(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2022-119136
(P2022-119136A)

(43)公開日　令和4年8月16日(2022.8.16)

(51)Int.Cl.			F I			テーマコード(参考)
H04L	9/10	(2006.01)	H04L	9/00	621Z	
G09C	1/00	(2006.01)	G09C	1/00	650B	

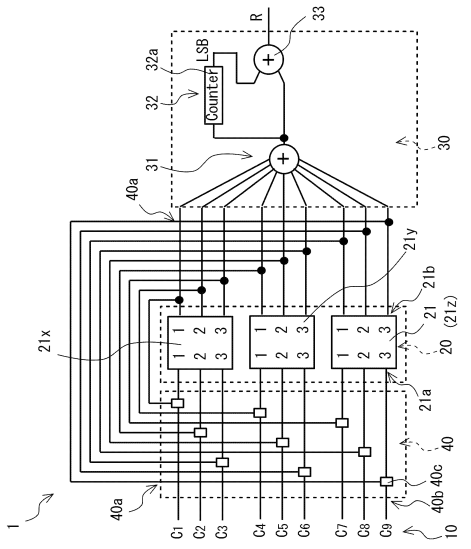
審査請求 未請求　請求項の数 10　ＯＬ　（全 26 頁）

(21)出願番号　特願2021-16161(P2021-16161)
(22)出願日　令和3年2月3日(2021.2.3)

(71)出願人　899000068
学校法人早稲田大学
東京都新宿区戸塚町１丁目１０４番地
(74)代理人　100215371
弁理士　古茂田　道夫
(72)発明者　篠原　尋史
東京都新宿区戸塚町１丁目１０４番地　学校法人早稲田大学内
(72)発明者　李　根
東京都新宿区戸塚町１丁目１０４番地　学校法人早稲田大学内
(72)発明者　劉　昆洋
東京都新宿区戸塚町１丁目１０４番地　学校法人早稲田大学内

(54)【発明の名称】チップ固有乱数発生装置

(57)【要約】
【課題】本発明は、低コスト化及び低消費電力化が可能であり、かつ機械学習攻撃に対する耐性が高いチップ固有乱数発生装置を提供することを目的とする。
【解決手段】本発明のチップ固有乱数発生装置は、集積回路チップに搭載されるチップ固有乱数発生装置であって、複数のチャレンジ入力端子と、上記チャレンジ入力端子の下流側に接続され、複数のルックアップテーブルが並列に配置されている第１ルックアップテーブル部と、上記第１ルックアップテーブル部の下流側に接続され、レスポンス出力を生成する出力部とを備え、上記ルックアップテーブルが、複数の入力端子及び複数の出力端子を有するとともに、チップ固有乱数を発生する複数のＰＵＦにより、上記入力端子に入力される信号を符号変換して上記出力端子に出力する。
【選択図】図1



【特許請求の範囲】
【請求項１】
集積回路チップに搭載されるチップ固有乱数発生装置であって、
複数のチャレンジ入力端子と、
上記チャレンジ入力端子の下流側に接続され、複数のルックアップテーブルが並列に配置されている第１ルックアップテーブル部と、
上記第１ルックアップテーブル部の下流側に接続され、レスポンス出力を生成する出力部と
を備え、
上記ルックアップテーブルが、複数の入力端子及び複数の出力端子を有するとともに、チップ固有乱数を発生する複数のＰＵＦにより、上記入力端子に入力される信号を符号変換して上記出力端子に出力するチップ固有乱数発生装置。
【請求項２】
上記第１ルックアップテーブル部及び上記出力部の間に接続され、複数の上記ルックアップテーブルがさらに並列に配置されている第２ルックアップテーブル部を備え、
上記第１ルックアップテーブル部の１のルックアップテーブルの複数の出力端子が、上記第２ルックアップテーブル部の複数のルックアップテーブルの入力端子に接続されている請求項１に記載のチップ固有乱数発生装置。
【請求項３】
上記チャレンジ入力端子と、上記第１ルックアップテーブル部との間に配置されるフィードバック部を備え、
上記フィードバック部が、上記出力部へ入力される第１信号と、上記チャレンジ入力端子から入力される第２信号との論理演算を行い、その結果を上記第１ルックアップテーブル部に入力する請求項１又は請求項２に記載のチップ固有乱数発生装置。
【請求項４】
上記フィードバック部が、上記第１信号のうち異なるルックアップテーブルに起因する論理演算結果を、上記第１ルックアップテーブル部の１のルックアップテーブルの入力端子に入力するよう構成されている請求項３に記載のチップ固有乱数発生装置。
【請求項５】
上記フィードバック部が、上記第１信号のうち１のルックアップテーブルに起因する論理演算結果を、上記第１ルックアップテーブル部の全てのルックアップテーブルの入力端子に入力するよう構成されている請求項３又は請求項４に記載のチップ固有乱数発生装置。
【請求項６】
上記フィードバック部への上記第１信号の入力及び上記第２信号の入力が、同期して更新される請求項３、請求項４又は請求項５に記載のチップ固有乱数発生装置。
【請求項７】
上記チャレンジ入力端子から上記出力部の出力に至る経路中に、現在の論理入力により決定される第１出力回路と、上記第１出力回路の過去の出力履歴により決定される第２出力回路と、上記第１出力回路及び上記第２出力回路の出力の論理演算を行う論理演算回路とを有し、
上記出力部のレスポンス出力が、上記論理演算回路の出力により決定される請求項１から請求項６のいずれか１項に記載のチップ固有乱数発生装置。
【請求項８】
少なくとも１つの上記ルックアップテーブルが、
上記ルックアップテーブルの入力端子と同数の入力端子及び上記ルックアップテーブルの出力端子より多数の出力端子を有するルックアップテーブル本体と、
上記ルックアップテーブル本体の出力から上記ルックアップテーブルの出力端子と同数の出力を生成する出力制御回路と
を有する請求項１から請求項７のいずれか１項に記載のチップ固有乱数発生装置。
【請求項９】

上記ＰＵＦが、ビットセルから構成されており、
上記ビットセルが、互いに逆極性のデータを保持可能なラッチ回路を有し、上記ラッチ回路が、第１ＣＭＯＳインバータと第２ＣＭＯＳインバータとを含み、
上記ビットセルが、上記第１ＣＭＯＳインバータ及び第２ＣＭＯＳインバータを構成するＭＯＳトランジスタの一部にホットエレクトロンの注入又はＢＴＩによる安定化回路を有する請求項１から請求項８のいずれか１項に記載のチップ固有乱数発生装置。
【請求項１０】
ＰＵＦが生成するチップ固有乱数を安定化する乱数安定化部を備え、
上記乱数安定化部が、不安定と検出されたＰＵＦが発生するチップ固有乱数をマスクする乱数マスク回路を有する請求項１から請求項９のいずれか１項に記載のチップ固有乱数発生装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、チップ固有乱数発生装置に関する。
【背景技術】
【０００２】
ＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）の進展とともにモノに対するセキュリティの課題が高まっている。例えば不揮発メモリにパスワードを書きこむ方法では読み取りや改ざんを容易に行うことができる。これに対し、ＰＵＦ（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ：物理複製困難関数）を用いた半導体チップの認証方法が注目されている。
【０００３】
ＰＵＦは半導体の製造バラつき等を利用して、チップ固有の論理値を出力する。ＰＵＦを用いた回路としては、例えば図１０に示すアービターＰＵＦ１００が公知である（例えば特開２０２０－１８３４５号公報参照）。アービターＰＵＦ１００では、２本の多段遅延回路１０１がｎ段の直列接続された経路を構成し、各ステージについて２本の多段遅延回路１０１を、入力C_i（C_1、C_2、・・・、Ｃｎ）により選択回路１０２で切替えた２つの経路を用意する。この２つの経路のうち、例えばどちらが先着するかをアービター１０３が判定し、アービターＰＵＦ１００の出力（レスポンス）が決まる。
【０００４】
アービターＰＵＦ１００では、２本の多段遅延回路１０１は、設計値上は等しい遅延値を持つように設計される。しかし、実際に製造されると製造ばらつきにより２本の多段遅延回路１０１は異なる遅延値を有することとなる。例えばＤｅｌａｙ１ＡとＤｅｌａｙ１Ｂとのいずれが遅くなるかは半導体チップごとに異なり、かつ制御することはできない。そこで、半導体チップの製造後に、この半導体チップに入力C_i（チャレンジ入力）を与えたときのレスポンス出力Ｒを予め多数取得し、例えばこの半導体チップを使用するサーバに、この半導体チップの固有の論理値として（例えば半導体チップの製造番号と紐付して）格納しておく。上記サーバは、この半導体チップにチャレンジ入力C_iを送信すると、どのようなレスポンス出力Ｒが返信されてくるか、予め分かっているので、例えば認証のための暗号化キーが通信されることはなく、秘匿性が高められる。
【０００５】
しかし、アービターＰＵＦ１００の２つの経路の総遅延時間は、各ステージの遅延の線形和となるため、数百程度のＣＲＰ（Ｃｈａｌｌｅｎｇｅ　Ｒｅｓｐｏｎｓｅ　Ｐａｉｒ：チャレンジとレスポンスとの組）の機械学習で出力が予測できるという機械学習攻撃に対する脆弱性がある。
【０００６】
この脆弱性を解消する方法として、例えば１つのチャレンジ入力ごとに１つのＰＵＦを準備する方法が考えられる。この手法では、各チャレンジ入力に対して独立にレスポンスが変化し得るため、上述のサーバにはチャレンジ入力ごとにレスポンス出力が格納されて使

用される（例えば特開２０１９－１２１８８５号公報参照）。
【０００７】
しかし、このような構成にあってはＰＵＦの数が非常に多くなるため、集積回路チップの低コスト化や低消費電力化に不利である。
【先行技術文献】
【特許文献】
【０００８】
【特許文献１】特開２０２０－１８８３４５号公報
【特許文献２】特開２０１９－１２１８８５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００９】
本発明は、以上のような事情に基づいてなされたものであり、低コスト化及び低消費電力化が可能であり、かつ機械学習攻撃に対する耐性が高いチップ固有乱数発生装置を提供することを目的とする。
【課題を解決するための手段】
【００１０】
本発明の一態様に係るチップ固有乱数発生装置は、集積回路チップに搭載されるチップ固有乱数発生装置であって、複数のチャレンジ入力端子と、上記チャレンジ入力端子の下流側に接続され、複数のルックアップテーブルが並列に配置されている第１ルックアップテーブル部と、上記第１ルックアップテーブル部の下流側に接続され、レスポンス出力を生成する出力部とを備え、上記ルックアップテーブルが、複数の入力端子及び複数の出力端子を有するとともに、チップ固有乱数を発生する複数のＰＵＦにより、上記入力端子に入力される信号を符号変換して上記出力端子に出力する。
【００１１】
当該チップ固有乱数発生装置は、複数のチャレンジ入力端子の下流側に、複数のルックアップテーブルが並列に配されている。個々のルックアップテーブルは、複数のＰＵＦにより、上記入力端子に入力される信号を符号変換するので、出力の不規則性が高く、有限のＣＲＰからその出力を機械学習により予測することが困難である。従って、当該チップ固有乱数発生装置は、機械学習攻撃に対する耐性が高い。また、複数のチャレンジ入力端子に対して分割してルックアップテーブルを設けるので、ルックアップテーブル全体の規模が比較的小さく、集積回路チップの低コスト化と低消費電力化とに有利である。
【００１２】
上記第１ルックアップテーブル部及び上記出力部の間に接続され、複数の上記ルックアップテーブルがさらに並列に配置されている第２ルックアップテーブル部を備え、上記第１ルックアップテーブル部の１のルックアップテーブルの複数の出力端子が、上記第２ルックアップテーブル部の複数のルックアップテーブルの入力端子に接続されているとよい。このように第２ルックアップテーブル部を備え、上記第１ルックアップテーブル部の１のルックアップテーブルの複数の出力端子を上記第２ルックアップテーブル部の複数のルックアップテーブルの入力端子に接続することで、有限のＣＲＰからその出力を機械学習により予測することをさらに困難なものとすることができる。従って、機械学習攻撃に対する耐性をさらに高めることができる。
【００１３】
上記チャレンジ入力端子と、上記第１ルックアップテーブル部との間に配置されるフィードバック部を備え、上記フィードバック部が、上記出力部へ入力される第１信号と、上記チャレンジ入力端子から入力される第２信号との論理演算を行い、その結果を上記第１ルックアップテーブル部に入力するとよい。このようにフィードバック部を設けることで、ルックアップテーブルの入出力端子数や個数を増やすことなくチャレンジ入力数やレスポンス数を増やしたり、機械学習攻撃に対する耐性をさらに高めたりすることができる。
【００１４】

