(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6695805号
(P6695805)

(45)発行日　令和2年5月20日(2020.5.20)　(24)登録日　令和2年4月24日(2020.4.24)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/73 | (2013.01) | G06F | 21/73 | |
| H01L 21/822 | (2006.01) | H01L | 27/04 | U |
| H01L 27/04 | (2006.01) | H04L | 9/00 | 621Z |
| H04L 9/10 | (2006.01) | H04L | 9/00 | 673C |
| H04L 9/32 | (2006.01) | | | |

請求項の数 19　(全 19 頁)

(21)出願番号　特願2016-552915 (P2016-552915)
(86)(22)出願日　平成27年2月19日 (2015.2.19)
(65)公表番号　特表2017-512337 (P2017-512337A)
(43)公表日　平成29年5月18日 (2017.5.18)
(86)国際出願番号　PCT/EP2015/053505
(87)国際公開番号　WO2015/124673
(87)国際公開日　平成27年8月27日 (2015.8.27)
審査請求日　平成30年2月13日 (2018.2.13)
(31)優先権主張番号　14290043.0
(32)優先日　平成26年2月19日 (2014.2.19)
(33)優先権主張国・地域又は機関
欧州特許庁 (EP)

(73)特許権者　515280492
ルネサス・エレクトロニクス・ヨーロッパ・ゲゼルシャフト・ミット・ベシュレンクテル・ハフツング
RENESAS ELECTRONICS EUROPE GMBH
ドイツ、４０４７２　デュッセルドルフ、アルカディアシュトラーセ、１０
(74)代理人　110001195
特許業務法人深見特許事務所

最終頁に続く

(54)【発明の名称】部品が本質的な特徴に基づいて起動される集積回路

(57)【特許請求の範囲】
【請求項１】
集積回路であって、
前記集積回路に本質的に固有の値を有する固有コード（４）を生成するように構成された固有コード発生器（３）と、
前記固有コード（４）に基づいて、前記固有コードの少なくとも一部を暗号化された形態で含む登録パターン（６）を生成するように構成された登録パターン発生器（５）とを備え、
前記集積回路は、前記登録パターン（６）を登録装置（２）に送信し、前記登録装置からイネーブルデータ（７）を受信するように構成され、前記集積回路はさらに、
前記イネーブルデータ（７）および前記固有コード（４）を用いて構成データ（１０）を生成するように構成された構成ファイル発生器（９）と、
前記集積回路の特徴（１３）を起動しまたはディスエーブルにし、かつ前記構成データ（１０）に依存して前記集積回路をカスタマイズするように構成された特徴起動モジュール（１１）とを備え、
前記構成ファイル発生器（９）は、
前記構成データが有効であるか否かを判定するためのエラーチェックを実行し、
前記構成データが有効であるならば、前記特徴起動モジュール（１１）へ前記構成データを出力し、
前記構成データが有効でないならば、誤差信号を出力し、

前記固有コード発生器（３）、前記登録パターン発生器（５）、前記構成ファイル発生器（９）および前記特徴起動モジュール（１１）は、前記誤差信号に基づいてリセットされる、集積回路。

【請求項２】

前記固有コード発生器（３）は、物理的複製防止機能を備える、請求項１に記載の集積回路。

【請求項３】

前記登録パターン発生器（５）は、前記コード（４）からノイズを除去するように構成される、請求項２に記載の集積回路。

【請求項４】

前記登録パターン発生器（５）は、登録パターンを暗号化するように構成され、前記集積回路は、前記登録パターン（６）を暗号化された形態で前記登録装置（２）に送信するように構成される、請求項１～３のうちいずれか１項に記載の集積回路。

【請求項５】

前記構成データ（１０）は起動パターンを備える、請求項１～４のうちいずれか１項に記載の集積回路。

【請求項６】

前記特徴起動モジュール（１１）は、不正確な構成データに応答して最小の特徴の組を起動するように構成される、請求項１～５のうちいずれか１項に記載の集積回路。

【請求項７】

前記固有コード発生器（３）、前記登録パターン発生器（５）、前記構成ファイル発生器（９）、および前記特徴起動モジュール（１１）は最小の特徴の組に含まれる、請求項１～６のうちいずれか１項に記載の集積回路。

【請求項８】

前記固有コード発生器（３）、前記登録パターン発生器（５）、前記構成ファイル発生器（９）、および前記特徴起動モジュール（１１）はそれぞれの固定論理モジュールを備え、前記それぞれの固定論理モジュールは、プログラム可能な論理回路によって構成されていない、請求項１～７のうちいずれか１項に記載の集積回路。

【請求項９】

前記特徴起動モジュール（１１）は、前記構成データに依存して少なくとも周辺モジュールを起動するように構成される、請求項１～８のうちいずれか１項に記載の集積回路。

【請求項１０】

前記特徴起動モジュール（１１）は、前記構成データに依存してクロック速度を設定するように構成される、請求項１～９のうちいずれか１項に記載の集積回路。

【請求項１１】

前記特徴起動モジュール（１１）は、前記構成データに依存して利用可能なメモリの量を設定するように構成される、請求項１～１０のうちいずれか１項に記載の集積回路。

【請求項１２】

前記イネーブルデータ（７）を格納するための不揮発性メモリ（８）をさらに備える、請求項１～１１のうちいずれか１項に記載の集積回路。

【請求項１３】

メモリを含む、請求項１～１２のうちいずれか１項に記載の集積回路。

【請求項１４】

登録装置であって、

請求項１～１３のうちいずれか１項に記載の集積回路（１）を構成するための集積回路構成データ（１５）と、

前記集積回路構成データ（１５）と前記集積回路によって生成された登録パターン（６）とを用いて、前記集積回路についてのイネーブルデータ（７）を生成するように構成されたイネーブルデータ発生器（１６）とを備える、登録装置。

【請求項１５】

システムであって、
請求項１～１３のうちいずれか１項に記載の集積回路（１）と、
請求項１４に記載の登録装置（２）とを備え、
前記集積回路と前記登録装置とは、通信し、任意に安全に通信する、システム。
【請求項１６】
集積回路を登録する方法であって、前記集積回路は、
前記集積回路に本質的に固有の値を有する固有コード（４）を生成するように構成された固有コード発生器（３）と、
前記固有コード（４）に基づいて、前記固有コードの少なくとも一部を暗号化された形態で含む登録パターン（６）を生成するように構成された登録パターン発生器（５）とを備え、
前記集積回路は、前記登録パターン（６）を登録装置（２）に送信し、前記登録装置からイネーブルデータ（７）を受信するように構成され、前記集積回路はさらに、
前記イネーブルデータ（７）および前記固有コード（４）を用いて構成データ（１０）を生成するように構成された構成ファイル発生器（９）と、
前記集積回路の特徴（１３）を起動しまたはディスエーブルにし、かつ前記構成データ（１０）に依存して前記集積回路をカスタマイズするように構成された特徴起動モジュール（１１）とを備え、
前記構成ファイル発生器（９）は、
前記構成データが有効であるか否かを判定するためのエラーチェックを実行し、
前記構成データが有効であるならば、前記特徴起動モジュール（１１）へ前記構成データを出力し、
前記構成データが有効でないならば、誤差信号を出力し、
前記固有コード発生器（３）、前記登録パターン発生器（５）、前記構成ファイル発生器（９）および前記特徴起動モジュール（１１）は、前記誤差信号に基づいてリセットされ、
前記方法は、
前記固有コード発生器（３）により、前記固有コード（４）を生成することと、
前記登録パターン発生器（５）により、前記固有コード（４）に基づいて、前記登録パターン（６）を生成することと、
前記登録パターン発生器（５）により、前記登録パターン（６）を前記登録装置に送ることと、
前記集積回路により、前記登録装置から、前記集積回路を構成するための集積回路構成データ（１５）と前記登録パターンとを用いて生成された前記イネーブルデータ（７）を受信することと、
前記集積回路により、遠隔に生成された前記イネーブルデータを前記集積回路の内部または外部のメモリに格納することとを備える、方法。
【請求項１７】
集積回路（１）を構成する方法であって、前記方法は、
前記集積回路に含まれる固有コード発生器（３）により、前記集積回路に固有の値を有する固有コード（４）を生成することと、
前記集積回路に含まれる登録パターン発生器（５）により、前記固有コード（４）に基づいて、前記固有コードの少なくとも一部を暗号化された形態で含む登録パターン（６）を生成することと、
前記集積回路に含まれる構成ファイル発生器（９）により、遠隔に生成されたイネーブルデータ（７）と、前記固有コード（４）とを用いて構成データ（１０）を生成することと、
前記集積回路に含まれる特徴起動モジュール（１１）により、前記構成データに依存して、前記集積回路の特徴（１３）を起動しまたは停止させ、かつ前記集積回路をカスタマイズすることとを備え、

