(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2004-152437
(P2004-152437A)
(43)公開日　平成16年5月27日(2004.5.27)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11C 29/00	G11C 29/00	673Z	2G132
G01R 31/28	G06F 12/14	320A	5B017
G06F 12/14	G06F 12/16	330A	5B018
G06F 12/16	G01R 31/28	B	5B025
G11C 16/02	G01R 31/28	D	5L106

審査請求 未請求　請求項の数 5　OL　（全 7 頁）　最終頁に続く

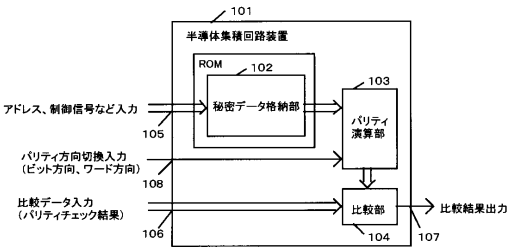
(21)出願番号　特願2002-318390(P2002-318390)
(22)出願日　平成14年10月31日(2002.10.31)

(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　100105647
弁理士　小栗　昌平
(74)代理人　100105474
弁理士　本多　弘徳
(74)代理人　100108589
弁理士　市川　利光
(74)代理人　100115107
弁理士　高松　猛
(74)代理人　100090343
弁理士　濱田　百合子

最終頁に続く

(54)【発明の名称】半導体集積回路装置

(57)【要約】
【課題】チップ面積の増大を抑え、高い秘匿性、高い信頼性で秘密データ格納部の検査を行う。
【解決手段】秘密データを格納する秘密データ格納部３０２と、秘密データ格納部１０２から読み出されたデータを復元不可能なデータ形式に変換するＣＲＣ演算部３０３と、ＣＲＣ演算部３０３から出力されたデータと外部から入力された比較用データ（ＣＲＣ変換結果）との比較結果を外部に出力する比較部３０４とを備える。また、ＣＲＣ演算部３０３は、入力端子３０８に入力されるＣＲＣ演算初期値切換制御信号によりＣＲＣ演算の初期値を切り換えることができる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
データを格納するデータ格納手段と、
前記データ格納手段から読み出されたデータを復元不可能なデータ形式に変換する不可逆変換手段と、
前記不可逆変換手段から出力されたデータと外部から入力された比較用データとの比較結果を外部に出力する比較手段と、
を備える半導体集積回路装置。
【請求項２】
前記不可逆変換手段は、外部からの制御により変換方式の変更が可能であることを特徴とする請求項１に記載の半導体集積回路装置。
【請求項３】
前記不可逆変換手段はパリティ演算を行うものであり、外部からの制御によりパリティの演算方向をビット方向とワード方向に切り換え可能であることを特徴とする請求項２に記載の半導体集積回路装置。
【請求項４】
前記不可逆変換手段は、巡回冗長演算を行うことを特徴とする請求項１または２に記載の半導体集積回路装置。
【請求項５】
外部からの制御により巡回冗長演算の初期値の切り換えが可能であることを特徴とする請求項４に記載の半導体集積回路装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、データ格納部を検査するテスト回路を内蔵した半導体集積回路装置に関する。
【０００２】
【従来の技術】
従来、半導体集積回路装置においては、その信頼性を確保するために、製造時の出荷検査は必須である。しかし、データの秘匿性が要求される秘密データを格納する秘密データ格納部を内蔵した半導体集積回路装置においては、秘密データの秘匿性を損なわないために、データが外部から読み取ることができないように秘密データ格納部を検査する必要がある。
【０００３】
図４および図５は秘密データ格納部をテストするテスト回路を搭載した従来の半導体集積回路装置の構成を示す図である。図４に示す半導体集積回路装置４０１は、秘密データ格納部４０２および比較部４０３を内蔵し、秘密データ格納部４０２の検査時には、外部のＬＳＩテスタから入力端子４０５に入力した比較用のデータと、秘密データ格納部４０２より読み出されたデータとの比較を行い、比較結果のみを出力端子４０６より外部に出力する。以上の構成により、外部に直接秘密データを出力することなく、秘密データ格納部の検査を行うことができる。
【０００４】
図５に示す半導体集積回路装置５０１は、秘密データ格納部５０２、比較データ格納部５０３、ＣＲＣ演算部５０４および比較部５０５を内蔵し、秘密データ格納部５０２の検査時には、秘密データ格納部５０２から読み出されＣＲＣ演算部５０４で巡回冗長演算されたデータと、比較データ格納部５０３から読み出されたデータとの比較を行い、比較結果のみを出力端子５０８より外部に出力する。以上の構成により、外部に直接秘密データの出力や比較用のデータの入力を行うことなく秘密データ格納部の検査を行うことができ、また、図４に示した半導体集積回路装置では可能であった検査用プログラムの解析などにより秘密データの読み出しも不可能となるため、データの秘匿性をより高めることができる。