上記フィードバック部が、上記第１信号のうち異なるルックアップテーブルに起因する論理演算結果を、上記第１ルックアップテーブル部の１のルックアップテーブルの入力端子に入力するよう構成されているとよい。このように上記第１信号のうち異なるルックアップテーブルに起因する論理演算結果を、上記第１ルックアップテーブル部の１のルックアップテーブルの入力端子に入力することで、有限のＣＲＰからその出力を機械学習により予測することをさらに困難なものとすることができる。従って、機械学習攻撃に対する耐性をさらに高めることができる。

【００１５】

上記フィードバック部が、上記第１信号のうち１のルックアップテーブルに起因する論理演算結果を、上記第１ルックアップテーブル部の全てのルックアップテーブルの入力端子に入力するよう構成されているとよい。このように上記第１信号のうち１のルックアップテーブルに起因する論理演算結果を、上記第１ルックアップテーブル部の全てのルックアップテーブルの入力端子に入力することで、有限のＣＲＰからその出力を機械学習により予測することをさらに困難なものとすることができる。従って、機械学習攻撃に対する耐性をさらに高めることができる。

【００１６】

上記フィードバック部への上記第１信号の入力及び上記第２信号の入力が、同期して更新されるとよい。このように上記フィードバック部への上記第１信号の入力及び上記第２信号の入力を同期して更新することで、当該チップ固有乱数発生装置の出力が不安定となることを抑止ができる。

【００１７】

上記チャレンジ入力端子から上記出力部の出力に至る経路中に、上記チャレンジ入力端子から上記出力端子に至る経路中に、現在の論理入力により決定される第１出力回路と、上記第１出力回路の過去の出力履歴により決定される第２出力回路と、上記第１出力回路及び上記第２出力回路の出力の論理演算を行う論理演算回路とを有し、上記出力部のレスポンス出力が、上記論理演算回路の出力により決定されるとよい。このように現在の論理入力により決定される第１出力と、上記第１出力の過去の履歴により決定される第２出力との論理演算により上記出力部のレスポンス出力が決定されるように構成することで、ルックアップテーブルの入出力端子数や個数を増やすことなく、機械学習攻撃に対する耐性をさらに高めることができる。

【００１８】

少なくとも１つの上記ルックアップテーブルが、上記ルックアップテーブルの入力端子と同数の入力端子及び上記ルックアップテーブルの出力端子より多数の出力端子を有するルックアップテーブル本体と、上記ルックアップテーブル本体の出力から上記ルックアップテーブルの出力端子と同数の出力を生成する出力制御回路とを有するとよい。ＰＵＦにより決まる出力は、製造バラつき等を利用しているため、例えば電源投入ごとに出力が異なりレスポンス出力が不安定となるといった場合が生じ得る。これに対し、上記ルックアップテーブルの入力端子と同数の入力端子及び上記ルックアップテーブルの出力端子より多数の出力端子を有するルックアップテーブル本体を有することで、ルックアップテーブルに冗長な出力を設け、出力制御回路により、これらの出力から安定度の高い出力を選択的に利用し、レスポンス出力を安定化させることができる。また、上述の構成により、上記ルックアップテーブル本体の多数の出力の論理演算で上記ルックアップテーブルの出力を生成することを可能とし、機械学習攻撃に対する耐性をさらに高めることができる。

【００１９】

上記ＰＵＦが、ビットセルから構成されており、上記ビットセルが、互いに逆極性のデータを保持可能なラッチ回路を有し、上記ラッチ回路が、第１ＣＭＯＳインバータと第２ＣＭＯＳインバータとを含み、上記ビットセルが、上記第１ＣＭＯＳインバータ及び第２ＣＭＯＳインバータを構成するＭＯＳトランジスタの一部にホットエレクトロンの注入又はＢＴＩによる安定化回路を有するとよい。このようにＰＵＦをいわゆるＳＲＡＭのビットセルで構成し、ホットエレクトロンの注入又はＢＴＩによる安定化回路を有することで、

レスポンス出力を安定化させることができる。
【００２０】
ＰＵＦが生成するチップ固有乱数を安定化する乱数安定化部を備え、上記乱数安定化部が、不安定と検出されたＰＵＦが発生するチップ固有乱数をマスクする乱数マスク回路を有するとよい。このように不安定と検出されたＰＵＦが発生するチップ固有乱数をマスクする構成を有することで、レスポンス出力を安定化させることができる。
【発明の効果】
【００２１】
本発明のチップ固有乱数発生装置は、低コスト化及び低消費電力化が可能であり、かつ機械学習攻撃に対する耐性が高い。
【図面の簡単な説明】
【００２２】
【図１】図１は、本発明の一実施形態に係るチップ固有乱数発生装置を示す模式的構成図である。
【図２】図２は、図１のルックアップテーブルの構成の一実施形態を示す模式的構成図である。
【図３】図３は、図２のビットセルの構成の一実施形態を示す模式的構成図である。
【図４】図４は、図３のビットセルの構成とは異なる実施形態のビットセルの構成を示す模式的構成図である。
【図５】図５は、図２とは異なるルックアップテーブルの構成の実施形態を示す模式的構成図である。
【図６】図６は、図５のビットセルの構成の一実施形態を示す模式的構成図である。
【図７】図７は、図２及び図５とは異なるルックアップテーブルの構成の実施形態を示す模式的構成図である。
【図８】図８は、図１とは異なるフィードバック部の構成の実施形態を示す模式的構成図である。
【図９】図９は、図１とは異なる実施形態に係るチップ固有乱数発生装置を示す模式的構成図である。
【図１０】図１０は、従来のチップ固有乱数発生装置を示す模式的構成図である。
【発明を実施するための形態】
【００２３】
［第１実施形態］
以下、本発明の第１の実施形態に係るチップ固有乱数発生装置について、適宜図面を参照しつつ説明する。
【００２４】
図１に示すチップ固有乱数発生装置１は、集積回路チップに搭載されるチップ固有乱数発生装置である。上記集積回路チップは、典型的には半導体チップであるが、ＰＵＦを搭載可能であれば、半導体チップに限定されるものではない。
【００２５】
当該チップ固有乱数発生装置１は、複数のチャレンジ入力端子１０と、チャレンジ入力端子１０の下流側に接続される第１ルックアップテーブル部２０と、第１ルックアップテーブル部２０の下流側に接続される出力部３０と、チャレンジ入力端子１０と第１ルックアップテーブル部２０との間に配置されるフィードバック部４０とを備える。
【００２６】
＜チャレンジ入力端子＞
チャレンジ入力端子１０は、集積回路チップ外部から送信されてくるチャレンジ入力C_iを当該チップ固有乱数発生装置１へ入力するための端子である。
【００２７】
チャレンジ入力端子１０の端子数（チャレンジ入力Ｃｉのビット幅）の下限としては、９が好ましく、１６がより好ましく、２０がさらに好ましい。一方、チャレンジ入力端子１

０の端子数の上限としては、２５６が好ましく、１２８がより好ましく、４９がさらに好ましく、２５が特に好ましい。チャレンジ入力端子１０の端子数が上記下限未満であると、機械学習攻撃に対する耐性が低下するおそれがある。逆に、チャレンジ入力端子１０の端子数が上記上限を超えると、例えば当該チップ固有乱数発生装置１を利用するサーバ上に当該チップ固有乱数発生装置１をモデル化するために必要となる記憶領域が大きくなり過ぎるおそれがある。なお、チャレンジ入力端子１０の端子数が多いほど機械学習攻撃に対する耐性は高まる傾向にあるが、当該チップ固有乱数発生装置１は、チャレンジ入力端子１０の端子数が上記上限以下であっても、チャレンジ入力端子１０の端子数が１００程度である従来のチップ固有乱数発生装置と同等の機械学習攻撃に対する耐性を得ることが可能である。

【００２８】

チャレンジ入力端子１０の端子数は、後述するルックアップテーブル２１への分割のし易さから、n^2（ｎ：２以上の自然数）であるとよい。つまり、チャレンジ入力端子１０の端子数は、９、１６、２５又は３６とすることが特に好ましい。以下、チャレンジ入力端子１０の端子数が９である場合を例にとり説明するが、当該チップ固有乱数発生装置１のチャレンジ入力端子１０の端子数が９に限定されることを意味するものではない。

【００２９】

＜第１ルックアップテーブル部＞

第１ルックアップテーブル部２０には、複数のルックアップテーブル２１が並列に配置されている。ルックアップテーブル２１は、複数の入力端子２１ａ及び複数の出力端子２１ｂを有する。

【００３０】

複数のルックアップテーブル２１の入力端子２１ａの端子数の合計は、チャレンジ入力端子１０の端子数と等しい。また、各チャレンジ入力端子１０は、いずれかのルックアップテーブル２１の入力端子２１ａと１対１で接続されている。また、入力端子２１ａの端子数は、各ルックアップテーブル２１間で等しいことが好ましく、さらにルックアップテーブル２１の数と等しいことがさらに好ましい。当該チップ固有乱数発生装置１では、このように複数のチャレンジ入力端子１０に対して分割してルックアップテーブル２１を設けるので、ルックアップテーブル２１全体の規模が比較的小さい。このため、ルックアップテーブル２１のデータをすべて記憶して当該チップ固有乱数発生装置１をモデル化することもできる。つまり、半導体チップ側に十分に多数のＣＲＰが用意されている場合であっても、その全てを利用することができる。

【００３１】

ルックアップテーブル２１の出力端子２１ｂの端子数は、入力端子２１ａと同数である必要はないが、ハードウェアの利用効率と機械学習攻撃に対する耐性との観点から、入力端子２１ａと同数であることが好ましい。

【００３２】

つまり、チャレンジ入力端子１０の端子数が９である場合、第１ルックアップテーブル部２０は、３つの入力端子２１ａ及び３つの出力端子２１ｂを有する３つのルックアップテーブル２１を有することが好ましい。以下、この構成を前提に説明するが、複数のルックアップテーブル２１の構成は、これに限定されるものではない。

【００３３】

ルックアップテーブル２１は、チップ固有乱数を発生する複数のＰＵＦにより、入力端子２１ａに入力される信号を符号変換して出力端子２１ｂに出力する。当該チップ固有乱数発生装置１では、図２に示すように、ＰＵＦがＳＲＡＭのビットセル２１ｃから構成されている。ビットセル２１ｃは、電源投入時に、又はＰＵＦデータ出現動作時に、そのビットセル２１ｃを構成するトランジスタのばらつきにより０又は１の論理値を保持する。このため、ビットセル２１ｃが保持する論理値は、予測不可能なチップ固有の値となる。

