(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6474056号
(P6474056)
(45)発行日　平成31年2月27日(2019.2.27)　(24)登録日　平成31年2月8日(2019.2.8)

(51)Int.Cl.　F I
H04L 9/10 (2006.01)　H04L 9/00 621Z
G11C 13/00 (2006.01)　G11C 13/00 215
G11C 13/00 420

請求項の数 22　(全 53 頁)

(21)出願番号　特願2015-209809(P2015-209809)
(22)出願日　平成27年10月26日(2015.10.26)
(65)公開番号　特開2016-105585(P2016-105585A)
(43)公開日　平成28年6月9日(2016.6.9)
審査請求日　平成30年5月21日(2018.5.21)
(31)優先権主張番号　特願2014-236707(P2014-236707)
(32)優先日　平成26年11月21日(2014.11.21)
(33)優先権主張国　日本国(JP)

(73)特許権者　314012076
パナソニックＩＰマネジメント株式会社
大阪府大阪市中央区城見２丁目１番６１号
(74)代理人　100101683
弁理士　奥田　誠司
(74)代理人　100155000
弁理士　喜多　修市
(74)代理人　100180529
弁理士　梶谷　美道
(74)代理人　100125922
弁理士　三宅　章子
(74)代理人　100135703
弁理士　岡部　英隆
(74)代理人　100188813
弁理士　川喜田　徹

最終頁に続く

(54)【発明の名称】耐タンパ性を有する不揮発性メモリ装置、集積回路カード、不揮発性メモリ装置の認証方法、不揮発性メモリ装置を用いた暗号化方法および復号化方法

(57)【特許請求の範囲】
【請求項１】
可変状態では、異なる複数の電気的信号の印加に応じて抵抗値が複数の抵抗値範囲の間を不揮発的かつ可逆的に遷移する性質を有する複数のメモリセルがアレイ状に配置されたメモリセルアレイと、
コントロール信号の入力を受け付ける制御回路と、
前記制御回路に入力された前記コントロール信号に基づき、前記複数のメモリセルの少なくとも一部の各々の前記抵抗値に関する複数の抵抗値情報を取得する読み出し回路と、
前記読み出し回路によって取得された前記複数の抵抗値情報に基づいて２値化基準値を算出する演算回路と、を備え、
前記読み出し回路は、前記２値化基準値に基づいて、前記複数の抵抗値情報の各々、および前記複数のメモリセルの前記少なくとも一部と異なる一部の各々の前記抵抗値に関する複数の抵抗値情報の各々の少なくとも一方に対して２つの値から選択的に１つの値を割り当てることにより個体識別情報を生成する、不揮発性メモリ装置。
【請求項２】
前記複数の抵抗値範囲は、第１抵抗値範囲、および前記第１抵抗値範囲より抵抗値が小さい第２抵抗値範囲を含み、
前記複数のメモリセルの各々は、初期状態では、前記抵抗値が前記第１および第２抵抗値範囲のいずれとも異なる初期抵抗値範囲にあり、
前記複数のメモリセルの各々は、電気的ストレスが印加されることにより、前記初期状

