導体集積回路における冗長データ記憶手段は、前記ＲＯＭであるものとする。
【００１０】
さらに、請求項３の発明では、前記請求項２の半導体集積回路におけるチェック用冗長データは、前記ＲＯＭにおいて、前記機密情報データと異なるアドレスに格納されているものとする。
【００１１】
また、請求項４の発明では、前記請求項２の半導体集積回路におけるチェック用冗長データは、前記ＲＯＭにおいて、前記機密情報データと同一アドレスに格納されているものとする。
【００１２】
また、請求項５の発明が講じた解決手段は、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を検査する方法として、前記機密情報データに所定の演算を施して得たチェック用冗長データを予め当該半導体集積回路の冗長データ記憶手段に記憶させておく前処理と、前記ＲＯＭから機密情報データを読み出し、読み出した機密データ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、前記冗長データ記憶手段からチェック用冗長データを読み出し、前記演算処理の結果と読み出したチェック用冗長データとを比較す

る処理とを備えたものである。
【発明の効果】
【００１３】
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。
【発明を実施するための最良の形態】
【００１４】
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。
【００１５】
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、ＲＯＭ１０のテストが実現可能に構成されている。
【００１６】
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）～（ｎ）が、ＲＯＭ１０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）～（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）～（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ＲＯＭ１０の上位アドレスに実装されている。
【００１７】
ＲＯＭ１０のアドレス空間において、機密情報データ（０）～（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）～（ｎ）は、最上位アドレスから順に格納されている。例えば、ＲＯＭ１０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、ＲＯＭ１０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、ＲＯＭ１０のコンプリメンタリチェックに適している。
【００１８】
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。
【００１９】
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ＲＯＭ１０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、ＲＯＭ１０から読み出された機密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。
【００２０】
通常動作時は、テスト信号ＴＥＳＴは“Ｌ”（ロウレベル）になり、セレクタ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。
【００２１】
一方、テスト時は、テスト信号ＴＥＳＴは“Ｈ”になり、セレクタ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。
【００２２】
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。アドレスレコーダ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。

【００２３】

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。

【００２４】

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。

【００２５】

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。

【００２６】

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。

【００２７】

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。

【００２８】

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。

【００２９】

また、出力ＡＯＵＴ２が“Ｈ”の間、１サイクル期間は信号ＣＯＭＰｅｎ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ＣＯＭＰｅｎ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。