【００３４】

ビットセル２１ｃの個数は、ルックアップテーブル２１の入力端子２１ａの端子数をｋ及

び出力端子数２１ｂの端子数をｍとするとき、ｍ×2^{k}個とするとよい。ビットセル２１ｃの個数を2^{m}個とすることで、全ての入力及び出力に対して、独立してチップ固有乱数を発生することができる。３つの入力端子２１ａ及び３つの出力端子２１ｂを有するルックアップテーブル２１では、図２に示すように、ビットセル２１ｃの個数は、２４（＝３×2^{3}）であることが好ましい。

【００３５】

また、ルックアップテーブル２１は、ローデコーダ２１ｄと、カラムデコーダ２１ｅと、センスアンプ２１ｆとを有する。入力端子２１ａは３入力であり、図２では、A_0、A_1、A_2で示されている。また、出力端子２１ｂは３出力であり、図２では、DQ_0、DQ_1、DQ_2で示されている。２４個のビットセル２１ｃは、４列２行の８個のビットセル２１ｃが、出力端子２１ｂの３出力それぞれに対応して３群設けられている。A_0、A_1、A_2のうち、A_0及びA_1の２入力がローデコーダ２１ｄに入力され、WL_0～WL_3のいずれかのワードラインが選択される。これにより４列の中から１列が選択される。また、A_2の１入力がカラムデコーダ２１ｅに入力され、BL_0又はBL_1のいずれかのビットラインが選択される。これらの組み合わせにより各出力に対して１つのビットセル２１ｃが選択される。選択されたビットセル２１ｃの記憶する論理値（０又は１）は、センスアンプ２１ｆにより読みだされ、対応する出力DQ_i（ｉ＝０、１、２）へ出力される。なお、ＣＳＢはチップセレクト信号（Ｂは信号がローアクティブであることを意味している）であり、ＣＳＢが０である場合にビットセル２１ｃの論理の読み出しが行われる。これらは公知のＳＲＡＭの構成である。

【００３６】

（ホットエレクトロンの注入によるビットセルの安定化）

ビットセル２１ｃとして、例えば公知の６トランジスタ型のセルを用いてもよいが、図３に示すように、ビットセル２１ｃが、互いに逆極性のデータを保持可能なラッチ回路５０を有し、ラッチ回路５０が、第１ＣＭＯＳインバータ５１と第２ＣＭＯＳインバータ５２とを含み、ビットセル２１ｃが、第１ＣＭＯＳインバータ５１及び第２ＣＭＯＳインバータ５２を構成するＭＯＳトランジスタの一部にホットエレクトロンの注入による安定化回路５３を有する構成としてもよい。

【００３７】

具体的には、安定化回路５３は、第１ＣＭＯＳインバータ５１を構成するＰＭＯＳ５１ａと並列に接続される第１ＰＭＯＳ５３ａと、第２ＣＭＯＳインバータ５２を構成するＰＭＯＳ５２ａと並列に接続される第２ＰＭＯＳ５３ｂとを有する。第１ＰＭＯＳ５３ａ及び第２ＰＭＯＳ５３ｂのゲート電位は共通信号V_{PG}により制御されている。

【００３８】

安定化回路５３は、通常の動作時は共通信号V_{PG}を電源電位として、第１ＰＭＯＳ５３ａ及び第２ＰＭＯＳ５３ｂをオフ状態で使用する。一方、当該チップ固有乱数発生装置１が搭載されている集積回路チップの出荷前のテスト時又はバーンイン試験時には共通信号V_{PG}を接地電位とし、第１ＰＭＯＳ５３ａ及び第２ＰＭＯＳ５３ｂをオン状態で行う。仮にビットセル２１ｃが、その製造ばらつきにより第１ＣＭＯＳインバータ５１の電位V_Aが電源電位、第２ＣＭＯＳインバータ５２の電位V_Bが接地電位となる傾向にあるとする。この状態において、第１ＰＭＯＳ５３ａ及び第２ＰＭＯＳ５３ｂをオン状態とすると、第１ＣＭＯＳインバータ５１を構成するＮＭＯＳ５１ｂが飽和領域で動作することとなり、ホットエレクトロンが注入される。ホットエレクトロンが注入されると、第１ＣＭＯＳインバータ５１を構成するＮＭＯＳ５１ｂの閾値電圧が増大し、このＮＭＯＳ５１ｂがオン状態となり難くなるから、第１ＣＭＯＳインバータ５１の電位V_Aは、電源電位でさらに安定する。つまり、ビットセル２１ｃの出力が安定する。逆に、第１ＣＭＯＳインバータ５１の電位V_Aが接地電位、第２ＣＭＯＳインバータ５２の電位V_Bが電源電位となる場合は、同様の理由で第２ＣＭＯＳインバータ５２を構成するＮＭＯＳ５２ｂの閾値電圧が増大し、第２ＣＭＯＳインバータ５２の電位V_Bは、電源電位でさらに安定する。

【００３９】

このように安定化回路５３が第１ＣＭＯＳインバータ５１及び第２ＣＭＯＳインバータ５２を構成するＭＯＳトランジスタの一部にホットエレクトロンを注入することで、第１ＣＭＯＳインバータ５１と第２ＣＭＯＳインバータ５２との間の製造バラつきの差を増大させることができる。ビットセル２１ｃが保持する論理値は、上述のように、第１ＣＭＯＳインバータ５１と第２ＣＭＯＳインバータ５２との製造バラつきにより決まる。第１ＣＭＯＳインバータ５１と第２ＣＭＯＳインバータ５２との間の製造バラつきの差が小さい場合、例えば周囲の温度や電圧といったような環境の変化等で保持する論理値が変わってしまうという不安定な現象（ビットエラー）が生じ得る。ビットエラーが生じると、ＣＲＰで不一致が生じるから、さらにＣＲＰを追加した再判定や予め不安定なチャレンジ入力Ｃｉを記憶してそれを使用しない等の処置を行う必要が生じ、ＣＲＰの損失が生じる。従って、この安定化回路５３によりレスポンス出力Ｒを安定化させ、ビットエラー率を低減することができる。つまり、ＣＲＰ損失を低減させ、効率的な認証を行うことができるようになるので、サーバ側の負担も低減できる。

【００４０】

なお、ビットセル２１ｃは、図３に示すように、第１ＣＭＯＳインバータ５１の出力とビットラインＢＬとの間及び第２ＣＭＯＳインバータ５２の出力とビットラインの反転ＢＬＢとの間にそれぞれ設けられ、ワードラインＷＬによりゲート電位が制御されているパストランジスタ５４を有する。このパストランジスタ５４によりワードラインＷＬで選択された列に属するビットセル２１ｃが保持する論理値がBL_0又はBL_1のいずれかのビットラインに出力される状態となる。公知の６トランジスタ型のビットセルは、第１ＣＭＯＳインバータ５１（２トランジスタ）、第２ＣＭＯＳインバータ５２（２トランジスタ）及び２つのパストランジスタ５４により構成される。

【００４１】

安定化回路５３の構成は、図３に示す構成に限定されるものではなく、例えば図４に示すように、安定化回路５５として、第１ＣＭＯＳインバータ５１を構成するＰＭＯＳ５１ａと並列に接続される第１ＮＭＯＳ５５ａと、第２ＣＭＯＳインバータ５２を構成するＰＭＯＳ５２ａと並列に接続される第２ＮＭＯＳ５５ｂとを有する構成を採用することもできる。この安定化回路５５では、予めＰＵＦが記憶している値を反転させる。その後、V_{ND}を接地電位とし、V_{NG}を第１ＮＭＯＳ５５ａ及び第２ＮＭＯＳ５５ｂの閾値電圧又はそれより若干高い程度の電圧（例えば１．０Ｖ）とする。この状態でV_Pに高電圧（例えば３．３Ｖ）を印加する。そうすると、論理が１であるＣＭＯＳインバータを構成するＮＭＯＳに飽和電流が流れ、ホットキャリアが注入される。なお、ＰＵＦが記憶している値を反転させる方法としては、例えば後述するＢＴＩによるビットセルの安定化で用いられる図５の構成を採用することができる。

【００４２】

（ＢＴＩによるビットセルの安定化）

また、ビットセルの動作を安定化させる手段として、ＢＴＩ（Ｂｉａｓ　Ｔｅｍｐｅｒａｔｕｒｅ　Ｉｎｓｔａｂｉｌｉｔｙ）を用いることもできる。図５にビットセル２１ｇがＢＴＩによる安定化回路５６を有する場合のルックアップテーブル２２の構成例を示す。ＢＴＩを用いる場合、図５に示すように、例えば同一の列に属する８個のビットセル２１ｇで安定化回路５６を共有することができる。この場合、個々のビットセル２１ｇは、例えば公知の６トランジスタ型のセル（図６参照）を用いることができる。なお、図５に示すルックアップテーブル２２において、ビットセル２１ｇ及び安定化回路５６以外の構成要素は、図２に示すルックアップテーブル２１と同様である。また、図６に示すビットセル２１ｇの構成要素は、図３に示すビットセル２１ｃと同様である。このため、これらの詳細説明を省略する。

【００４３】

ＢＴＩによる安定化回路５６は、センスアンプ２１ｆにより読みだされたビットセル２１ｇの論理値を反転させる書込用ＣＭＯＳインバータ５６ａと、書込用ＣＭＯＳインバータ５６ａの出力論理値を、読みだしたビットセル２１ｇに書き込む書込用ドライバ５６ｂと

を有する。
【００４４】
以下、動作原理について、仮にビットセル２１ｇが、その製造ばらつきにより第１ＣＭＯＳインバータ５１の電位V_Aが電源電位、第２ＣＭＯＳインバータ５２の電位V_Bが接地電位となる傾向にあるとして説明する。なお、逆の電位で安定する傾向にある場合についても、同様である。
【００４５】
第１ＣＭＯＳインバータ５１の電位V_Aが電源電位であるから、第１ＣＭＯＳインバータ５１のＰＭＯＳ５１ａがオン状態にあり、第２ＣＭＯＳインバータ５２の電位V_Bが接地電位であるから、第２ＣＭＯＳインバータ５２のＮＭＯＳ５２ｂがオン状態にある。ここで、安定化回路５６を動作させる、すなわち入力ＷＥＢをアクティブとすると、反転論理を書き込むから、逆に第１ＣＭＯＳインバータ５１のＮＭＯＳ５１ｂがオン状態となり、第２ＣＭＯＳインバータ５２のＰＭＯＳ５２ｂもオン状態となる。ＢＴＩは、オン状態のトランジスタに作用するので、第１ＣＭＯＳインバータ５１のＮＭＯＳ５１ｂ及び第２ＣＭＯＳインバータ５２のＰＭＯＳ５２ｂの閾値電圧が上昇する。この結果、第１ＣＭＯＳインバータ５１の電位V_Aが電源電位で、第２ＣＭＯＳインバータ５２の電位V_Bは接地電位で、より安定する。このＢＴＩによるビットセル２１ｇの安定化は、ホットエレクトロンの注入によるビットセル２１ｃの安定化と同様に、当該チップ固有乱数発生装置１が搭載されている集積回路チップの出荷前のテスト時又はバーンイン試験時に行うことができる。
【００４６】
安定化回路５６の構成は、図５に示す構成に限定されるものではなく、例えば書込用ＣＭＯＳインバータ５６ａを省略して、集積回路チップの外部からビットセル２１ｇの論理値を読み出し、その反転論理を書込用ドライバ５６ｂにより書き込んでもよい。
【００４７】
このようにＢＴＩを用いても、安定化回路５６によりレスポンス出力Ｒを安定化させ、ビットエラー率を低減することができる。つまり、ＣＲＰ損失を低減させ、効率的な認証を行うことができるようになるので、サーバ側の負担も低減できる。
【００４８】
（出力制御回路によるビットセルの安定化）
図７に示すルックアップテーブル２３のように、ルックアップテーブル本体２３ａと、出力制御回路２３ｂとを有する構成を用いて、ビットセル２１ｃの動作を安定化させることもできる。
【００４９】
ルックアップテーブル本体２３ａは、ルックアップテーブル２３の入力端子２３ｃと同数の入力端子及びルックアップテーブル２３の出力端子２３ｄより多数の出力端子を有する。当該チップ固有乱数発生装置１では、ルックアップテーブル２３の入力端子２３ｃ及び出力端子２３ｄがともに３端子である場合を想定しているので、ルックアップテーブル本体２３ａの入力端子数は３である。一方、ルックアップテーブル本体２３ａの出力端子数は４以上となる。以降、ルックアップテーブル本体２３ａの出力端子数が４である場合を例にとり説明するが、ルックアップテーブル本体２３ａの出力端子数は４に限定されるものではない。
【００５０】
ルックアップテーブル本体２３ａは、出力端子数が４となる以外は、例えば図２に示すルックアップテーブル２１と同様に構成することができる。ルックアップテーブル本体２３ａは、図２に示すルックアップテーブル２１より出力端子数が１つ多いので、１カラム分（図２の破線部分）が並列に追加されることとなる。上述の点を除き構成が同様であるので、詳細説明を省略する。
【００５１】
出力制御回路２３ｂは、ルックアップテーブル本体２３ａの出力からルックアップテーブ