態から前記可変状態に変化する、請求項１に記載の不揮発性メモリ装置。
【請求項３】
前記演算回路は、前記読み出し回路によって取得された、前記複数の抵抗値情報の中央値を前記２値化基準値として算出する、請求項１または２に記載の不揮発性メモリ装置。
【請求項４】
前記読み出し回路は、前記複数の抵抗値情報の各々と、前記演算回路が算出する前記２値化基準値との大小関係に基づいて、複数の第１の誤差情報を取得し、
前記演算回路は、前記複数の第１の誤差情報と所定の係数とに基づいて複数の第２の誤差情報を算出する感度調整回路と、
前記２値化基準値に前記複数の第２の誤差情報を加えることにより、前記２値化基準値を更新する累積加算回路とを含む、請求項１に記載の不揮発性メモリ装置。
【請求項５】
前記読み出し回路は、前記複数のメモリセルから第１の所定の数の第１の複数のメモリセルを順次選択し、選択した前記第１の複数のメモリセルの各々の抵抗値に関する第１の複数の抵抗値情報を取得し、前記演算回路は、前記第１の複数の抵抗値情報に基づいて第１の２値化基準値を算出し、
前記読み出し回路は、前記複数のメモリセルから前記第１の所定の数と同じ又は異なる第２の所定の数の第２の複数のメモリセルを順次選択し、選択した前記第２の複数のメモリセルの各々の抵抗値に関する第２の複数の抵抗値情報を取得し、前記第１の２値化基準値に基づいて、前記第２の複数の抵抗値情報の各々に対して前記２つの値から選択的に１つの値を割り当てることにより、第１の個体識別情報を生成する、請求項１から４のいずれかに記載の不揮発性メモリ装置。
【請求項６】
前記演算回路は、前記第１の２値化基準値に所定のオフセット値を加算または減算して第２の２値化基準値を取得し、
前記読み出し回路は、前記第２の２値化基準値に基づいて、前記第２の複数の抵抗値情報の各々に対して前記２つの値から選択的に１つの値を割り当てることにより、第２の個体識別情報を生成する、請求項５に記載の不揮発性メモリ装置。
【請求項７】
誤り訂正およびパリティー生成回路をさらに備え、
前記制御回路は、予め、前記演算回路に前記第１の２値化基準値を算出させ、前記読み出し回路に前記第１の個体識別情報を生成させ、前記誤り訂正およびパリティー生成回路に前記第１の個体識別情報からパリティーデータを生成させ、前記パリティーデータを前記メモリセルアレイ内に保存させ、
使用時に、前記制御回路は、前記演算回路に前記使用時における前記第１の２値化基準値を算出させ、前記読み出し回路に前記使用時における前記第１の個体識別情報を生成させ、前記誤り訂正およびパリティー生成回路に、前記メモリセルアレイ内に保存された前記パリティーデータを用いて前記使用時における前記第１の個体識別情報を訂正させ、第３の個体識別情報を取得する、請求項５に記載の不揮発性メモリ装置。
【請求項８】
データの乱数性を検定する乱数検定回路をさらに備え、
前記乱数検定回路は、前記第１の個体識別情報が所定の乱数の基準を満足しているか否かを検定するとともに検定結果を出力する、請求項５に記載の不揮発性メモリ装置。
【請求項９】
暗号化および復号化を行う暗号処理回路をさらに備え、
前記暗号処理回路は、前記個体識別情報を暗号鍵として用いて、入力されたデータを暗号化して暗号化データを生成し、
前記暗号化データが前記メモリセルアレイに第１種データおよび第２種データの少なくとも一方として記憶され、
前記第１種データは、前記複数のメモリセルの各々が前記初期状態にあるか前記可変状