前記構成ファイル発生器（９）は、
前記構成データが有効であるか否かを判定するためのエラーチェックを実行し、
前記構成データが有効であるならば、前記特徴起動モジュール（１１）へ前記構成データを出力し、
前記構成データが有効でないならば、誤差信号を出力し、
前記固有コード発生器（３）、前記登録パターン発生器（５）、前記構成ファイル発生器（９）および前記特徴起動モジュール（１１）は、前記誤差信号に基づいてリセットされる、方法。

【請求項１８】

前記集積回路（１）が始動するたびに行われる、請求項１７に記載の方法。

【請求項１９】

前記誤差信号に応答して、リセット信号を生成するリセット機能（２６）を有し、
前記固有コード発生器（３）、前記登録パターン発生器（５）、前記構成ファイル発生器（９）および前記特徴起動モジュール（１１）は、前記リセット信号に応答してリセットされる、請求項１に記載の集積回路。

【発明の詳細な説明】

【技術分野】

【０００１】

説明

本発明は、マイクロコントローラまたはシステムオンチップなどの固定論理集積回路に関する。

【背景技術】

【０００２】

いくつかの集積回路のある特徴は、「特徴化（featurization）」として知られる処理によってイネーブルにするかまたはディスエーブルにすることができる。たとえば、特徴化を用いて、通信ポート、タイマーなどといった多くの周辺モジュールの動作電圧、最大クロック動作周波数、記憶容量、およびアベイラビリテイといった広範な異なる機能およびデバイス特性を構成することができる。

【０００３】

特徴化は、フルセットの機能を有するもの（本願明細書では「豊富な機能を持つ集積回路」と称する）から機能が少ないもの（本願明細書では「別形」と称する）まで、チップ上に存在する固定された機能の組を有する異なって特徴化された広範な集積回路を提供するための安価で容易な方法を提示する。

【０００４】

特徴化は、特徴起動機能によって使用され、機能をイネーブルにするかまたはディスエーブルにすることになる装置構成ファイルを不揮発性メモリにプログラムすることを含む。不揮発性メモリへのアクセスは、集積回路製造中に規定される構成アクセス鍵を用いて制御され得る。プログラミングツールが正確な鍵を有さない場合、装置構成ファイルをプログラムすることはできない。

【０００５】

しかし鍵が損なわれると、特徴化処理が阻害される可能性がある。たとえば、無許可のユーザが鍵にアクセスした場合、彼らは、装置構成ファイルを使用して、豊富な機能を持つ集積回路を作成することができる。

【０００６】

フィールドプログラマブルゲートアレイ（ＦＰＧＡ）といったプログラム可能な論理回路において知的財産（ＩＰ）コアを保護するための配置が知られている。

【０００７】

たとえば、米国特許第８４２７１９３Ｂ１号明細書は、ＦＰＧＡなどのプログラム可能な集積回路に実装される回路設計に組込まれたＩＰコアを保護することに関係する。米国特許出願公開第２０１１／１１３３９２Ａ１号明細書は、ＩＰコアを保護する方法につい

て記載している。国際公開第２００８／１２５９９９Ａ２号は、ＦＰＧＡまたはソフトウェアモジュールなどの製品または構成要素における少なくとも１つの機能の制御された起動について記載している。国際公開第２００９／０２４９１３Ａ２号は、ＦＰＧＡなどの設定可能なメモリを有する装置のＩＤを一意的に表す物理的複製防止機能への反応を生成することについて記載している。英国特許出願公開第２２６８６０５Ａ号明細書は、電話交換システムなどのコンピュータ型システムの購入者に機能的なオプションを提供する方法に関係する。

【０００８】

Jorge Guajardo他による"FPGA Intrinsic PUFs and Their Use for IP Protection", Cryptographic Hardware and Embedded Systems - CHES 2007, pages 63 to 80 (2007)、およびJorge Guajardo他による"Physically Unclonable Functions and Public-Key Crypto for FPGA IP Protection", Field Programmable Logic and Applications, 2007 - FPL 207, pages 189 to 195 (2007)も参照する。

【発明の概要】

【課題を解決するための手段】

【０００９】

概要

本発明の第１の局面によれば、固定論理集積回路が提供される。集積回路は、集積回路に本質的に固有の値を有するコードを生成するように構成された固有コード発生器と、固有コードに基づいて登録パターンを生成するように構成された登録パターン発生器とを備える。コードは好ましくはオンデマンドで生成され、一時的である。集積回路は、遠隔に生成されたイネーブルデータ（登録パターンおよび遠隔に格納された構成データを用いて生成される）を格納するためのメモリを備え得る。集積回路は、遠隔に生成されたイネーブルデータおよび固有コードを用いて構成データを生成するように構成された構成ファイル発生器を備える。集積回路は、集積回路の特徴を起動しかつ／またはディスエーブルにし、かつ／または構成データに依存して集積回路をカスタマイズするように構成された特徴起動モジュールを備える。

【００１０】

これは、マイクロコントローラなどの固定論理集積回路の特徴化に対してより厳しい制御を提供するのに役立つことができる。１組の構成データは、集積回路で生成され、集積回路についての固有コード、および具体的にはその集積回路に提供される対応するイネーブルデータの組の両方を有することに依存するからである。したがって、１組のイネーブルデータが傍受されコピーされても、別の異なる固定論理集積回路の特徴を起動するために使用することはできない。

【００１１】

また、各製造された集積回路とそのそれぞれのイネーブルにされた特徴の組とを識別する情報を収集することができるため、半導体ファウンドリで行われる製造をファブレスまたはファブライト集積回路製造業者が監視する方法を提供することができる。これは、過剰生産を低減するかまたは防止するのに役立つことができる。

【００１２】

本願明細書において、「特徴化」という用語は、特徴化だけでなく、トリミングおよびＩＤの初期設定などのカスタマイゼーションも含むことが意図される。したがって、いくつかの状況では、特徴化は特定の特徴をイネーブルにするかまたはディスエーブルにすることを必ずしも含む必要はない。しかし、ある状況では、特徴化は、トリミングまたはＩＤの初期設定なしに、特定の特徴をイネーブルにするかまたはディスエーブルにすることを排他的に含み得る。他の状況において、特徴化は特定の機能ならびにトリミングおよび／またはＩＤの初期設定をイネーブルにするかまたはディスエーブルにすることを含み得る。