ル２３の出力端子２３ｄと同数の出力を生成する。
【００５２】
図７に出力制御回路２３ｂの構成例を示している。この出力制御回路２３ｂでは、出力端子２３ｄの各出力DQ_i（ｉ＝０、１、２）は、CN_i、CR_iにより制御されている。ルックアップテーブル本体２３ａの４つの出力をDO_j（ｊ＝０～３）として、出力DQ_0を例にとり、さらに詳説すると、（CN_0、CR_0）＝（０、０）である場合、出力DQ_0は０でマスクされる。
【００５３】
（CN_0、CR_0）＝（１、０）又は（０、１）である場合は、それぞれDO_0、DO_3が選択される。例えばDO_0を出力する場合が通常の状態であるとすると、通常の状態では不安定な出力を示す現象が認められる場合、これをDO_3に差し替えることで安定性を向上させることができる。ＰＵＦにより決まる出力は、上述のように製造バラつき等を利用しているため、例えば電源投入ごとに出力が異なりレスポンス出力が不安定となるといった場合が生じ得る。これに対し、ルックアップテーブル２３の入力端子２３ｃと同数の入力端子及びルックアップテーブル２３の出力端子２３ｄより多数の出力端子を有するルックアップテーブル本体２３ａを有することで、ルックアップテーブル２３に冗長な出力を設け、出力制御回路２３ｂにより、これらの出力から安定度の高い出力を選択的に利用し、レスポンス出力を安定化させることができる。
【００５４】
また、（CN_0、CR_0）＝（１、１）とすると、ルックアップテーブル本体２３ａの出力を論理演算した結果（ここではDO_0とDO_3との排他的論理和）をルックアップテーブル２３の出力端子２３ｄ（ここではDQ_0）に出力する。このようにルックアップテーブル本体２３ａの出力の論理演算結果を出力することで、機械学習攻撃に対する耐性を高めることができる。
【００５５】
さらに、例えば（CN_0、CR_0）＝（１、０）、（０、１）、（１、１）を動的に、あるいは周期的に切り替えてもよい。これにより、あたかも異なるＰＵＦを有するルックアップテーブルのように振る舞わせることができるので、機械学習攻撃で構築しなければならないモデルが複雑になる。また、フィードバックを繰り返すうちに以前と同一のルックアップテーブル入力値が偶然出現した場合等に発生する周期性による乱数性の低下を抑止することができる。従って、機械学習攻撃に対する耐性を高めることができる。
【００５６】
（その他）
ＰＵＦが生成するチップ固有乱数を安定化する乱数安定化部を備え、上記乱数安定化部が、不安定と検出されたＰＵＦが発生するチップ固有乱数をマスクする乱数マスク回路を有してもよい。
【００５７】
ルックアップテーブル２１内で不安定な出力を示すビットセル２１ｃが検出されている場合において、ルックアップテーブル２１の入力端子２１ａに、このビットセル２１ｃを選択する入力が入力された場合、このビットセル２１ｃの出力をその論地値にかかわらず論理値０又は１に固定する。このように不安定と検出されたＰＵＦが発生するチップ固有乱数をマスクする構成を有することで、レスポンス出力Ｒを安定化させることができる。
【００５８】
具体的構成として、例えばルックアップテーブル２１の各ビットセル２１ｃに対応したシャドーメモリ（不揮発性メモリ）を用意し、不安定であることが検出されたビットセル２１ｃのメモリ値を０、他のビットセル２１ｃのメモリ値を１とする。各ビットセル２１ｃの選択とともに、上記シャドーメモリの該当するメモリ値も選択し、両者の論理積（ＡＮＤ）をルックアップテーブル２１の出力とする。このように構成することで、不安定なビットセル２１ｃの出力を０に固定することができる。
【００５９】

不安定なビットセル２１ｃの検出は、例えば当該チップ固有乱数発生装置１が搭載されている集積回路チップの出荷前に、温度や電源電圧条件を変えてテストを行い不安定性を判定してもよいし、安定性検出回路を搭載して、ＣＲＰの不一致から例えばＡＩ等を利用して検出してもよい。

【００６０】

以上、ビットセル２１ｃの安定化を図る手段についていくつか述べたが、２以上の手段を同一のルックアップテーブル２１に対して同時に使用してもよい。また、異なるルックアップテーブル２１に対して異なる手段を実装することを妨げない。

【００６１】

＜出力部＞

出力部３０は、図１に示すようにレスポンス出力Ｒを生成する。出力部３０は、出力部３０への現在の論理入力により決定される第１レスポンス出力回路３１と、第１レスポンス出力回路３１の過去の出力履歴により決定される第２レスポンス出力回路３２と、第１レスポンス出力回路３１及び第２レスポンス出力回路３２の出力の論理演算を行う論理演算回路３３とを有する。出力部３０のレスポンス出力Ｒは、論理演算回路３３の出力により決定される。つまり、当該チップ固有乱数発生装置１は、チャレンジ入力端子１０から出力部３０の出力に至る経路中に、現在の論理入力により決定される第１出力回路（第１レスポンス出力回路３１）と、上記第１出力回路の過去の出力履歴により決定される第２出力回路（第２レスポンス出力回路３２）と、上記第１出力回路及び上記第２出力回路の出力の論理演算を行う論理演算回路３３とを有している。

【００６２】

第１レスポンス出力回路３１は、組み合わせ論理により実現されている。第１レスポンス出力回路３１の組み合わせ論理は、任意に設定できるが、例えば図１に示すように第１ルックアップテーブル部２０の出力端子２１ｂの全ビットについて排他的論理和を演算する論理回路とすることができる。排他的論理和は、ランダムな入力に対して０と１とを出力する確率が等しいので、機械学習攻撃に対する耐性を高め易い。

【００６３】

第２レスポンス出力回路３２の出力は、第１レスポンス出力回路３１の出力のみでは決定されず、この第１レスポンス出力回路３１の過去の履歴に依存する。図７では、第２レスポンス出力回路３２として、第１レスポンス出力回路３１の出力の１（又は０）の数を数えるカウンタ回路を用い、その最下位ビット（ＬＳＢ）を出力としている。つまり、第１レスポンス出力回路３１の出力が１（又は０）となるたびに第２レスポンス出力回路３２の出力は反転し、第１レスポンス出力回路３１の出力が１（又は０）であっても第２レスポンス出力回路３２の出力は０にも１にもなり得る。

【００６４】

なお、第２レスポンス出力回路３２は、第１レスポンス出力回路３１の過去の出力履歴により決定される論理回路であれば、カウンタ回路に限定されるものではなく、例えばシフトレジスタ回路等を用いてもよい。例えば最上位ビットから入力されるシフトレジスタ回路を用いる場合、例えば最下位ビットを用いてもよいし、下位２ビットの排他的論理和を用いてもよい。また、第２レスポンス出力回路３２として、新たな一連のＣＲＰ生成動作の都度、履歴をリセットする構成又は履歴をリセットしない構成を採用可能であるが、履歴をリセットしない構成が好ましい。

【００６５】

論理演算回路３３の論理は、任意に決定できるが、例えば第１レスポンス出力回路３１と同様に、排他的論理和を演算する組み合わせ回路とすることができる。

【００６６】

このように現在の論理入力により決定される第１レスポンス出力と、上記第１レスポンス出力の過去の履歴により決定される第２レスポンス出力との論理演算により出力部３０のレスポンス出力Ｒを決定することで、あたかも異なるＰＵＦを有するルックアップテーブルのように振る舞わせることができるので、機械学習攻撃で構築しなければならないモデ

ルが複雑になる。従って、機械学習攻撃に対する耐性をさらに高めることができる。
【００６７】
特に第２レスポンス出力回路３２として履歴をリセットしない構成では、同じチャレンジ入力Ｃｉに対しても過去の履歴により異なるレスポンス出力Ｒを発生させることができる。従来のチップ固有乱数発生装置では、同じチャレンジ入力Ｃｉに対して同じレスポンス出力Ｒが発生するため、通信経路の盗聴等によりレスポンス出力Ｒが知られると、なりすましに用いられるおそれがある。このため、従来のチップ固有乱数発生装置では、原則としてＣＲＰは使い捨てされ、１度しか使用されない。これに対し、同じチャレンジ入力Ｃｉに対して異なるレスポンス出力Ｒが得られる場合、同じチャレンジ入力Ｃｉが繰り返し使用されても、レスポンス出力Ｒを予測することは困難である。従って、第２レスポンス出力回路３２として履歴をリセットしない構成を採用することで、過去に使用したチャレンジ入力Ｃｉを繰り返し使用できる認証システムの構築が可能となる。すなわち膨大なＣＲＰを準備する必要がなく、ひいては機械学習攻撃に対する耐性を維持しつつ、当該チップ固有乱数発生装置１の低コスト化及び低消費電力化が可能となる。
【００６８】
＜フィードバック部＞
フィードバック部４０は、出力部３０へ入力される第１信号４０ａと、チャレンジ入力端子１０から入力される第２信号４０ｂとの論理演算を行い、その結果を第１ルックアップテーブル部２０に入力する。このようにフィードバック部４０を設けることで、ルックアップテーブル２１の規模（入出力端子数及び個数）を増やすことなく、機械学習攻撃に対する耐性をさらに高めることができる。また、フィードバック部４０を有することで、複数のビット幅を持つチャレンジ入力Ｃｉを時分割して入力できるので、ルックアップテーブル２１の規模を増やすことなくチャレンジ入力数を増やすことができる。さらに、同一のチャレンジ入力Ｃｉを維持してもフィードバックと出力を繰り返すことでレスポンス数を増やすことができる。このように１組のチャレンジ入力Ｃｉで多数のレスポンス出力Ｒを得ることで、認証に要するＣＲＰ数が少なくなるため、高スループット化及び低エネルギー化を図ることができる。
【００６９】
上記論理演算は、第１論理演算回路４０ｃで行われる。上記論理演算としては、特に限定されないが、例えば第１信号４０ａと第２信号４０ｂとの各ビット単位での排他的論理和を用いることができる。なお、上記論理演算は、演算される論理式が動的に変わるものであってもよい。例えば１回目の論理演算では第１信号４０ａの入力が存在しないような場合があるが、このように第１信号４０ａの入力が存在しないタイミングでは正転出力とし、第１信号４０ａの入力が存在するタイミングでは反転出力とするといったように、論理の生成過程を複雑化することで機械学習攻撃に対する耐性をさらに高められる。
【００７０】
また、フィードバック部４０への第１信号４０ａの入力及び第２信号４０ｂの入力は、同期して更新されるとよい。具体的には、チャレンジ入力端子１０から入力される第２信号４０ｂの変化タイミングに同期するクロックにより値が更新される順序回路（フリップフロップ）を設け、この順序回路に第１信号４０ａ論理値又は第１ルックアップテーブル部２０に入力する論理値を記憶させるとよい。なお、第１ルックアップテーブル部２０に入力する論理値を記憶させる場合は、その論理値の変化により第１ルックアップテーブル部２０を経て第１信号４０ａへ速やかに変化が伝達されることになるので、実質的に第１信号４０ａの入力は、第２信号４０ｂの入力に同期して更新されることとなる。
【００７１】
このようにフィードバック部４０への第１信号４０ａの入力及び第２信号４０ｂの入力を同期して更新することで、当該チップ固有乱数発生装置１の出力が不安定となることを抑止ができる。
【００７２】
図１で、第１ルックアップテーブル部２０の３つのルックアップテーブル２１を、チャレ