態にあるかを示しており、
前記第２種データは、前記複数のメモリセルの各々の前記抵抗値が前記第１抵抗値範囲にあるか第２抵抗値範囲にあるかを示している、請求項２に記載の不揮発性メモリ装置。
【請求項１０】
前記読み出し回路は、記憶された前記暗号化データ、および前記個体識別情報を読み出して前記暗号処理回路に送信し、
前記暗号処理回路は、前記個体識別情報を復号鍵として前記暗号化データを復号化する、請求項９に記載の不揮発性メモリ装置。
【請求項１１】
前記複数のメモリセルの各々は、
第１電極と、
第２電極と、
前記第１電極および前記第２電極の間に介在する抵抗変化層を有する抵抗変化素子とを備える、請求項１から１０のいずれかに記載の不揮発性メモリ装置。
【請求項１２】
前記抵抗変化層は、絶縁体で構成された層を含む、請求項１１に記載の不揮発性メモリ装置。
【請求項１３】
前記抵抗変化層は、前記絶縁体で構成された層を貫く導電パスを有する、請求項１２に記載の不揮発性メモリ装置。
【請求項１４】
前記抵抗変化層は、金属酸化物を含む材料によって構成される、請求項１１から１３のいずれかに記載の不揮発性メモリ装置。
【請求項１５】
前記抵抗変化層は、酸素不足型の金属酸化物を含む材料によって構成された層を含む、請求項１１から１３のいずれかに記載の不揮発性メモリ装置。
【請求項１６】
前記金属酸化物は、遷移金属酸化物およびアルミニウム酸化物の少なくとも一方である、請求項１４または１５に記載の不揮発性メモリ装置。
【請求項１７】
前記金属酸化物は、タンタル酸化物、ハフニウム酸化物およびジルコニウム酸化物の少なくとも一つである、請求項１４または１５に記載の不揮発性メモリ装置。
【請求項１８】
前記絶縁体は金属酸化物を含み、
前記導電パスは、前記金属酸化物よりも酸素含有率が低い酸素不足型の金属酸化物を有する、請求項１３に記載の不揮発性メモリ装置。
【請求項１９】
可変状態では、異なる複数の電気的信号の印加に応じて抵抗値が複数の抵抗値範囲の間を不揮発的かつ可逆的に遷移する性質を有する複数のメモリセルがアレイ状に配置されたメモリセルアレイと、
コントロール信号の入力を受け付ける制御回路と、
前記制御回路に入力された前記コントロール信号に基づき、前記複数のメモリセルの少なくとも一部の各々の前記抵抗値に関する複数の抵抗値情報を取得する読み出し回路と、
前記読み出し回路によって取得された前記複数の抵抗値情報に基づいて２値化基準値を算出する演算回路と、を備え、
前記読み出し回路は、前記２値化基準値に基づいて、前記複数の抵抗値情報の各々、および前記複数のメモリセルの前記少なくとも一部と異なる一部の各々の前記抵抗値に関する複数の抵抗値情報の各々の少なくとも一方に対して２つの値から選択的に１つの値を割り当てることにより個体識別情報を生成する、不揮発性メモリ装置と、
前記コントロール信号が入力され、前記個体識別情報に関連する情報が出力される入出

力インタフェース部と、を備えた集積回路カード。
【請求項２０】
請求項６に記載の不揮発性メモリ装置が正規の装置であることを認証するための認証方法であって、
複数の前記所定のオフセット値を用いて、各オフセット値に応じて異なる個体識別情報を生成して外部装置に保持し、
出荷後、前記不揮発性メモリ装置が使用されるときに、外部から入力されたオフセット値を特定するチャレンジデータを利用して個体識別情報を生成し、
生成した前記個体識別情報を前記外部装置に送信し、
生成した前記個体識別情報と、予め前記外部装置に保持されていた個体識別情報とが一致しているか否かを判断し、
一致している場合には、前記不揮発性メモリ装置が正規の装置であるとして認証する、
不揮発性メモリ装置の認証方法。
【請求項２１】
請求項５に記載の不揮発性メモリ装置を用いた暗号化方法であって、
前記不揮発性メモリ装置は、暗号化および復号化を行う暗号処理回路をさらに備え、
前記不揮発性メモリ装置にデータを入力し、
入力された前記データを、前記暗号処理回路が、前記個体識別情報を暗号鍵として用いて暗号化して暗号化データを生成し、
前記暗号化データを記憶する、暗号化方法。
【請求項２２】
請求項２１に記載の暗号化方法によって暗号化された暗号化データの復号化方法であって、
記憶された前記暗号化データを受け取り、
前記不揮発性メモリセルのアレイから、前記個体識別情報を読み出し、
前記暗号処理回路が、前記個体識別情報を復号鍵として用いて前記暗号化データを復号化する、復号化方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、抵抗変化型の不揮発性メモリセルを複数有し、かつ耐タンパ性を有する不揮発性メモリ装置に関する。
【背景技術】
【０００２】
ネットバンキングまたはネットショッピングなど、インターネットを介して行われる電子商取引サービスの市場は急速に拡大している。このときの決済方法として電子マネーが用いられ、その媒体として利用される集積回路（“Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ”、以下、ＩＣと略称する。）カードおよびスマートフォン端末も同様に利用が拡大している。これらのサービスには、決済時の安全性のため、通信における相互認証および通信データの暗号化にあたって常により高いレベルのセキュリティー技術が求められる。
【０００３】
ソフトウェア技術に関しては、高度な暗号化アルゴリズムを中心としたプログラム処理の暗号化技術が蓄積されており、十分なセキュリティーが達成されている。しかし、技術進歩により、回路内部の情報を外部から直接読み取られる懸念が急速に高まっている。
【０００４】
特許文献１は、このような懸念への対応策を提案している。一般的にはセキュリティーを強化したＩＣでは、内部に搭載する暗号回路を用いて機密情報を暗号化して利用しており、情報の漏洩を防止している。この場合、内部に保持している暗号鍵（「秘密鍵」ともいう。）の情報を外部に漏洩させないことが必須となる。
【０００５】