【００１３】

登録パターンは、好ましくは、固有コードの少なくとも一部を暗号化された形態で含む

。
【００１４】
固有コード発生器は、好ましくは物理的複製防止機能（ＰＵＦ）である。物理的複製防止機能は、ＳＲＡＭ物理的複製防止機能であり得る。
【００１５】
登録パターン発生器は、好ましくは、コードからノイズを除去するように構成される。登録パターン発生器は、登録パターンを暗号化するように構成され得る。集積回路は、登録パターンを暗号化された形態で外部登録装置に送信するように構成され得る。
【００１６】
構成モジュールは、構成データに依存して１組の特徴を起動するように構成され得る。構成モジュールは、構成データに依存して、１組の周辺モジュール（ユニバーサルな非同期レシーバ／トランスミッタ（ＵＡＲＴ）またはアナログ－デジタル変換器（ＡＤＣ）など）を起動するように構成される。構成モジュールは、構成データに依存してクロック速度を設定するように構成され得る。
【００１７】
特徴起動モジュールは、不正確な構成データに応答して最小の特徴の組を起動するように構成され得る。最小の特徴の組は、特徴化を可能にするモジュールを含み得る。好ましくは、最小の特徴の組は、特徴化のみにおいてまたは主として特徴化に使用されるモジュールを主に、または該モジュールのみを含む。たとえば、固有コード発生器、登録パターン発生器、構成ファイル発生器、および特徴起動モジュールは、最小の特徴の組に含まれ得る。固有コード発生器、登録パターン発生器、構成ファイル発生器、特徴起動モジュール、およびそれぞれの固定論理モジュールは、好ましくは固定論理モジュールを備える。
【００１８】
集積回路はデジタル集積回路であり得る。集積回路はメモリを含み得る。メモリはＤＲＡＭまたはＳＲＡＭなどの揮発性メモリであり得る。メモリは、ＥＰＲＯＭ、ＥＥＰＲＯＭ（登録商標）、ＮＯＲフラッシュまたはＮＡＮＤフラッシュなどの不揮発性メモリであり得る。集積回路は、マイクロプロセッサ、マイクロコントローラ、または信号処理チップなどのマイクロ集積回路であり得る。集積回路は、フラッシュメモリが埋込まれたマイクロコントローラであり得る。集積回路は、フラッシュメモリが埋込まれていないプロセッサであり得る。集積回路は、システムオンチップ（ＳｏＣ）であり得る。集積回路は、特定用途向け集積回路チップ、標準ロジック、またはディスプレイドライバなどの論理集積回路であり得る。
【００１９】
本発明の第２の局面によれば、登録装置が提供される。（コンピュータシステム上でソフトウェアで実装され得る）登録装置は、論理集積回路を構成するための構成データと、構成データおよび集積回路によって生成された登録パターンを用いて集積回路についてのイネーブルデータを生成するように構成されたイネーブルデータ発生器とを備える。
【００２０】
本発明の第３の局面によれば、集積回路および登録装置を備えるシステムが提供される。集積回路および登録装置は、安全に（つまり暗号化されて）通信し得る。登録パターンを送る当事者（たとえば半導体ファウンドリ）は、証明書または他の認証手段を用いて登録装置によって認証され得る。
【００２１】
本発明の第４の局面によれば、集積回路を登録する方法が提供される。当該方法は、集積回路に固有の値を有するコードを生成することを備える。当該方法は、固有コードに基づいて登録パターンを生成することと、登録パターンを外部登録装置に送ることとを備える。当該方法は、登録装置からイネーブルデータを受信することを備える。当該方法は、遠隔に生成されたイネーブルデータをオンチップで（すなわち集積回路上に）格納することを備え得る。
【００２２】

当該方法は、遠隔に生成されたイネーブルデータをオフチップで（つまり外部メモリに）格納することを備え得る。

【００２３】

集積回路を登録する方法は、ハードウェアで実装される方法であり得る。

本発明の第５の局面によれば、集積回路を構成する方法が提供される。当該方法は、遠隔に生成されたイネーブルデータと、集積回路に固有の値を有するコードとを用いて構成データを生成することを備える。当該方法は、構成データに依存して集積回路の特徴を起動しかつ／または停止させることを備える。

【００２４】

当該方法は、外部メモリからイネーブルデータを検索することを含み得る。

集積回路を構成することは、集積回路が開始するたびに行われ得る。

【００２５】

集積回路を構成する方法は、ハードウェアで実装される方法であり得る。

図面の簡単な説明

本発明のある実施形態について、添付の図面を参照して例として記載する。

【図面の簡単な説明】

【００２６】

【図１】集積回路および外部登録装置の概略ブロック図である。

【図２】集積回路、外部メモリおよび外部登録装置の概略ブロック図である。

【図３】マイクロコントローラまたはシステムオンチップの概略ブロック図である。

【図４】集積回路のあらかじめ起動された特徴を例示する図である。

【図５】特徴化の制御を例示する図である。

【図６】登録に含まれるモジュールの概略ブロック図である。

【図７】登録の方法のプロセスフロー図である。

【図８】起動パターンのオンチップ生成を例示する図である。

【図９】特徴起動の方法のプロセスフロー図である。

【図１０】周辺モジュールのマルチビット起動を例示する図である。

【図１１】クロック周波数を設定することを例示する図である。

【図１２】起動パターンのいくつかの例の表である。

【図１３】メモリの上位境界を設定することを例示する図である。

【図１４】ファブライト製造環境における装置登録を例示する図である。

【図１５】ファブレス製造環境における装置登録を例示する図である。

【発明を実施するための形態】

【００２７】

ある実施形態の詳細な説明

図１を参照して、集積回路１および外部登録装置２が示される。集積回路１は、（プログラム可能論理回路に対して）固定論理装置である。したがって、集積回路１は論理回路および他のモジュールを含み、それらの機能は、製造時には固定されているが、製造後に個々に選択可能にイネーブルまたはディスエーブルにされることができ、かつ／またはカスタマイズされることができる。

【００２８】

集積回路１は、集積回路１に本質的に固有コード４を再生可能に生成するための固有コード発生器３を含む。固有コード発生器３は、物理的複製防止機能（ＰＵＦ）に基づく。固有コード４は、集積回路１における要素に本質的である物理的特性に依存する。たとえば、固有コード発生器３は、メモリ要素の始動時の値を用いて固有コード４を生成し得る。コード４は、同じ設計を有し、同じマスクの組（図示せず）を用いて同時に製造される他の集積回路（図示せず）に対しても集積回路１に固有である。コード４は、オンデマンドで生成され、一時的である。換言すれば、コード４は生成され、その後永久に格納されるのではない。初期設定されたシリアル番号または他の初期設定されたルートオブトラスト（route-of trust）は、固有コード４として使用されない。

【００２９】
集積回路１は、固有コード４を用いて登録パターン６を生成するための装置登録モジュール５を含む。登録段階において、集積回路１は登録装置２に登録パターン６を送信し、引き換えに構成イネーブラー７（本願明細書において「コードコンストラクタデータ」または「ヘルパデータ」とも称する）を受信する。集積回路１は、当初の（つまりノイズがある）固有コード４を登録装置２に平文で送信しない。したがって、当初の固有コード４は集積回路２から離れない。代わりに、暗号化され得る登録パターン６などの処理されたコードのみが送信される。集積回路１は、構成イネーブラー７を格納するための不揮発性メモリ８と、固有コード４および構成イネーブラー７を用いて特徴起動パターン１０を生成するための構成ファイル発生器９とを含み得る。集積回路１は、集積回路特徴１３（本願明細書において単に「特徴」と称する）をイネーブルにし、かつ／またはディスエーブルにするためのイネーブルおよび／またはディスエーブル信号１２を生成する特徴起動モジュール１１を含む。特徴は、ユニバーサルな非同期レシーバ／トランスミッタ（ＵＡＲＴ）またはアナログ－デジタル変換器（ＡＤＣ）などの周辺モジュールであり得る。特徴は、クロック速度などのパラメータであり得る。