ンジ入力端子１０のC_1～C_3を入力とする下位ルックアップテーブル２１ｘ、チャレンジ入力端子１０のC_4～C_6を入力とする中位ルックアップテーブル２１ｙ、チャレンジ入力端子１０のC_7～C_9を入力とする上位ルックアップテーブル２１ｚとすると、下位ルックアップテーブル２１ｘの入力は、第１ビットには、下位ルックアップテーブル２１ｘの第１ビットがフィードバックされ、第２ビットには、中位ルックアップテーブル２１ｙの第１ビットがフィードバックされ、第３ビットには、上位ルックアップテーブル２１ｚの第１ビットがフィードバックされて論理演算がなされている。中位ルックアップテーブル２１ｙ及び上位ルックアップテーブル２１ｚも同様の構成をとっている。

【００７３】

このようにフィードバック部４０が、第１信号４０ａのうち異なるルックアップテーブル２１に起因する論理演算結果を、第１ルックアップテーブル部２０の１のルックアップテーブル２１の入力端子２１ａに入力するよう構成されているとよい。第１信号４０ａのうち異なるルックアップテーブル２１に起因する論理演算結果を、第１ルックアップテーブル部２０の１のルックアップテーブル２１の入力端子２１ａに入力することで、有限のＣＲＰからその出力を機械学習により予測することをさらに困難なものとすることができる。従って、機械学習攻撃に対する耐性をさらに高めることができる。

【００７４】

逆に、下位ルックアップテーブル２１ｘの出力は、第１ビットが下位ルックアップテーブル２１ｘの第１ビットにフィードバックされ、第２ビットが中位ルックアップテーブル２１ｙの第１ビットにフィードバックされ、第３ビットが上位ルックアップテーブル２１ｚの第１ビットにフィードバックされて論理演算がなされている。中位ルックアップテーブル２１ｙ及び上位ルックアップテーブル２１ｚも同様の構成をとっている。

【００７５】

このようにフィードバック部４０が、第１信号４０ａのうち１のルックアップテーブル２１に起因する論理演算結果を、第１ルックアップテーブル部２０の全てのルックアップテーブル２１の入力端子２１ａに入力するよう構成されているとよい。第１信号４０ａのうち１のルックアップテーブル２１に起因する論理演算結果を、第１ルックアップテーブル部２０の全てのルックアップテーブル２１の入力端子２１ａに入力することで、有限のＣＲＰからその出力を機械学習により予測することをさらに困難なものとすることができる。従って、機械学習攻撃に対する耐性をさらに高めることができる。

【００７６】

機械学習攻撃に対する耐性をさらに高めるため、図８のようにフィードバック部４１を構成してもよい。フィードバック部４１は、第１信号４０ａを入力とする第２論理演算回路４０ｄをさらに有し、第１信号４０ａのうち異なるルックアップテーブル２１に起因する論理演算結果を、第１ルックアップテーブル部２０の１のルックアップテーブル２１の１の入力端子２１ａに入力するよう構成されている。

【００７７】

下位ルックアップテーブル２１ｘ、中位ルックアップテーブル２１ｙ及び上位ルックアップテーブル２１ｚを添え字ｉ（ｉ＝ｘ、ｙ、ｚ）、各ルックアップテーブル２１の各ビットを添え字ｊ（ｊ＝１、２、３）で表し、第２論理演算回路４０ｄの出力b_{ij}は、各ルックアップテーブル２１の出力をDQ_{ij}とするとき、例えば

b_{x1}＝ＥＸＯＲ（DQ_{11}、DQ_{21}、DQ_{31}）
b_{x2}＝ＥＸＯＲ（DQ_{12}、DQ_{22}、DQ_{32}）
b_{x3}＝ＥＸＯＲ（DQ_{13}、DQ_{23}、DQ_{33}）
b_{y1}＝ＥＸＯＲ（DQ_{11}、DQ_{23}、DQ_{32}）
b_{y2}＝ＥＸＯＲ（DQ_{12}、DQ_{21}、DQ_{33}）
b_{y3}＝ＥＸＯＲ（DQ_{13}、DQ_{22}、DQ_{31}）
b_{z1}＝ＥＸＯＲ（DQ_{11}、DQ_{22}、DQ_{33}）
b_{z2}＝ＥＸＯＲ（DQ_{12}、DQ_{23}、DQ_{31}）
b_{z3}＝ＥＸＯＲ（DQ_{13}、DQ_{21}、DQ_{32}）

とすることができる。
【００７８】
＜利点＞
当該チップ固有乱数発生装置１は、複数のチャレンジ入力端子１０の下流側に、複数のルックアップテーブル２１が並列に配されている。個々のルックアップテーブル２１は、複数のＰＵＦにより、入力端子２１ａに入力される信号を符号変換するので、出力の不規則性が高く、有限のＣＲＰからその出力を機械学習により予測することが困難である。従って、当該チップ固有乱数発生装置１は、機械学習攻撃に対する耐性が高い。また、複数のチャレンジ入力端子１０に対して分割してルックアップテーブル２１を設けるので、ルックアップテーブル２１全体の規模が比較的小さく、集積回路チップの低コスト化と低消費電力化とに有利である。
【００７９】
［第２実施形態］
以下、本発明の第２の実施形態に係るチップ固有乱数発生装置について、適宜図面を参照しつつ説明する。
【００８０】
図９に示すチップ固有乱数発生装置２は、集積回路チップに搭載されるチップ固有乱数発生装置である。当該チップ固有乱数発生装置２は、複数のチャレンジ入力端子１０と、チャレンジ入力端子１０の下流側に接続される第１ルックアップテーブル部２０と、第１ルックアップテーブル部２０の下流側に接続される出力部３０と、チャレンジ入力端子１０と第１ルックアップテーブル部２０との間に配置されるフィードバック部４０と、第１ルックアップテーブル部２０及び出力部３０の間に接続される第２ルックアップテーブル部６０とを備える。第１ルックアップテーブル部２０には、複数のルックアップテーブル２１が並列に配置されており、ルックアップテーブル２１が、複数の入力端子２１ａ及び複数の出力端子２１ｂを有するとともに、チップ固有乱数を発生する複数のＰＵＦにより、入力端子２１ａに入力される信号を符号変換して出力端子２１ｂに出力する。また、出力部３０は、レスポンス出力Ｒを生成する。
【００８１】
第１ルックアップテーブル部２０、出力部３０及びフィードバック部４０は、第１実施形態と同様に構成できるので、同一符号を付し詳説を省略する。以下、主に第２ルックアップテーブル部６０について説明する。また、第１実施形態と同様に、チャレンジ入力端子１０の端子数が９であり、第１ルックアップテーブル部２０が、３つの入力端子２１ａ及び３つの出力端子２１ｂを有する３つのルックアップテーブル２１を有する場合を例にとり説明するが、当該チップ固有乱数発生装置２は、この構成に限定されることを意味するものではない。
【００８２】
第２ルックアップテーブル部６０は、複数のルックアップテーブル６１が並列に配置されている。第２ルックアップテーブル部６０を構成する複数のルックアップテーブル６１の入力端子６１ａの端子数の合計は、第１ルックアップテーブル部２０を構成する複数のルックアップテーブル２１の入力端子２１ａの端子数の合計と等しい。
【００８３】
各ルックアップテーブル６１は、第１ルックアップテーブル２１と同様に構成することができる。ここでは、第２ルックアップテーブル部６０が、３つの入力端子６１ａ及び３つの出力端子６１ｂを有する３つのルックアップテーブル６１を有する場合を例にとり説明するが、当該チップ固有乱数発生装置２は、この構成に限定されることを意味するものではない。
【００８４】
図９に示すチップ固有乱数発生装置２では、第１ルックアップテーブル部２０の下位ルックアップテーブル２１ｘの３ビットの出力は、それぞれ第２ルックアップテーブル部６０を構成する３つのルックアップテーブル６１の第１ビットへ入力されている。同様に、第

１ルックアップテーブル部２０の中位ルックアップテーブル２１ｙの３ビットの出力は、それぞれ第２ルックアップテーブル部６０を構成する３つのルックアップテーブル６１の第２ビットへ入力され、第１ルックアップテーブル部２０の上位ルックアップテーブル２１ｚの３ビットの出力は、それぞれ第２ルックアップテーブル部６０を構成する３つのルックアップテーブル６１の第３ビットへ入力されている。

【００８５】

このように第１ルックアップテーブル部２０の１のルックアップテーブル２１の複数の出力端子２１ｂが、第２ルックアップテーブル部６０の複数のルックアップテーブル６１の入力端子６１ａに接続されているとよい。

【００８６】

＜利点＞

当該チップ固有乱数発生装置２は、第２ルックアップテーブル部６０を備え、第１ルックアップテーブル部２０の１のルックアップテーブル２１の複数の出力端子２１ｂを第２ルックアップテーブル部６０の複数のルックアップテーブル６１の入力端子６１ａに接続することで、有限のＣＲＰからその出力を機械学習により予測することをさらに困難なものとすることができる。従って、当該チップ固有乱数発生装置２は、機械学習攻撃に対する耐性をさらに高めることができる。

【００８７】

［その他の実施形態］

上記実施形態は、本発明の構成を限定するものではない。従って、上記実施形態は、本明細書の記載及び技術常識に基づいて上記実施形態各部の構成要素の省略、置換又は追加が可能であり、それらは全て本発明の範囲に属するものと解釈されるべきである。

【００８８】

上記実施形態では、ＰＵＦがＳＲＡＭのビットセルから構成されている場合を説明したが、ＰＵＦとして他の構成を採用することもできる。ＰＵＦとして、例えば不揮発メモリＰＵＦ、直列ＮＡＮＤ　ＰＵＦ、グリッジＰＵＦ、アービターＰＵＦ、リングオシレータＰＵＦ、バタフライＰＵＦ等のＰＵＦを使用することもできる。