【０００５】
比較データ格納部を内蔵する半導体集積回路装置は、例えば、特許文献１に開示されている。
【０００６】
【特許文献１】
特開２００１－３４４９９２号公報
【０００７】
【発明が解決しようとする課題】
しかし、図４に示した半導体集積回路装置では、検査の際に比較用のデータをＬＳＩテスタ等から入力する必要があるため、例えば、検査用プログラムの解析により秘密データを特定することが可能であり、非常に高い秘匿性が必要とされる用途には使用できないという問題があった。一方、図５に示した半導体集積回路装置では、比較データ格納部を内蔵することによりチップ面積が増大し、製造コストが上がるという問題がある。また、比較データ格納部が故障していた場合、秘密データ格納部の信頼性が保証できないという問題があった。
【０００８】
本発明は以上の課題を解決するもので、チップ面積の増大を抑え、高い秘匿性、高い信頼性で秘密データ格納部の検査が可能な半導体集積回路装置を提供することを目的とする。
【０００９】
【課題を解決するための手段】
前記の問題を解決するために、請求項１の半導体集積回路装置は、データを格納するデータ格納手段と、前記データ格納手段から読み出されたデータを復元不可能なデータ形式に変換する不可逆変換手段と、前記不可逆変換手段から出力されたデータと外部から入力された比較用データとの比較結果を外部に出力する比較手段と、を備える。
【００１０】
上記構成によれば、データ格納部のデータを不可逆変換したデータを比較対象とすることで、比較用データを解析して可逆的にデータ格納部のデータを復元することが不可能になり秘匿性を高めることができる。さらに、比較用データ格納部を内蔵しないためチップ面積の増大が小さく製造コストの抑えることができる。さらに、比較用データ格納部を内蔵しないため故障時の信頼性低下を回避できる。
【００１１】
請求項２の半導体集積回路装置は、請求項１記載の半導体集積回路装置において、前記不可逆変換手段は、外部からの制御により変換方式の変更が可能であることを特徴とする。
【００１２】
上記構成によれば、外部制御で変換方式を切り換える複数回の検査が可能となるため、より信頼性の高い検査が可能となる。
【００１３】
請求項３に記載の半導体集積回路装置は、請求項２記載の半導体集積回路装置において、前記不可逆変換手段はパリティ演算を行うものであり、外部からの制御によりパリティの演算方向をビット方向とワード方向に切り換え可能であることを特徴とする。
【００１４】
上記構成によれば、不可逆変換演算を単純加算のパリティ演算で行うことで、回路を簡易に構成することができ回路規模の縮小が可能となる。また、ビット方向とワード方向で演算方向を切り換えることで、より信頼性の高い検査が可能となる。
【００１５】
請求項４に記載の半導体集積回路装置は、請求項１または２に記載の半導体集積回路装置において、前記不可逆変換手段は、巡回冗長演算を行うことを特徴とする。
【００１６】
上記構成によれば、不可逆変換演算を巡回冗長演算で行うことにより、不可逆性を強めることができ、秘匿性を高めることができる。