【００３０】
登録装置２は、集積回路１についての装置構成ファイル１５を格納する記憶装置１４と、構成イネーブラー７を生成するための構成イネーブラー発生器１５とを含む。

【００３１】
構成イネーブラー７は、具体的には集積回路１について生成され、起動パターン１０は、構成イネーブラー７と、構成イネーブラー７を作成するために使用されたコード４とを用いてのみ生成することができる。さらに、起動パターン１０は必要に応じてオンチップで生成される。したがって、これは、特徴化のより厳しい制御を提供するのに役立つことができる。

【００３２】
図２を参照して、集積回路１には構成イネーブラー７を格納するための外部不揮発性メモリ８′が設けられ得る。したがって、集積回路１は、オンチップの不揮発性メモリ８を含む必要はない。

【００３３】
図３を参照して、第１および第２の集積回路$1_1$，$1_2$が示される。第１の集積回路$1_1$は、豊富な機能を持つ集積回路であることが意図され、第２の集積回路$1_2$は、部分的な機能を持つ集積回路、つまり豊富な機能を持つ集積回路よりも少ない機能がイネーブルにされるものであることが意図される。

【００３４】
第１および第２の集積回路$1_1$，$1_2$の特徴化は、それぞれの第１および第２の装置構成ファイル$15_1$，$15_2$によって設定される。第１および第２の装置構成ファイル$15_1$，$15_2$は、具体的には第１および第２の集積回路$1_1$，$1_2$について生成される。

【００３５】
したがって、第１の構成イネーブラー$1_1$がコピーされたとしても、フルセットの特徴をイネーブルにすることはいうまでもなく、第２の集積回路$1_2$の特徴化に使用することはできない。

【００３６】
再び図１を参照して、集積回路１の少なくともいくつかの固定論理特徴は、製造後および特徴化前に起動され動作可能である。したがって、登録に先立ち、集積回路１は少なくとも部分的に特徴化（または「部分的に起動」）される。特に、コード発生器３、装置登録モジュール５、構成ファイル発生器９、および特徴起動モジュール１１は、起動され動作可能である固定論理モジュールである。

【００３７】
図４を参照して、マイクロコントローラまたはシステムオンチップ１において、少なくとも１つの中央処理装置１７、有限のクロック速度で、つまり最速の利用可能な（つまり

最速の特徴化可能な）クロック速度未満で動作し得るクロック１８、その入手可能なサイズは利用可能な最大値未満にあり得るメモリ１９、および通信周辺モジュール２０が特徴化を可能にするためにアクティブであり動作可能である。

【００３８】

図５も参照して、コード発生器３、装置登録モジュール５、構成ファイル発生器９、および特徴起動モジュール１１（本願明細書では「あらかじめ起動されたオンチップモジュール」と称する）への電圧供給２１、クロック信号２２およびリセット信号２３は、集積回路１上において、中央処理装置１７または直接メモリアクセスモジュールなどの他の処理装置によって制御可能ではない。したがって、あらかじめ起動されたオンチップモジュール３，５，９，１１への供給電圧およびクロック信号線２１，２２は保護される。換言すれば、処理要素は、スイッチオンまたはオフすることも、あらかじめ起動されたオンチップモジュール３，５，９，１１への供給電圧およびクロックを変動させることもできない。たとえば、内部（つまりオンチップ）供給電圧２１は、ピン２５を介して集積回路１に提供される外部供給電圧２４から、取得され得る、たとえば直接供給され得、クロック信号２３はオンチップで生成され得る。さらに、あらかじめ起動されたオンチップモジュール３，５，９，１１へのリセット信号２３は、始動の終わりなどの制限された状況の組に応答して、または構成ファイル発生器９によって生成されている誤差信号２７に応答して、リセット機能２６によって生成され得る。リセット機能２６および誤差信号２７は保護される。したがって、処理要素（中央処理装置１７など）は、たとえあったとしても、ある状況以外では誤差信号２７を自由に生成し操作することができない。リセット機能２６はハードワイヤードで実施され得る。

【００３９】

あらかじめ起動されたオンチップモジュール３，５，９，１１は、好ましくは特定のオンチップ回路の形態を取る。

【００４０】

コード発生器３は、中央処理装置１７または他の処理装置によってアクセス可能ないずれのインターフェイスも有さない。コード発生器３は、好ましくは、１つの入力インターフェイスと１つの出力インターフェイスとを有し、出力インターフェイスは、装置登録モジュール５および構成ファイル発生器９に直接結合される。インターフェイスの数を限定することで、中央処理装置１７または他の処理要素もしくはユニットによってコード４の操作または変更を防止するかまたは妨げるのに役立つことができる。入力／出力インターフェイスは、コード発生器３を実装するために使用されるＰＵＦに依存して異なる形態を取ることができる。たとえば、ＳＲＡＭ　ＰＵＦの場合には、インターフェイスは、ノイズがあるデータのソースとして使用されることになるＳＲＡＭメモリ（図示せず）へのアドレスおよびデータ線であり得る。

【００４１】

好ましくは、コード発生器３は、コード４の生成に影響を及ぼすかまたは生成を操作し得る外部電圧２４による操作からそれを保護するための回路（図示せず）を埋込む。さらに、ノイズがあるデータのソースを、経時的に変動しないように自動的に再較正するための回路（図示せず）が設けられ得る。そのような回路は、たとえば、装置登録モジュール５および構成ファイル発生器９によって使用されないときは常に、コード発生器３内の供給電圧を動的にオフにすることができる。

【００４２】

装置登録モジュール５は、中央処理装置１７または他の処理要素が登録パターン６の生成をトリガすることを可能にする信号２９のために１つの入力インターフェイス２８を有する。装置登録モジュール５は、中央処理装置１７または他の処理装置（ＤＭＡなど）が登録パターン６を１つ以上の動作で読出すことを可能にする１つの出力インターフェイス２９を１つ以上のレジスタの形態で有する。装置登録モジュール５は、登録パターン６の生成がいつ完了したかを示すために、中央処理装置１７または他の処理装置に状況情報（図示せず）を提供し得る。