【００８９】

上記実施形態では、出力部が１ビットのレスポンスを出力する場合を説明したが、複数のレスポンスを出力する構成とすることもできる。この場合、例えば上述の実施形態であれば、３つの異なるルックアップテーブルの３ビットの出力端子から１ビットずつを排他的に選択して演算（例えば排他的論理和）した３ビットの出力をレスポンス出力とすることができる。レスポンス出力を多ビット化することで、レスポンス効率を高められ、認証時間の短縮や、消費電力の削減を図ることができる。

【００９０】

上記実施形態では、１層又は２層のルックアップテーブル部を備える場合を説明したが、３層以上のルックアップテーブルを備えてもよい。また、２層目以降のルックアップテーブルの出力端子数を入力端子数よりも少なくすることで所望のビット数のレスポンス出力を得てもよい。この場合、ルックアップテーブル部は、出力部の一部を兼ねる。このように多層化することで、機械学習攻撃に対する耐性をさらに高めることができる。

【００９１】

上記実施形態では、出力部が現在の論理入力により決定される第１レスポンス出力回路と、上記第１レスポンス出力の過去の出力履歴により決定される第２レスポンス出力回路と、上記第１レスポンス出力回路及び上記第２レスポンス出力回路の出力の論理演算を行う論理演算回路とを有する場合を説明したが、出力部は、第１レスポンス出力回路のみにより構成されてもよい。この場合、出力部の出力は、現在の論理入力のみにより決定される。

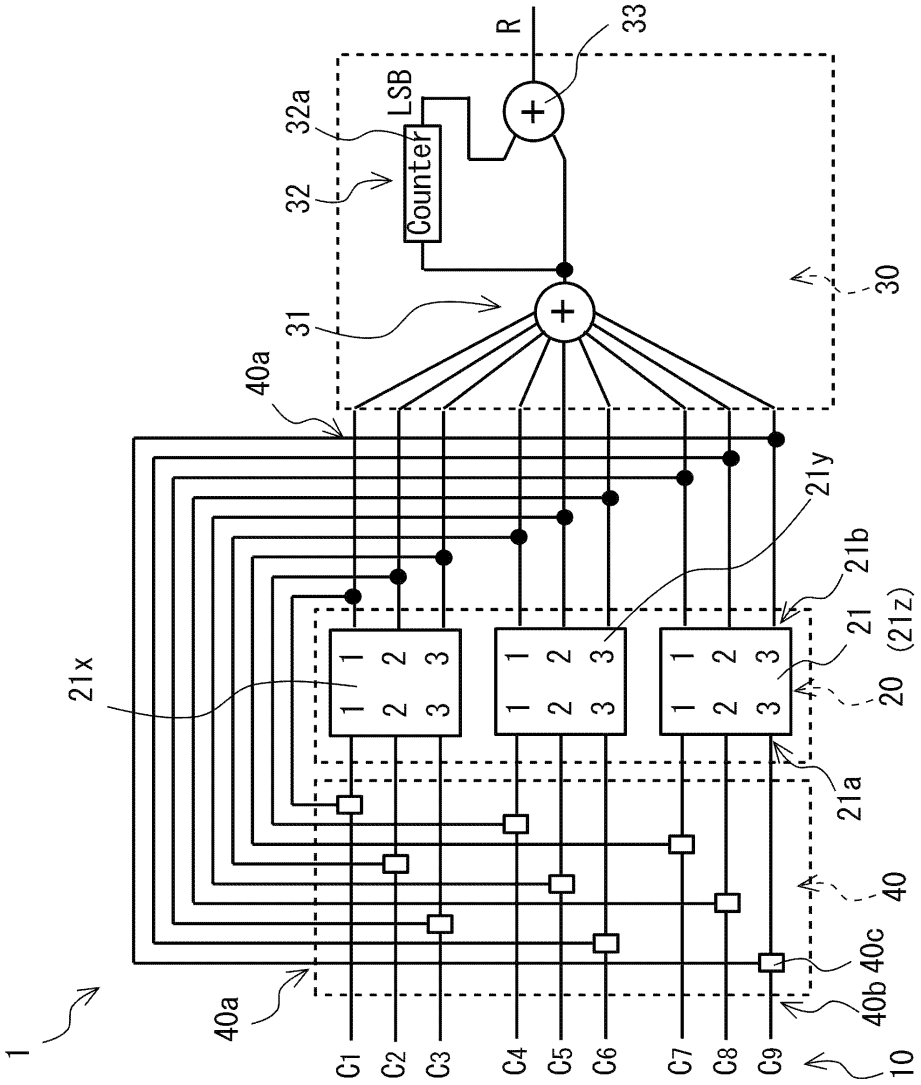
【００９２】

上記実施形態では、フィードバック部を備える場合を説明したが、フィードバック部は必須の構成要件ではない。フィードバック部を備えないチップ固有乱数発生装置も本発明の

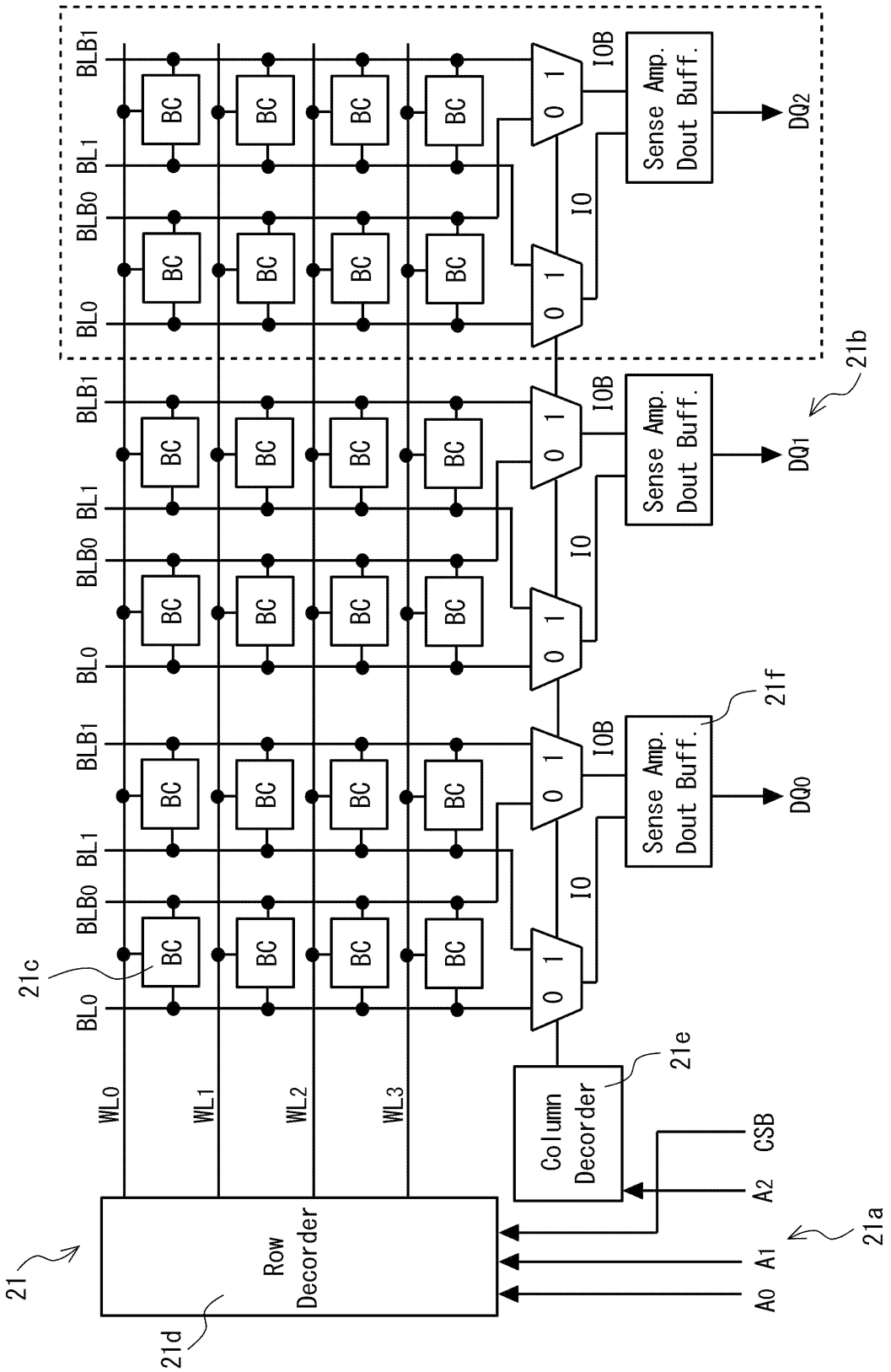
意図するところである。
【００９３】
上記第２実施形態では、フィードバック部の出力部へ入力される第１信号、つまり第２ルックアップテーブル部の出力信号と、チャレンジ入力端子から入力される第２信号との論理演算を行い、その結果を第１ルックアップテーブル部に入力する場合を示した。この構成に代えて、第１信号を第１ルックアップテーブル部の出力信号とすることもできる。また、第１信号が第２ルックアップテーブル部の出力信号である場合において、上記第２信号を第２ルックアップテーブル部の出力信号とし、上記第１信号と上記第２信号との論理演算の結果を第２ルックアップテーブル部に入力する構成とすることもできる。
【００９４】
上記実施形態では、出力部が第１レスポンス出力回路、第２レスポンス出力回路及び論理演算回路を有している場合を説明したが、これらの回路は、チャレンジ入力端子から出力端子に至る経路中の任意の位置、例えば第１ルックアップテーブル部の入力端子側、出力制御回路の出力側等に配置されていてもよい。このような位置に配置される場合であっても、出力部のレスポンス出力は上記論理演算回路の出力により決定されるので、同様の効果を奏する。
【産業上の利用可能性】
【００９５】
以上説明したように、本発明のチップ固有乱数発生装置は、低コスト化及び低消費電力化が可能であり、かつ機械学習攻撃に対する耐性が高い。
【符号の説明】
【００９６】
１、２　チップ固有乱数発生装置
１０　チャレンジ入力端子
２０　第１ルックアップテーブル部
２１、２２、２３　ルックアップテーブル
２１ａ、２３ｃ　入力端子
２１ｂ、２３ｄ　出力端子
２１ｃ、２１ｇ　ビットセル
２１ｄ　ローデコーダ
２１ｅ　カラムデコーダ
２１ｆ　センスアンプ
２１ｘ　下位ルックアップテーブル
２１ｙ　中位ルックアップテーブル
２１ｚ　上位ルックアップテーブル
２３ａ　ルックアップテーブル本体
２３ｂ　出力制御回路
３０　出力部
３１　第１レスポンス出力回路
３２　第２レスポンス出力回路
３３　論理演算回路
４０、４１　フィードバック部
４０ａ　第１信号
４０ｂ　第２信号
４０ｃ　第１論理演算回路
４０ｄ　第２論理演算回路
５０　ラッチ回路
５１　第１ＣＭＯＳインバータ
５１ａ　ＰＭＯＳ
５１ｂ　ＮＭＯＳ

５２　第２ＣＭＯＳインバータ
５２ａ　ＰＭＯＳ
５２ｂ　ＮＭＯＳ
５３　安定化回路
５３ａ　第１ＰＭＯＳ
５３ｂ　第２ＰＭＯＳ
５４　パストランジスタ
５５　安定化回路
５５ａ　第１ＮＭＯＳ
５５ｂ　第２ＮＭＯＳ
５６　安定化回路
５６ａ　書込用ＣＭＯＳインバータ
５６ｂ　書込用ドライバ
６０　第２ルックアップテーブル部
６１　ルックアップテーブル
６１ａ　入力端子
６１ｂ　出力端子
１００　アービターＰＵＦ
１０１　多段遅延回路
１０２　選択回路
１０３　アービター
Ｃｉ　チャレンジ入力
Ｒ　レスポンス出力