【００１７】
請求項５に記載の半導体集積回路は、請求項４に記載の半導体集積回路装置において、外部からの制御により巡回冗長演算の初期値の切り換えが可能であることを特徴とする。
【００１８】
上記構成によれば、外部制御で巡回冗長の初期値を切り換えて複数回の検査を行うことで、より信頼性の高い検査が可能となる。
【００１９】
【発明の実施の形態】
以下、本発明の実施の形態について、図面を参照しながら説明する。
図１は、本発明の第１の実施の形態に係る半導体集積回路装置の構成を示すブロック図である。図１において、半導体集積回路装置１０１は、秘密データ格納部１０２と、秘密データ格納部１０２から読み出されたデータのパリティビットの計算を行うパリティ演算部１０４と、パリティ演算部１０４から出力されたパリティ演算結果データと入力端子１０６から入力された比較用データ（パリティチェック結果）との比較を行い、比較結果のみを出力端子１０７から外部へ出力する比較部１０５とを備えている。また、パリティ演算部１０４は、入力端子１０９から入力されたパリティ方向切換制御信号により、パリティ演算の方向をビット方向とワード方向に切り換えることができる。
【００２０】
上記構成の半導体集積回路装置１０１において、秘密データ格納部１０３の検査時には、外部のＬＳＩテスタより、データの読み出しに必要なアドレスおよび制御信号を入力端子１０５から入力し、比較用データ（パリティチェック結果）を入力端子１０６から入力する。出力端子１０７には、秘密データのパリティ演算結果データと比較用データとの比較結果が出力され、この比較結果を外部のＬＳＩテスタで期待値比較して良否判定を行う。
【００２１】
第１の実施の形態によれば、秘密データ格納部のデータを不可逆変換したデータを比較対象とすることで、比較用データを解析して可逆的に秘密データ格納部のデータを復元することが不可能になり秘匿性を高めることができる。さらに、比較用データ格納部を内蔵しないためチップ面積の増大が小さく製造コストの抑えることができる。さらに、比較用データ格納部を内蔵しないため故障時の信頼性低下を回避できる。また、パリティ方向をビット方向とワード方向に切り換えて２度検査を実施することで、より信頼性の高い検査を実施することができる。
【００２２】
図２は、本発明の第２の実施の形態に係る半導体集積回路装置の構成を示すブロック図である。図２において、半導体集積回路装置２０１は、秘密データ格納部２０２と、秘密データ格納部２０２から読み出されたデータの巡回冗長演算を行うＣＲＣ演算部２０３と、ＣＲＣ演算部２０３から出力されたＣＲＣ演算結果データと入力端子２０７から入力された比較用データ（ＣＲＣ変換結果）との比較を行い、比較結果のみを出力する比較部２０４とを備えている。
【００２３】
上記構成の半導体集積回路装置２０１において、秘密データ格納部２０２の検査時には、外部のＬＳＩテスタより、データの読み出しに必要なアドレスおよび制御信号を入力端子２０５から入力し、比較用データ（ＣＲＣ変換結果）を入力端子２０６から入力する。出力端子２０７には、秘密データの巡回冗長演算結果データと比較用データとの比較結果が出力され、この比較結果を外部のＬＳＩテスタで期待値比較して良否判定を行う。
【００２４】
第２の実施の形態によれば、主に通信用途に用いられるＣＲＣ演算部を内蔵した半導体集積回路装置において、秘密データ格納部の結果を実施する際にＣＲＣ演算部を利用することで、回路の有効利用が可能となり回路規模の縮小が可能となる。また、巡回冗長演算を行うことにより、不可逆性を強めることができ、秘匿性を高めることができる。
【００２５】

図３は、本発明の第３の実施の形態に係る半導体集積回路装置の構成を示すブロック図である。図３に示す半導体集積回路装置３０１は、図２に示す半導体集積回路装置２０１を発展させたもので、ＣＲＣ演算部３０３の初期値を、入力端子３０８から入力されたＣＲＣ演算初期値切換制御信号により切り換え可能としたものである。ＣＲＣ初期値を切り換えて複数回検査を実施することにより、非常に信頼性の高い検査を実施することができる。

【００２６】

【発明の効果】

以上説明した発明によれば、データ格納部のデータを不可逆変換したデータを比較対象とすることで、比較用データを解析して可逆的にデータ格納部のデータを復元することが不可能になり秘匿性を高めることができる。さらに、比較用データ格納部を内蔵しないためチップ面積の増大が小さく製造コストの抑えることができる。さらに、比較用データ格納部を内蔵しないため故障時の信頼性低下を回避できる。

【００２７】

また、外部制御で不可逆演算の変換方式を切り換える複数回の検査が可能となるため、より信頼性の高い検査が可能となる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る半導体集積回路装置の構成を示すブロック図。