暗号回路の方式の代表的なものとしては３ＤＥＳ（Triple Data Encryption Standard）およびＡＥＳ（Advanced Encryption Standard）といったものが広く用いられている。これらの暗号化方式には、入出力となっている平文（暗号前データ）－暗号文のペアを入手し、最高速のコンピュータを駆使して解析しても、現実的な時間内では暗号鍵を特定できないような高度な暗号アルゴリズムが採用されており、その安全性は確認されている。しかしながら、暗号化されたデータへのハッキングは安全であるとされていても、暗号鍵が直接ハッキングされる脆弱性が懸念されていた。

【０００６】

古典的な手法のＩＣでは、暗号鍵を内部のフューズＲＯＭまたは不揮発性メモリに保存していた。前者の構成には、Ｘ線投射などによってフューズ素子の状態を観察し、フューズ素子の導通・非導通を解析し、保存されている鍵情報をハッキングされる、という問題があった。また、後者の構成はＸ線投射では解析されないものの、不揮発性メモリのメモリ素子両端に直接プローブをあて電気的に素子の状態を読み取ることにより鍵情報をハッキングされる問題があった。そのため、セキュリティーを強化したＩＣでは内部回路に直接プローブを当てられないように最先端の微細プロセスを用いて製造される。つまり、最新技術のプローブの先端径よりも細い配線ルールをもつ微細プロセスでＩＣを製造することで、プロービングによる解析の脅威を回避していた。

【０００７】

しかし、このような対策に対して、サイドチャンネル攻撃という手法がとられ始め、脅威とされてきている。サイドチャンネル攻撃とは、特許文献１に説明されるように、各信号処理回路の実行時の半導体デバイスの消費電力、および消費電力に依存する輻射電磁波などのサイドチャネル情報を用いて、暗号鍵を特定する手法である。この手法が脅威である理由は、攻撃者（ハッカー）がＩＣに物理的に損傷を与えず、実動作中に鍵情報をハッキングできることにある。

【０００８】

このようなサイドチャネル攻撃に分類される差分電力攻撃（ＤＰＡ：Ｄｉｆｆｅｒｅｎｔｉａｌ　Ｐｏｗｅｒ　Ａｎａｌｙｓｉｓ）は、１９９９年にＰ．　Ｋｏｃｈｅｒによって発表された。このＤＰＡ手法は、ＩＣ動作時の信号値または信号遷移頻度と、消費電力との間に相関関係があることを利用している。具体的には、ＤＰＡ手法は、このような相関関係を多数回積分し、ノイズを除去しながら機械学習制御をおこなうことで固定パターンを導き出し、鍵情報を特定する。特許文献１の例では、暗号処理回路の動作から特定される例が示されている。不揮発性メモリに記憶された鍵情報は、暗号処理を実行することをトリガとしたタイミングで読み出される。ＤＰＡの原理に鑑みれば、そのタイミングと同じようなタイミングで読み出されたデータが特定され取得されれば、ＤＰＡによりデータ内容が解析される恐れがある。また、ＩＣの内部仕様書が漏洩するとＩＣの制御方法がハッカーに理解され、上述のように不揮発性メモリに保存されたデータ全てが、暗号鍵情報も含めてハードコピーされ、ＩＣの複製が作成されてしまう。