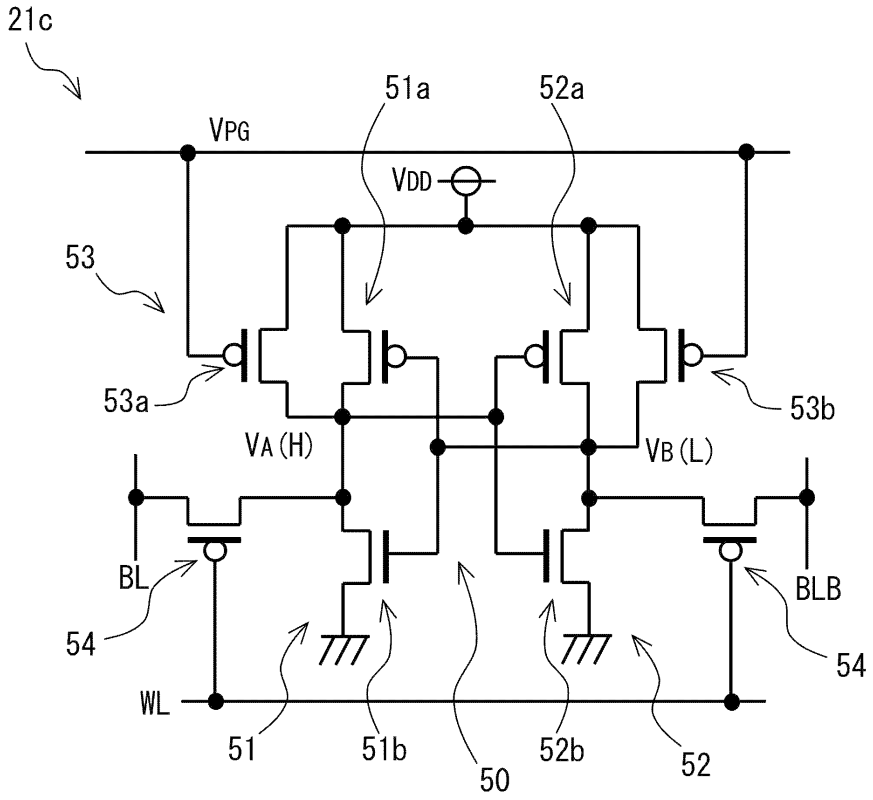
【図１】


R
33
LSB
32a
Counter
32
30
31
40a
21y
21b
21
(21z)
20
21x
1 2 3
1 2 3
21a
40
40c
40b
40a
1
C1 C2 C3 C4 C5 C6 C7 C8 C9
10

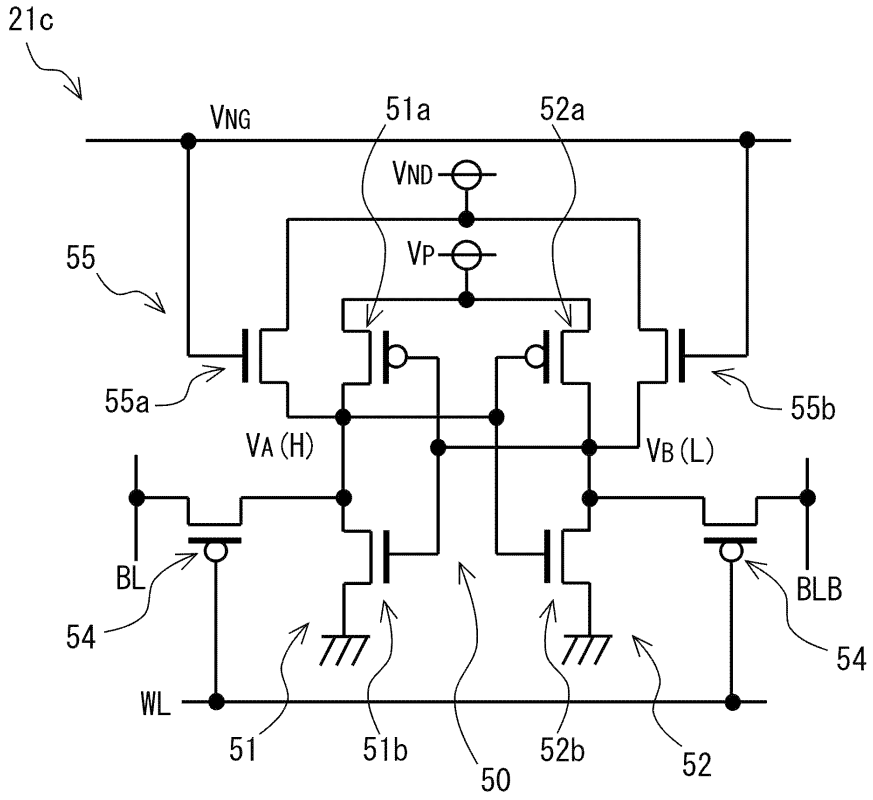
【図２】


21
Row Decorder
21d
21a
A0
A1
A2
CSB
21e
Column Decorder
WL0
WL1
WL2
WL3
21c
BL0
BLB0
BL1
BLB1
BC
0 1
IO
IOB
Sense Amp. Dout Buff.
DQ0
DQ1
DQ2
21f
21b