【図２】本発明の第２の実施の形態に係る半導体集積回路装置の構成を示すブロック図。

【図３】本発明の第３の実施の形態に係る半導体集積回路装置の構成を示すブロック図。

【図４】従来の半導体集積回路装置の構成を示すブロック図。

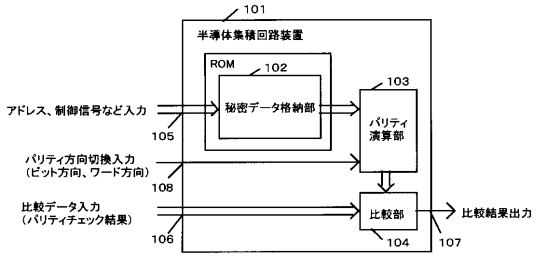
【図５】従来の半導体集積回路装置の構成を示すブロック図。

【符号の説明】

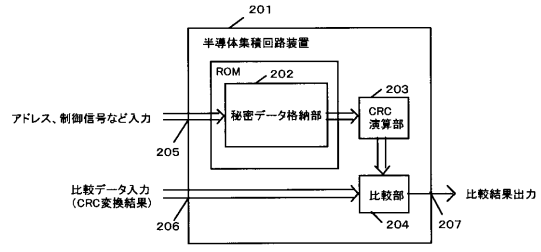
１０１　半導体集積回路装置
１０２　秘密データ格納部
１０３　パリティ演算部
１０４　比較部
１０５　入力端子
１０６　入力端子
１０７　出力端子
１０８　入力端子
２０１　半導体集積回路装置
２０２　秘密データ格納部
２０３　ＣＲＣ演算部
２０４　比較部
２０５　入力端子
２０６　入力端子
２０７　出力端子
３０１　半導体集積回路装置
３０２　秘密データ格納部
３０３　ＣＲＣ演算部
３０４　比較部
３０５　入力端子
３０６　入力端子
３０７　出力端子
３０８　入力端子
４０１　半導体集積回路装置
４０２　秘密データ格納部
４０３　比較部
４０４　入力端子

４０５　入力端子
４０６　出力端子
５０１　半導体集積回路装置
５０２　秘密データ格納部
５０３　比較データ格納部
５０４　ＣＲＣ演算部
５０５　比較部
５０６　入力端子
５０７　入力端子
５０８　出力端子

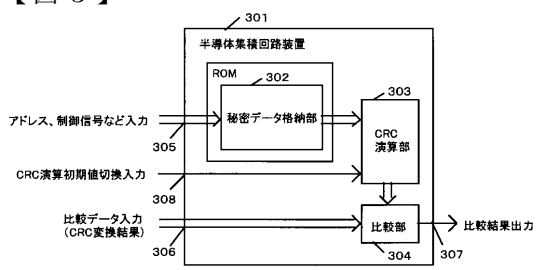
【図１】



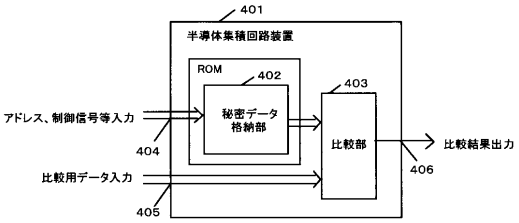
【図２】



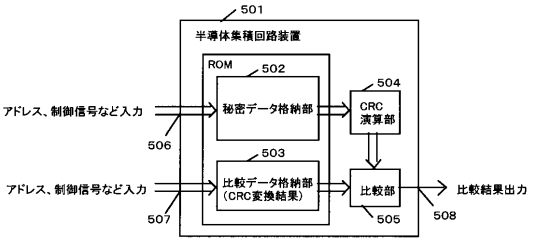
【図３】



【図４】



【図５】



フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	Ｇ０１Ｒ 31/28	Ｖ	
	Ｇ１１Ｃ 17/00	６０１Ｐ	

(72)発明者 片岡 武
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 AK09 AK12 AL00 AL11
5B017 AA03 BA09 CA12
5B018 GA03 JA26 NA04 QA13
5B025 AD05 AD13 AD16 AE09 AE10
5L106 AA07 DD00 EE03 FF05