【００４３】
装置登録モジュール５は、さらに処理する前にコード４からノイズを除去することによって、たとえば暗号化を適用することによってコード４を処理し得る。
【００４４】
また図１を参照して、特定のマイクロコントローラまたはシステムオンチップなどの集積回路１について生成された登録パターン６は、構成イネーブラー発生器１６が集積回路１にバインドされた構成イネーブラー７を生成するのに十分な情報を含む。登録パターン６を盗聴しても、潜在的な攻撃者がコード４を検索するのに十分な情報はもたらされない。登録パターン６は、いずれかのそのような操作が構成イネーブラー発生器１６によって検出されることができるようなやり方で、潜在的な操作からさらに保護され得る。登録パターン６は、構成イネーブラー発生器１６と共有される鍵でさらに暗号化され得る。
【００４５】
構成イネーブラー発生器１６は、登録装置として機能する安全性の高い開封防止用のハードウェアセキュリティーモジュール（ＨＳＭ）に実装される。この発生器１６のインストールおよびメンテナンスはＩＣ製造業者によって制御され対処される。装置構成ファイル１５は、ＨＳＭに安全に格納され、そのインストールおよびメンテナンスはＩＣ製造業者によって制御され対処される。
【００４６】
図１をなお参照して、構成イネーブラー７は、構成ファイル発生器９がコード４を起動パターン１０に転換するために十分な情報を含む。構成イネーブラー７および関連付けられた登録パターン６を知っている攻撃者は、構成イネーブラー発生器１６で処理された生成アルゴリズムを再構築するために十分な情報を有していない。構成ファイル発生器９は、構成イネーブラー７が操作されたかどうかを検出するためにも配置され得る。構成イネーブラー発生器１６は、構成ファイル発生器９と共有される鍵で構成イネーブラー７を暗号化し得る。
【００４７】
構成ファイル発生器９は、中央処理装置１７または他の処理要素（ＤＭＡなど）が１つ以上の動作で登録パターン６構成イネーブラー７を書込むことを可能にする入力インターフェイス３０を１つ以上のレジスタの形態で有する。構成ファイル発生器９は、起動パターン１０の生成が成功したことおよび／またはエラーがいつ生じたかを示すために、状況情報（図示せず）を中央処理装置１７または他の処理要素に提供し得る。
【００４８】
構成ファイル発生器９は、起動パターン１０を特徴起動モジュール１１に直接出力する。特徴起動モジュール１１は、中央処理装置１７または他の処理要素が使用することができる入力インターフェイスは有していない。これは、起動パターン１０の操作を妨げるかまたは防止するのに役立つことができる。
【００４９】
たとえばリセットに続いて集積回路１が動作を開始した後で、構成イネーブラー９はデフォルト値を有する起動パターン１０（本願明細書では「デフォルト起動パターン」と称する）を生成することができ、その結果、起動されている特徴１３がないか、または、通信モジュールなどの少数の予め規定された特徴１３が起動される。
【００５０】
特徴起動モジュール１１は、１組の独立した信号１２を出力して、１つ以上の特徴１３、たとえば周辺モジュールをイネーブルにする（または「起動する」）かまたはディスエーブルにする。各イネーブル（またはディスエーブル）信号１２は、通信インターフェイスモジュール、タイマー、グラフィカル処理装置などといった少なくとも１つの周辺モジュールのイネーブル入力（図示せず）に接続される。
【００５１】
各イネーブル（またはディスエーブル）信号１２は、ＡＮＤゲート（図示せず）を用いて、ユーザコンフィギュラブルなイネーブル信号（図示せず）と結合されることができる

。イネーブル（またはディスエーブル）信号１２は、中央処理装置１７または他の処理装置によって直接操作されることができないように配置される。

【００５２】

特徴１２がディスエーブルにされると、特徴１２は動作しない。したがって、中央処理装置１７または他の処理装置による試みは、通信しないこと、タイマーの音がしないこと、グラフィック処理がないことなどといった予期しない挙動をもたらす。

【００５３】

デフォルト起動パターン１０がリセット後に提供された場合、特徴起動モジュール１１は、すべての特徴１３、または一部を除くすべての特徴１３をディスエーブルにすることができる。したがって、集積回路１における１組の特徴１３があらかじめイネーブルにされていたとしても、それらの特徴１３はその後、リセットに続き再開に先立ってディスエーブルにされ得る。

【００５４】

特徴起動モジュール１１の出力は、整数値を提供する１つ以上のマルチビットレジスタの組（図示せず）も含み得る。これらのレジスタは、メモリアドレス境界、クロックマルチプライヤなどといった集積回路リソースに部分的または完全な構成情報を提供し得る。レジスタ（図示せず）は、中央処理装置１７または他の形態の処理装置によって操作されることができないように配置される。デフォルト起動パターン１０がリセット後に提供された場合、特徴起動モジュール１１は、最小装置構成、たとえば有限のメモリ空間を開けること、最小値クロックマルチプライヤを提供すること、などをもたらすことができる。

【００５５】

装置に本質的なパラメータを用いる特徴化は、２つの段階、すなわち登録および特徴起動段階に概して分割される。

【００５６】

登録

図６および図７を参照して、装置登録の処理が示される。

【００５７】

集積回路１において、装置登録モジュール５は、コード発生器３から固有コード４を取得し、コード４からノイズを除去し、登録パターン６を生成する（ステップＳ１）。暗号化モジュール１８は、登録装置２の公開鍵（図示せず）で登録パターン６を暗号化し得る（ステップＳ２）。装置登録モジュール５は、登録パターン６を登録装置２に送信する（ステップＳ３）。登録パターン６を送る当事者（たとえば半導体ファウンドリ）は、証明書（図示せず）または他の手段を用いて、登録装置２によって認証され得る。登録パターン６は、ｑビットの整数の形態を取る。

【００５８】

登録装置２は異なる形態を取ることができる。この場合、登録装置２は、プログラマブルハードウェアセキュリティーモジュール（ＨＳＭ）の形態を取る。

【００５９】

登録装置２は登録パターン６を受信し（ステップＳ４）、コードが暗号化されていれば、解読モジュール（図示せず）が登録パターン６を解読する（ステップＳ５）。構成イネーブラー発生器１６が記憶装置１４から装置構成ファイル１５を検索する（ステップＳ６）。構成イネーブラー発生器１６は、登録パターン６および装置構成ファイル１５に基づいて集積回路１に特有の構成イネーブラー７を生成し（ステップＳ７）、構成イネーブラー７を集積回路１に送信する（ステップＳ８）。構成イネーブラー７は、ｐビットの整数の形態を取る。好ましくは、ｐは少なくとも３２である。ｐおよびｑの値が大きいほど、より安全な登録を行なうことができる。

【００６０】

集積回路１は構成イネーブラー７を受信し（ステップＳ９）、不揮発性メモリに構成イネーブラーを格納する（ステップＳ１０）。

【００６１】

登録は、集積回路１に対して一度実行される。ただし登録装置２は多くの異なる集積回路１を登録してもよい。

【００６２】

特徴起動

図８および図９を参照して、特徴起動の処理が示される。

【００６３】

集積回路１が登録された後、特徴起動が行われることができる。

集積回路１が開始すると、特徴起動が行われる。

【００６４】

構成ファイル発生器９は、固有コード４を用いて、起動パターン１０の形態で構成ファイルを生成することを排他的に可能にする多くの機能を含む。構成ファイル発生器９は、ノイズ低減ユニット（図示せず）、無作為抽出器ユニット（図示せず）、デジタルパターン抽出ユニット（図示せず）、および後工程ユニット（図示せず）を含み得る。

【００６５】

構成ファイル発生器９は、メモリ８から構成イネーブラー７を検索する（ステップＳ１１）。固有コード発生器３は、コード４の別のインスタンスを生成する（ステップＳ１２）。構成ファイル発生器９は、コード４および構成イネーブラー７を用いて起動パターン１０を抽出する（ステップＳ１３）。起動パターン１０は、ｎビットの整数の形態を呈し、ここではｎ＜ｐである。

【００６６】

１つの構成イネーブラー７のみが集積回路１の正確な起動パターン１０を生成することになる。したがって、構成ファイル発生器９は、起動パターン１０が有効であるかどうかを判定するためのエラーチェックを行なうことができる（ステップＳ１４）。

【００６７】

起動パターン１０が有効な場合、構成ファイル発生器９は、構成レジスタ２５に格納されるように起動パターン１０を特徴起動モジュール１１に出力する（ステップＳ１５）。

【００６８】

しかし、起動パターン１０が無効の場合、構成ファイル発生器９は誤差信号３４を任意に出力し得る（ステップＳ１６）。誤差信号２４は、装置１をディスエーブルにすることができる装置リセット機能２７に供給され得る。しかし、いくつかの場合には、装置１は最小の組の機能で動作することができる。たとえば、すべてのコンフィギュラブル周辺モジュールがディスエーブルにされ、最低量のメモリが設定される。