【０００９】

近年、これらの課題を解決するために、ＰＵＦ（物理的複製困難関数；Physically Unclonable Function）技術が提案されている。ＰＵＦ技術は、製造ばらつきを活用してＩＣごとに異なるユニークな個体識別情報を生成する技術である。以降、本明細書ではＰＵＦ技術により生成された個体識別情報を「ディジタルＩＤデータ」と呼ぶ。ディジタルＩＤデータはＩＣの物理特性のばらつきに関連づけられた各デバイス固有の乱数データであると言える。ＩＣごとにその物理特性を人為的に制御することが不可能であるため、物理的な複製が不可能なデータを生成することができる。

【００１０】

なお、物理特性のばらつきの制御がある程度可能であったとしても、製造時に発生するランダムな工程ばらつきを利用する場合は、各ＩＣに固有でユニークなディジタルＩＤデータをＰＵＦ技術により作成するのは容易である。しかしながら、事前に決定した特定の個体識別情報を故意に作成することは、実際上は極めて困難である。半導体プロセスにお

いて様々な物理特性に製造ばらつきが生じる。製造ばらつきとして、例えば、半導体プロセスにおけるドーピング量、酸化物厚さ、チャネル長、金属配線層の幅および厚さ、寄生抵抗ならびに寄生容量などが挙げられる。

【００１１】

具体的な先行例として、特許文献２や非特許文献１のようなＳＲＡＭ ＰＵＦが例示され得る。これらの例では、ＳＲＡＭにおける各メモリセルにおいて、主にトランジスタのＶｔばらつき（動作電圧のばらつき）により電源投入時の初期値のディジタルデータが１状態になりやすいか、０状態になりやすいかが異なる現象を用いている。これは、各ＩＣに搭載されたＳＲＡＭのセルごとに固有であり、異なっている。つまり、ＳＲＡＭに電源投入したときの初期値データがディジタルＩＤデータとして用いられる。

【００１２】

特許文献３は、ＳＲＡＭ－ＰＵＦの変形例であり、ＳＲＡＭのメモリセルの不良ビットがランダムに発生する現象を用いている。更に、特許文献１および非特許文献２では、アービター（Ａｒｂｉｔｅｒ）ＰＵＦまたはグリッジＰＵＦと呼ばれるＰＵＦ技術が紹介されている。アービターＰＵＦおよびグリッジＰＵＦでは、ゲート遅延または配線遅延を用いて組み合わせ回路の出力が入力に対してランダムに変化することを用いている。製造ばらつきによって変化するゲート遅延または配線遅延は、各ＩＣにおける固有の遅延量となる。従って、ＩＣごとに異なるものの各ＩＣにおいては入力に対して、ほぼ等しい結果を出力するため、ディジタルＩＤデータを生成できる。

【００１３】

このように、ＰＵＦ技術により、各ＩＣ固有の乱数となるディジタルＩＤデータが複製できないデータとして生成される。このディジタルＩＤデータは、前述した秘密鍵を暗号化するデバイス鍵として用いられる。デバイス鍵（ディジタルＩＤデータ）によって暗号化された秘密鍵は、暗号化された状態で不揮発性メモリに保存される。すなわち、不揮発性メモリに記録された暗号化秘密鍵はデバイス鍵でしか元の秘密鍵データに復号できない。よって、ハッキングにより不揮発性メモリ内のデータが全てハードコピーされたとしても、各ＩＣ固有のデバイス鍵（ディジタルＩＤデータ）が複製できないため暗号化秘密鍵が元に戻せず利用することができない。