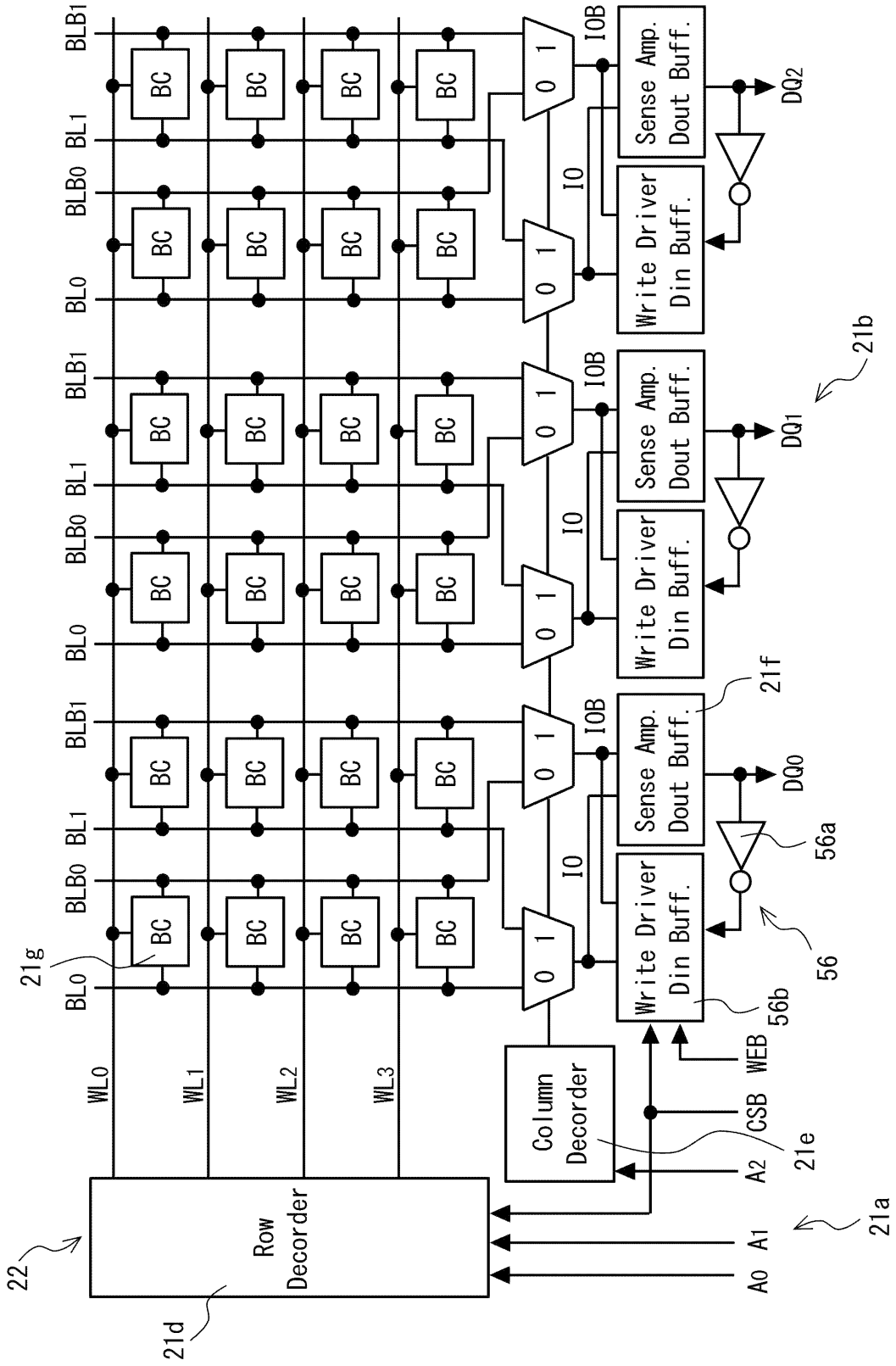
【図３】


21c
51a
52a
VPG
VDD
53
53a
53b
VA (H)
VB (L)
BL
BLB
54
54
WL
51
51b
50
52b
52

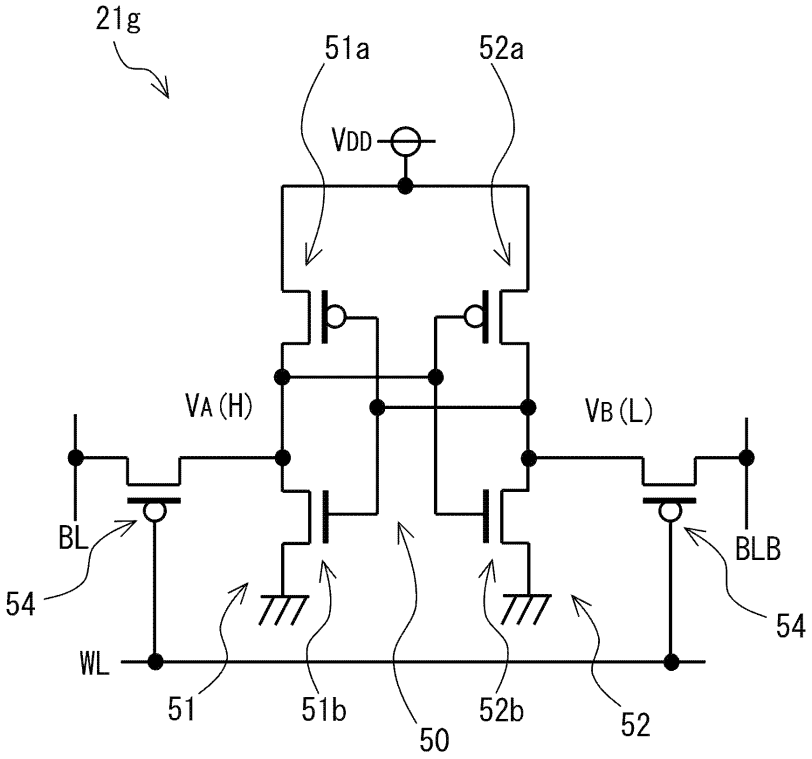
【図４】


21c
51a
52a
VNG
VND
VP
55
55a
55b
VA (H)
VB (L)
BL
BLB
54
54
WL
51
51b
50
52b
52

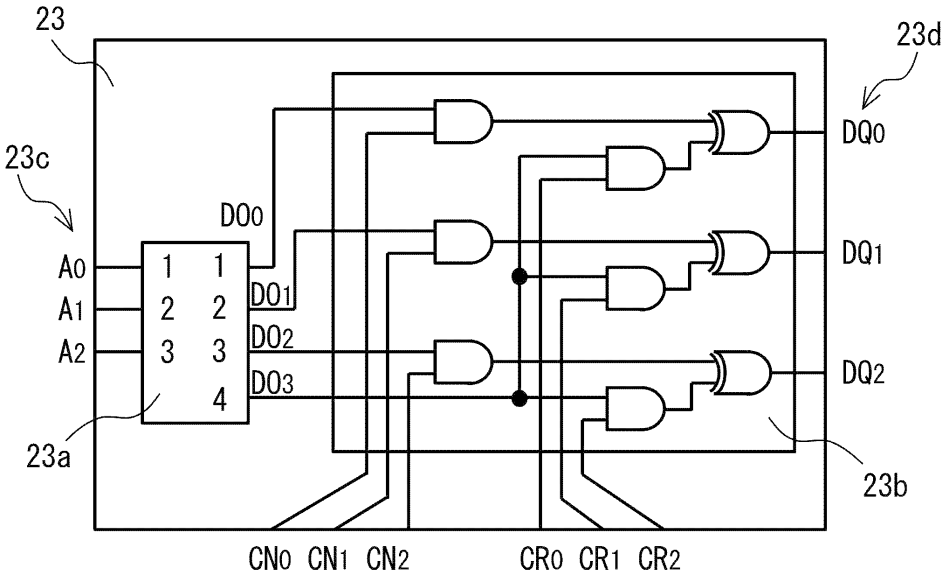
【図５】


BLB1
BL1
BLB0
BL0
BC
WL0
WL1
WL2
WL3
0 1
IO
IOB
Sense Amp. Dout Buff.
Write Driver Din Buff.
DQ2
DQ1
DQ0
21b
21f
21g
56a
56
56b
WEB
CSB
A2
A1
A0
21e
21a
Column Decorder
Row Decorder
22
21d

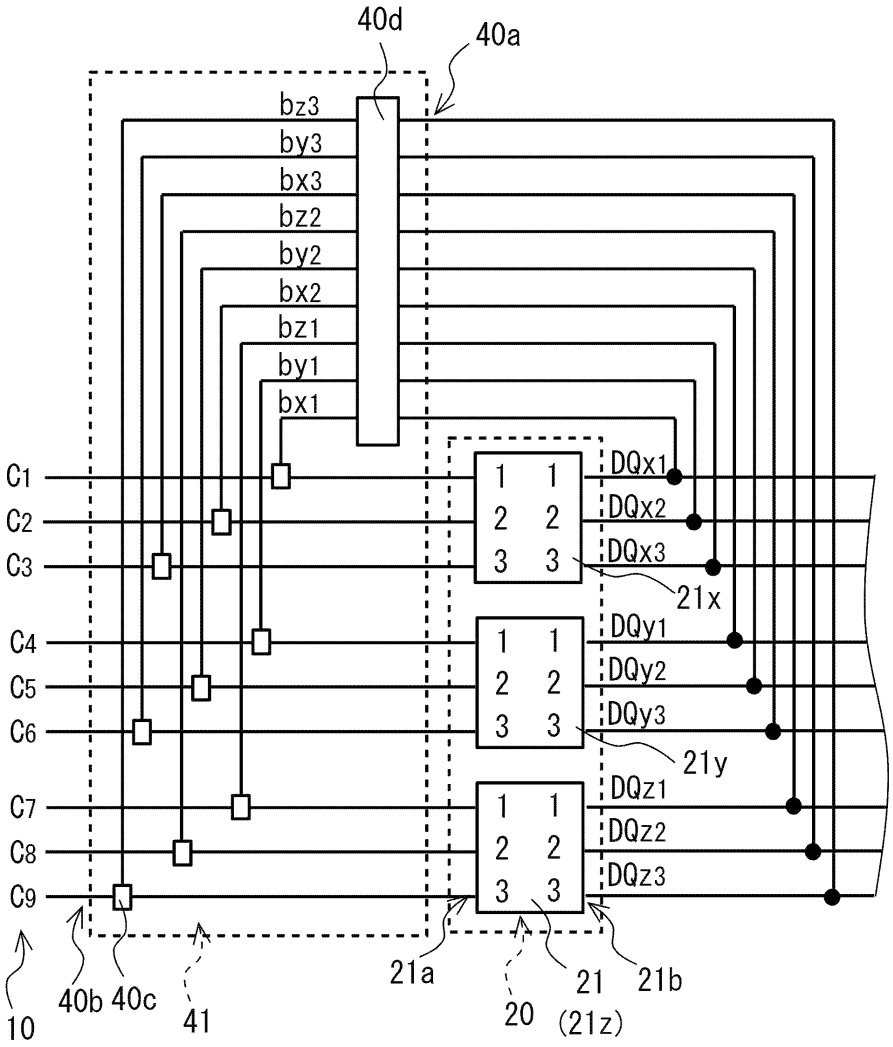
【図６】


21g
51a
52a
VDD
VA (H)
VB (L)
BL
BLB
54
54
WL
51
51b
50
52b
52

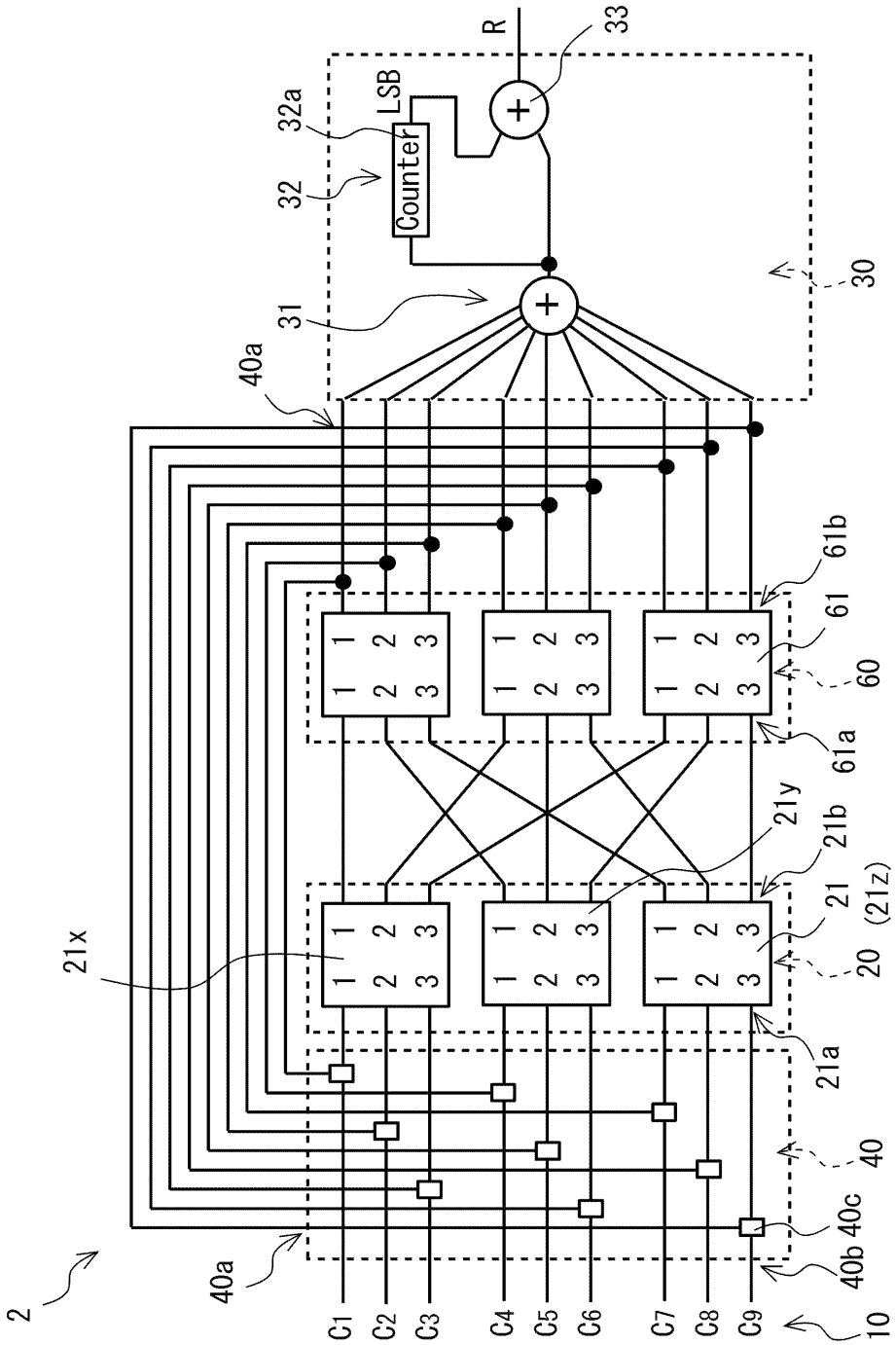
【図７】


23
23d
23c
DO0
A0
A1
A2
1 1
2 2
3 3
4
DO1
DO2
DO3
DQ0
DQ1
DQ2
23a
23b
CN0 CN1 CN2
CR0 CR1 CR2

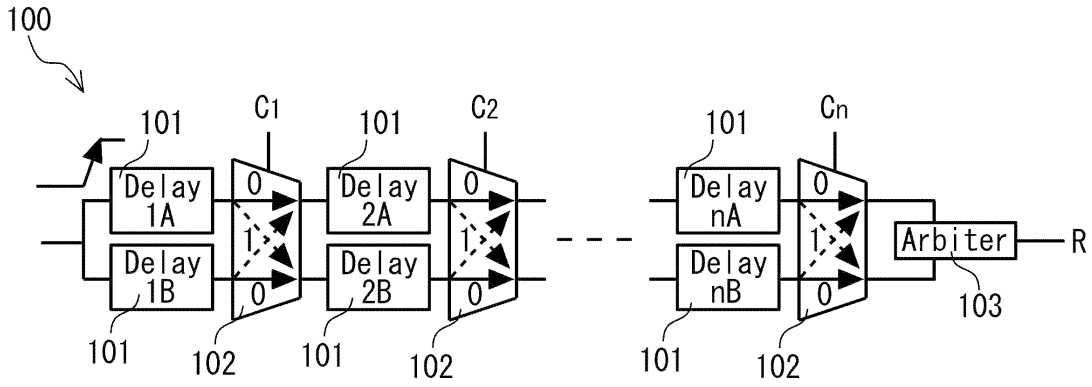
【図８】


40d
40a
bz3
by3
bx3
bz2
by2
bx2
bz1
by1
bx1
C1
C2
C3
C4
C5
C6
C7
C8
C9
1 1
2 2
3 3
DQx1
DQx2
DQx3
21x
DQy1
DQy2
DQy3
21y
DQz1
DQz2
DQz3
10
40b
40c
41
21a
20
21
(21z)
21b

【図９】


R
33
LSB
32a
Counter
32
30
31
40a
61b
61
60
61a
21y
21b
21
(21z)
20
21x
21a
40
40c
40b
2
40a
C1
C2
C3
C4
C5
C6
C7
C8
C9
10

【図１０】


100
101
C1
101
C2
101
Cn
Delay 1A
Delay 1B
Delay 2A
Delay 2B
Delay nA
Delay nB
0
1
Arbiter
R
103
101
102