【００６９】

構成イネーブラー７は、オフチップで格納されることができる。たとえば、集積回路１は、たとえば図２に示されるように別個のフラッシュまたはＥＥＰＲＯＭ（登録商標）チップに接続され得る。これは、フラッシュメモリを有さない集積回路の特徴化を可能にすることができる。

【００７０】

特徴起動の例

特徴起動は、メモリの上位境界のアドレス、クロック周波数などといったデバイスパラメータを固定する周辺モジュールおよび整数値の各々および／またはグループをイネーブルにするかまたはディスエーブルにする信号を生成するために用いることができる。

【００７１】

単純な符号化体系を用いて機能をイネーブルにするかまたはディスエーブルにすることができる。たとえば、２ビットの記号と、１つの反転入力および１つの非反転入力を有するＡＮＤゲートとを用いることができる。したがって、たとえば「０１」という値を有する記号は、値「１」を有する起動信号をもたらし得、その結果、ある機能がイネーブルにされる。「１０」などのいずれかの他の値を有する記号は、値「０」を有する起動信号をもたらし得、その結果、ある機能がイネーブルにされない。

【００７２】

図１０を参照して、ｒビットの起動信号が使用されてもよい。ここでｒ＞２である。たとえば、ｒは値４を取ることができる。

【００７３】

たとえば、主構成レジスタ３３のビット番号０～３を用いて、第１の周辺モジュール１３$_A$の起動を制御することができる。第１、第２、および第３のＡＮＤゲートＱ１，Ｑ２，Ｑ３が用いられ、第１および第２のＡＮＤゲートＱ１およびＱ２は、１つの反転入力および１つの非反転入力を有する。主構成レジスタ２３のビット番号０は、第１のゲートＱ１の反転入力に供給される。主構成レジスタ３３のビット番号１は、第１のゲートＱ１の非反転入力に供給される。主構成レジスタ２３のビット番号２は、第２のゲートＱ２の反転入力に供給される。主構成レジスタ３３のビット番号３は、第２のゲートＱ２の非反転入力に供給される。第１および第２のゲートＱ１，Ｑ２の出力は、第３のゲートＱ３への入力として供給される。したがって、ビット番号３～０において値「１０１０」（１６進法の０×Ａ）を有する記号は、第１の周辺モジュール１３$_A$をイネーブルにすることになる。他の値は周辺モジュール１３$_A$をイネーブルにすることはない。

【００７４】

同様に、第４、第５、および第６のＡＮＤゲートＱ４，Ｑ５，Ｑ６の同様の構成を用いて第２の周辺モジュール１３$_B$の起動を制御するために、主構成レジスタ２３のビット番号７～４を用いることができる。この場合、第５のＡＮＤゲートＱ５のみがビット番号６に対応する反転入力を有する。したがって、ビット番号７～４における値「０１１１」（１６進法の０×７）を有する記号は、第２の周辺モジュール１３$_B$をイネーブルにすることになる。

【００７５】

外部試験機器３６が周辺モジュール１３$_A$，１３$_B$を制御することを可能にするために、特徴起動モジュール１１と、生産試験モジュール３８によって制御される各周辺モジュール１３$_A$，１３$_B$との間にマルチプレクサ３７$_A$，３７$_B$を直列に設けることができる。生産試験モジュール３８は、登録パターンの必要性なしに集積回路１が試験されることを可能にすることができる。試験モジュール３８は、特徴起動に対する制御の迂回を妨げるかまたは防止するために保護される。たとえば、これは、使用後にモジュール３８を自動的に吹き飛ばすことによって、かつ／またはウェハスクライブ線（図示せず）にモジュール３８を配置することによって、モジュール３８に対するアクセスを制御するための鍵（図示せず）を用いることで実現され得る。これは、その後のウェハダイシング工程中にモジュール３８が破壊されることを意味することになる。

【００７６】

図１１を参照して、ｒビットの起動信号を用いてクロック速度を制御し得る。

ビット番号８および９は、２ビットの指数ｎをクロックマルチプライヤモジュール３９に提供する。ここでｎ＝０、１、２、または３である。ビット番号１０は、パリティコントロールである。ビット番号１１は、ビット１０に対して補足的な値を取る。ＸＯＲおよびＡＮＤゲートの配置を用いると、記号「０１１０」（１６進法の０×６）を用いてクロックマルチプライヤを４に設定することができる。

【００７７】

図１２は、主構成レジスタ３３のビット０～１１について３つの可能な起動コードをリストする表３０を示す。

【００７８】

図１３を参照して、主構成レジスタ３３の一部分を別のレジスタ３１にコピーしてパラメータを提供することができる。この例では、ビット番号１６～１８が上位アドレス境界レジスタ３１のビット２０～２２にコピーされる。ビット０～１９は「１」に設定され、ビット２３～３１は「０」に設定される。したがって、１ＭＢの精度を有する８ＭＢのフラッシュメモリの場合には、上位アドレス境界レジスタ４１は、０×０ＦＦＦＦＦ～０×ＦＦＦＦＦＦの値を取ることができる。

【００７９】

図１４および図１５を参照して、装置登録は、各製造された集積回路およびそのそれぞれのイネーブルにされた特徴の組を識別する情報が収集されるため、半導体ファウンドリ４３で行われる製造をファブレスまたはファブライトＩＰ所有者４２が監視するためのやり方を提供する。これは、過剰生産を低減するかまたは防止するのに役立つことができる。

【００８０】

上記の実施形態に対して多くの変更がなされ得ることが認識されるであろう。

たとえば、構成イネーブラー７はハッシュ関数によって保護されてもよい。

【００８１】

装置登録は、ファブレスまたはファブライト半導体ベンダーを過剰生産から保護することを可能にする。しかし、装置登録は、相手先商標製造会社および／またはオリジナル装置製造業者（または「顧客」）を保護して、彼らの製品が改竄または偽造されないように保護することもできる。可能な１つのスキームでは、固定論理集積回路は特徴化される前に顧客に送達される。そのため、集積回路は、特徴化処理が行われることを可能にするために部分的にのみ起動されるが、顧客ソフトウェアを実行することはできない。顧客はまず、彼らの生産設備にあるいずれかの登録装置を用いて、またはインターネットを通じて登録装置に遠隔にアクセスして登録処理を行う。