【００３０】

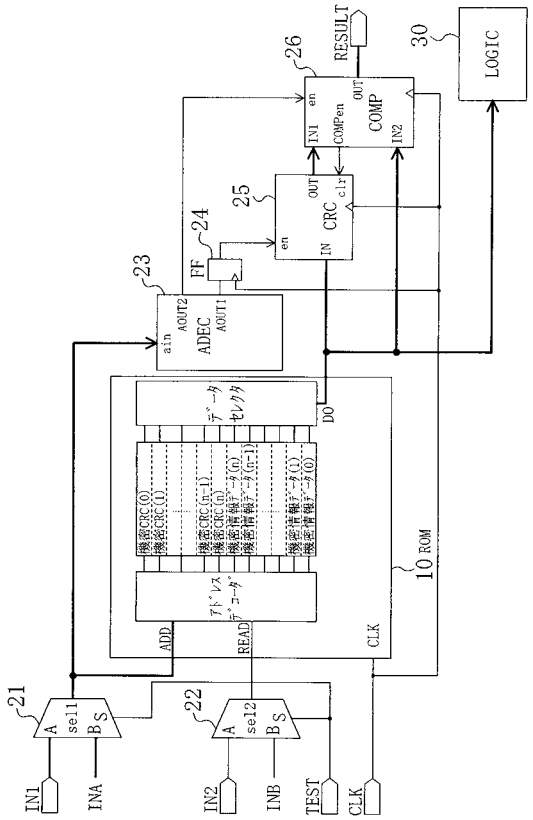
以上のような動作によって、機密情報データ（０）のテストが完了する。

【００３１】

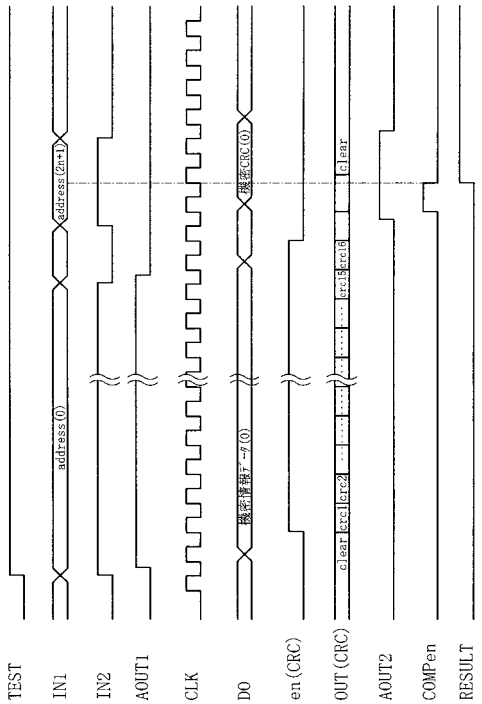
同様の動作を、アドレスaddress(1), address(2n)、アドレスaddress(2), address(2n-1)、…、アドレスaddress(n), address(n+1) を指定しながら実行し、信号ＲＥＳＵＬＴを外部からモニターする。この結果から、ＲＯＭ１０に、製造上の問題などに起因して異常が生じているか否かを判定することができる。

【００３２】
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。
【００３３】
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。
【００３４】
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。
【００３５】
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。
【００３６】
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。
【図面の簡単な説明】
【００３７】
【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】従来の構成の例を示す図である。
【符号の説明】
【００３８】
１０，１０Ａ　ＲＯＭ
２５　チェック演算回路

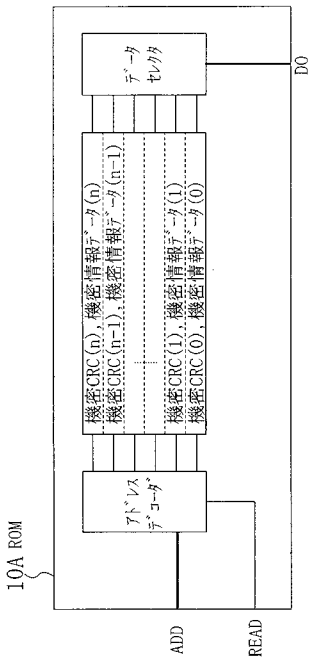
【図１】


RESULT
26
30
LOGIC
COMP
IN1
en
COMPen
OUT
IN2
25
CRC
IN
OUT
clr
en
24
FF
23
ADEC
a.in
AOUT2
AOUT1
データセレクタ
DO
機密CRC(0)
機密CRC(1)
機密CRC(n-1)
機密CRC(n)
機密情報データ(0)
機密情報データ(1)
機密情報データ(n-1)
アドレスデコーダ
10 ROM
ADD
READ
CLK
21
22
sel1
sel2
A
B
S
IN1
INA
IN2
INB
TEST
CLK

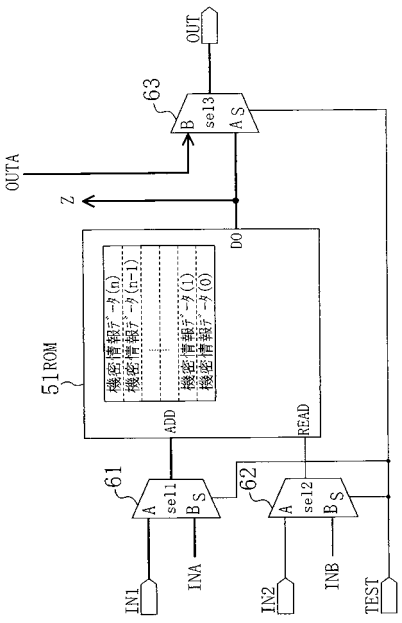
【図２】


TEST
IN1
IN2
AOUT1
CLK
DO
en(CRC)
OUT(CRC)
AOUT2
COMPen
RESULT
address(0)
address(2n+1)
機密CRC(0)
機密情報データ(0)
clear
crc1
crc2
crc(n)

【図３】


10A ROM
データセレクタ
DO
機密情報データ(n)
機密情報データ(n-1)
機密情報データ(1)
機密情報データ(0)
機密CRC(n)
機密CRC(n-1)
機密CRC(1)
機密CRC(0)
アドレスデコーダ
ADD
READ

【図４】


OUT
63
B
sel3
A
S
OUTA
Z
DO
51 ROM
機密情報データ(n)
機密情報データ(n-1)
機密情報データ(1)
機密情報データ(0)
ADD
READ
61
62
sel1
sel2
IN1
INA
IN2
INB
TEST

フロントページの続き

(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１００６番地 松下電器産業株式会社内

Ｆターム(参考) 2G132 AA09 AC03 AD06 AH00 AH07 AK09 AK15 AK29 AL11 AL33
5L106 AA07 DD11 DD14 FF01 GG05