【図１】

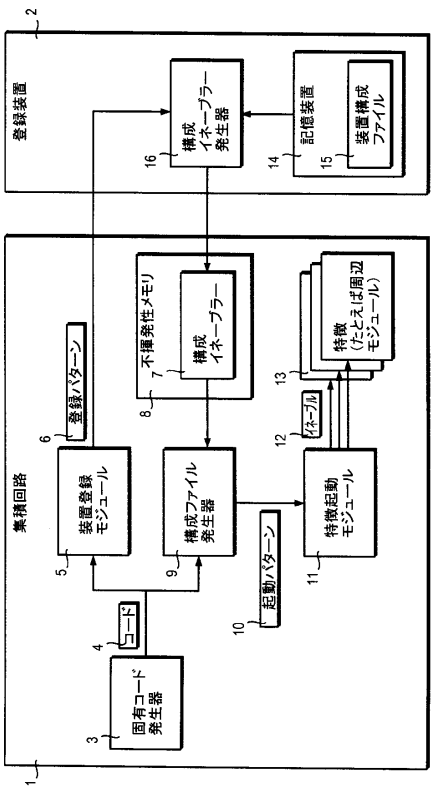


Fig. 1

【図２】

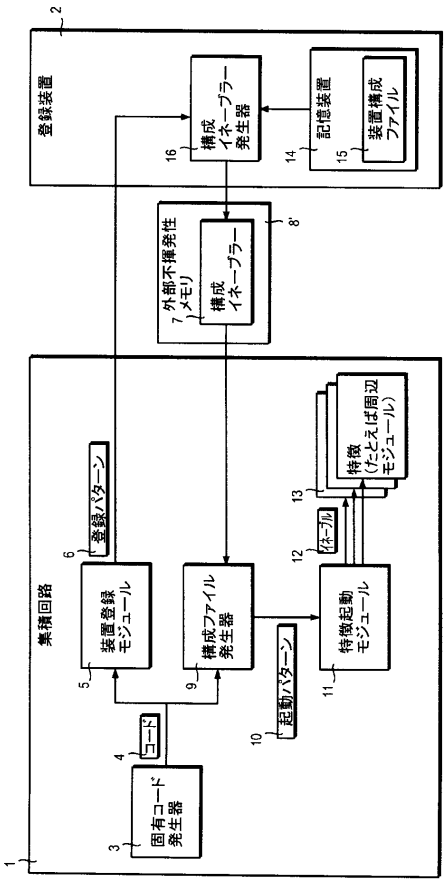


Fig. 2

【図３】

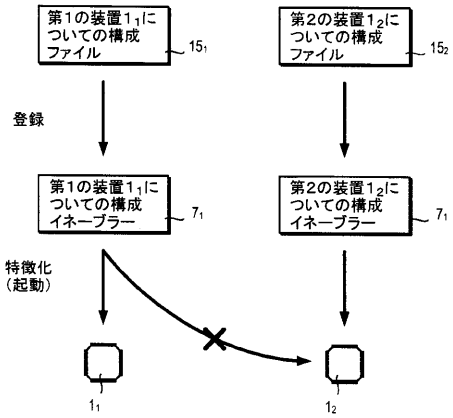


Fig. 3

【図４】

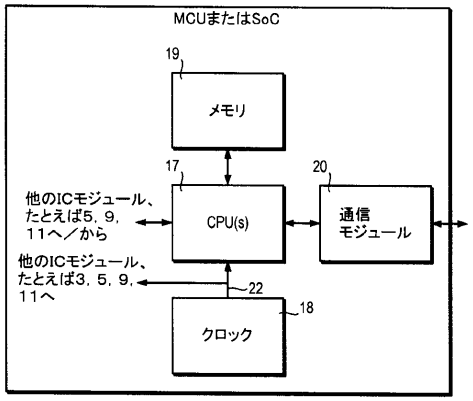


Fig. 4

【図５】

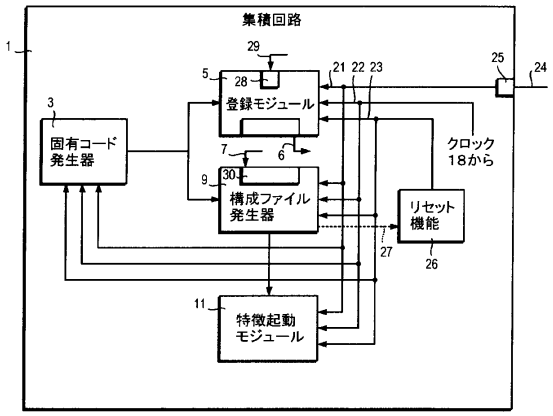


Fig. 5

【図６】

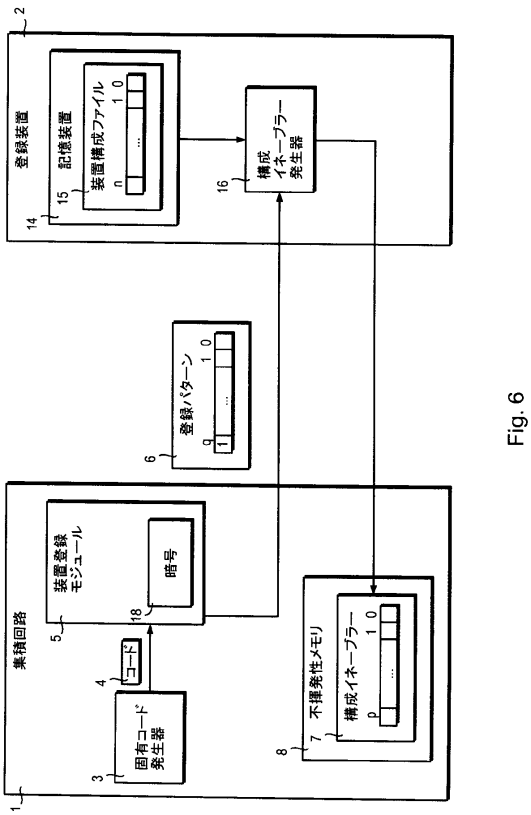


Fig. 6

【図７】

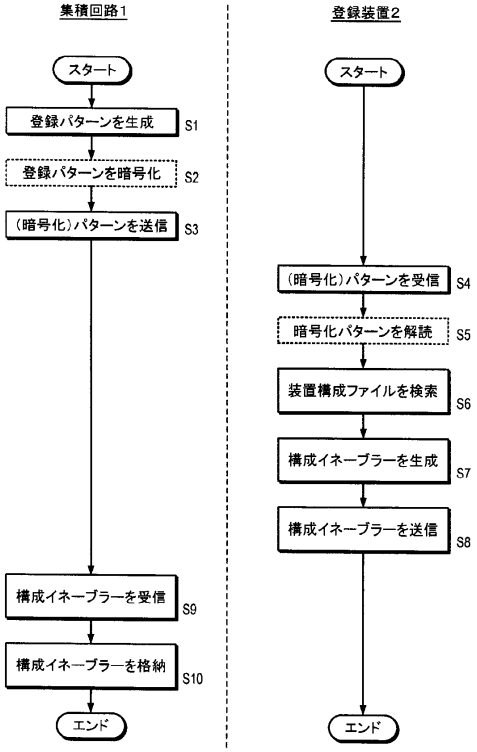


Fig. 7

【図８】

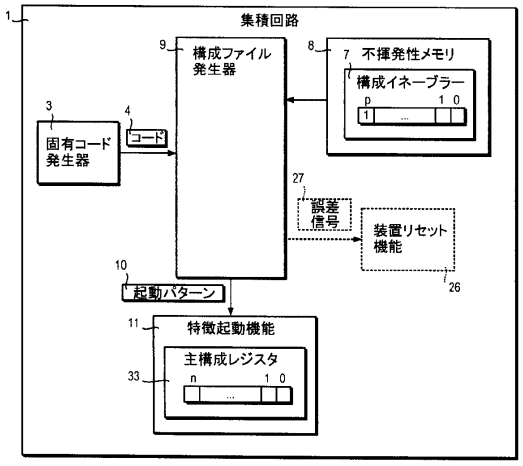


Fig. 8

【図９】

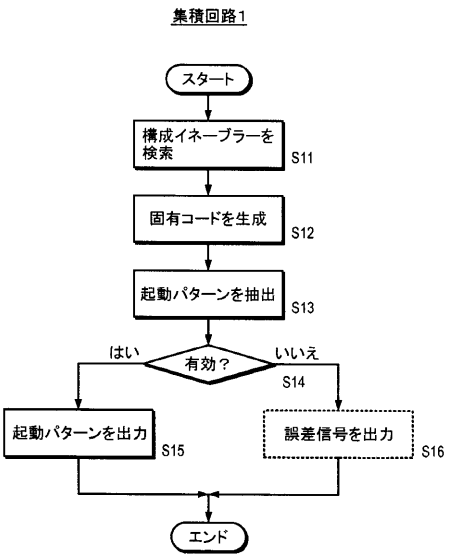


Fig. 9

【図１０】

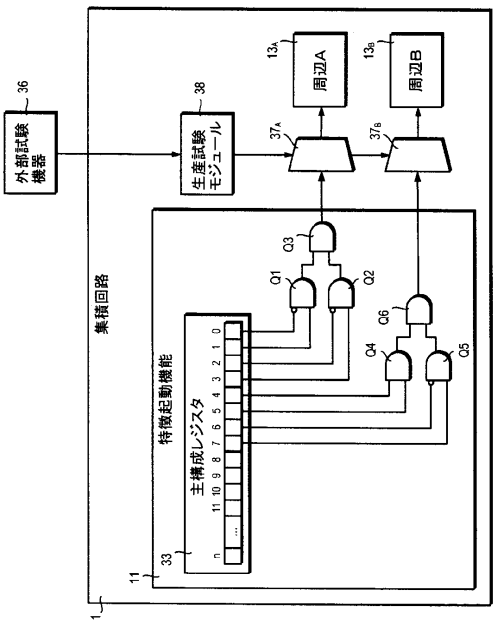


Fig. 10

【図１１】

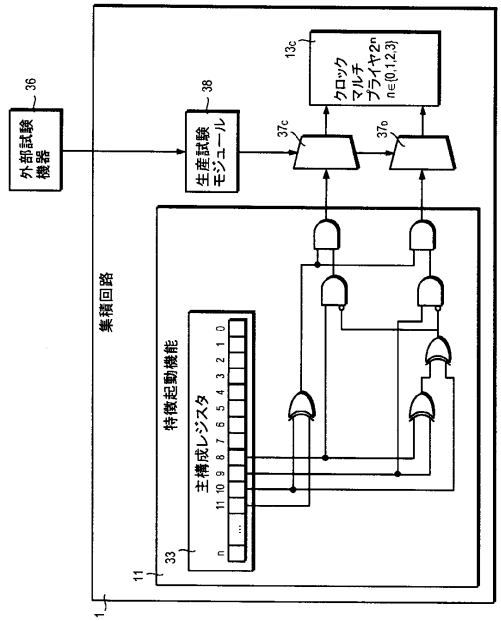


Fig. 11

【図１２】

| 起動パターン | 周辺A状態 | 周辺B状態 | クロック周波数マルチプライヤ |
|---|---|---|---|
| 0x60A | アクティブ | 非アクティブ | 4 |
| 0x870 | 非アクティブ | アクティブ | 1 |
| 0xB7A | アクティブ | アクティブ | 8 |

Fig. 12

40

【図１３】

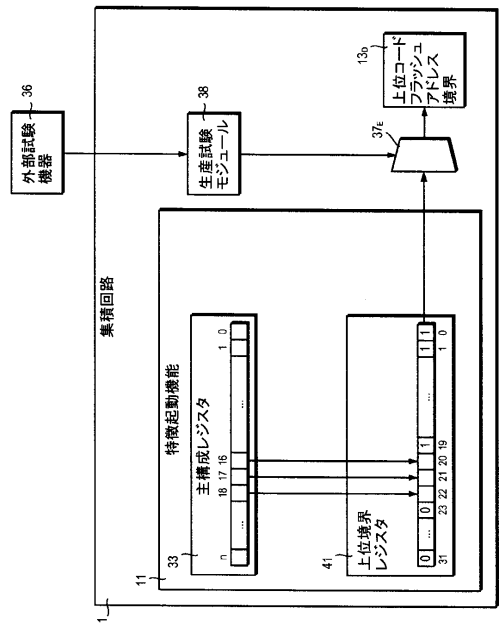


Fig. 13

【図１４】

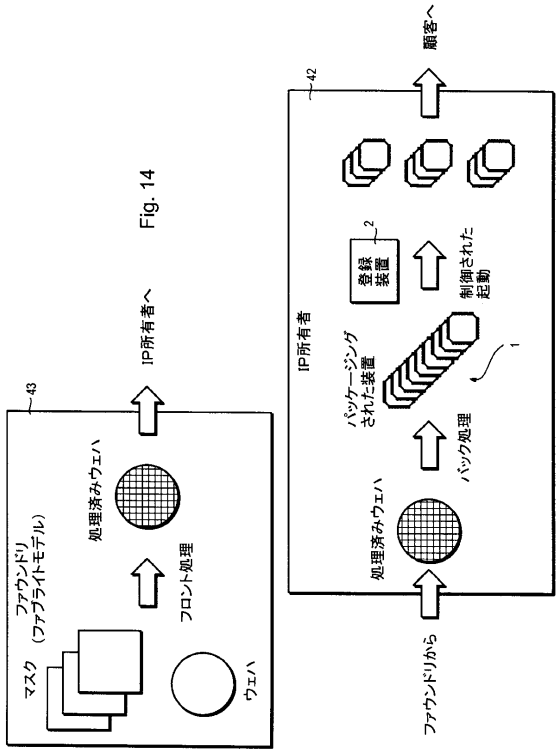


Fig. 14

【図１５】

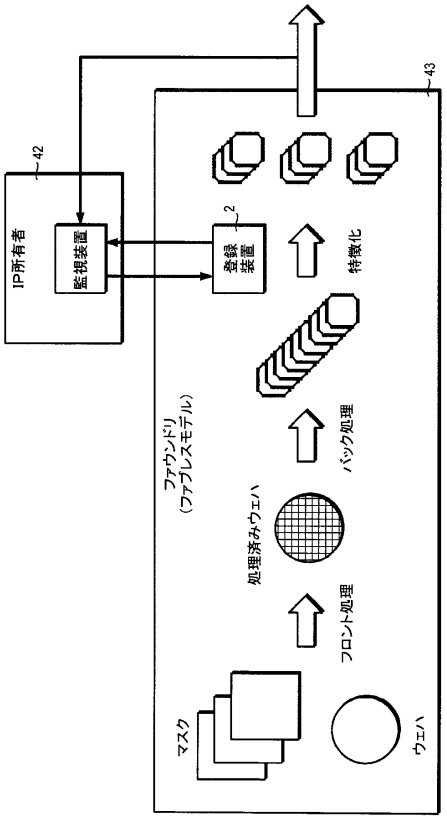
42
IP所有者
監視装置
2
登録装置
43
特徴化
バック処理
ファウンドリ
(ファブレスモデル)
処理済みウェハ
フロント処理
マスク
ウェハ

Fig. 15

フロントページの続き

(72)発明者　プラール，ファブリス
フランス、エフ－７８１４０　ベリジー、アブニュ・モラーヌ・ソルニエ、６、ルネサス・エレクトロニクス・ヨーロッパ・ゲゼルシャフト・ミット・ベシュレンクテル・ハフツング、シュキュルサル・フランセーズ内

審査官　岸野　徹

(56)参考文献　特開２００４－１４０３７６（ＪＰ，Ａ）
特開２０１３－００３４３１（ＪＰ，Ａ）
国際公開第２００８／１２５９９９（WO，Ａ１）
特表２００３－５２９８４８（ＪＰ，Ａ）
米国特許第０８４２７１９３（ＵＳ，Ｂ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／７３
Ｈ０１Ｌ　２１／８２２
Ｈ０１Ｌ　２７／０４
Ｈ０４Ｌ　９／１０
Ｈ０４Ｌ　９／３２