【００１４】

更に、ＰＵＦ技術により生成されるディジタルＩＤデータは、僅かな製造ばらつきを用いて生成されるため、生成するときの温度環境または電源状態、更には経年劣化などにより、利用する物理特性に変動が生じ、得られるデータに誤りが発生し得る。このため非特許文献１に示されるように、製造時の検査工程にてＰＵＦ技術によって生成されるディジタルＩＤデータを元に、誤り訂正用のパリティーデータを演算し、パリティーデータを別途不揮発性メモリなどに保存しておく。そして、システムがディジタルＩＤデータを利用するときに、ＰＵＦ技術によって生成した誤りを含んだディジタルＩＤデータはパリティーデータを用いて誤り訂正処理を実行することで、常に同じＩＤデータを得る。

【００１５】

このように誤りを含んだデータであるためデータの訂正を行うといった非効率な技術に思えるが、このことがもう一つの重要な特徴となる。ディジタルＩＤデータがＰＵＦ技術により生成しなおされるたびに、不規則にデータに誤りが生じるため、前述したサイドチャンネルアタックのようなハッキング攻撃を受けたとしてもデータパターンが定まらず解析を非常に困難にさせ、セキュリティー性を大きく向上させる。

【００１６】

このようにＰＵＦ技術は、暗号および相互認証を安全に行う上でセキュリティーを高める重要な技術である。

【先行技術文献】

【特許文献】

【００１７】

【特許文献１】国際公開ＷＯ２０１２／０１４２９１号公報

【特許文献２】特表２０１３－５４５３４０号公報
【特許文献３】特開２０１２－４３５１７号公報
【非特許文献】
【００１８】
【非特許文献１】“Ａ　０．１９ｐＪ／ｂ　ＰＶＴ－Ｖａｒｉａｔｉｏｎ－Ｔｏｌｅｒａｎｔ　Ｈｙｂｒｉｄ　Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ　Ｃｉｒｃｕｉｔ　ｆｏｒ　１００％　Ｓｔａｂｌｅ　Ｓｅｃｕｒｅ　Ｋｅｙ　Ｇｅｎｅｒａｔｉｏｎ　ｉｎ　２２ｎｍ　ＣＭＯＳ”　Ｓａｎｕ　Ｋ．　Ｍａｔｈｅｗ，　ｅｔ　ａｌ．　ＩＳＳＣＣ２０１４
【非特許文献２】“耐タンパディペダブルＶＬＳＩシステムの開発・評価”　Ｔａｋｅｓｈｉ　Ｆｕｊｉｎｏ，「ディペンダブルＶＬＳＩシステムの基盤技術」　ＣＲＥＳＴ２００９年採択テーマ２０１２年度実績報告資料
【発明の概要】
【発明が解決しようとする課題】
【００１９】
前述のようにＰＵＦ技術はＩＣのセキュリティー性を高める重要な技術である。しかしながら、セキュリティー性のさらなる向上が求められていた。
【００２０】
本願の、限定的ではない例示的なある実施形態は、セキュリティー性により優れたディジタルＩＤデータを生成するためのＰＵＦ技術を提供する。
【課題を解決するための手段】
【００２１】
本開示の一態様にかかる不揮発性メモリ装置は、可変状態では、異なる複数の電気的信号の印加に応じて抵抗値が複数の抵抗値範囲の間を不揮発的かつ可逆的に遷移する性質を有する複数のメモリセルがアレイ状に配置されたメモリセルアレイと、コントロール信号の入力を受け付ける制御回路と、前記制御回路に入力された前記コントロール信号に基づき、前記複数のメモリセルの少なくとも一部の各々の前記抵抗値に関する複数の抵抗値情報を取得する読み出し回路と、前記読み出し回路によって取得された前記複数の抵抗値情報に基づいて２値化基準値を算出する演算回路と、を備え、前記読み出し回路は、前記２値化基準値に基づいて、前記複数の抵抗値情報の各々、および前記複数のメモリセルの前記少なくとも一部と異なる一部の各々の前記抵抗値に関する複数の抵抗値情報の各々の少なくとも一方に対して２つの値から選択的に１つの値を割り当てることにより個体識別情報を生成する。
【００２２】
上述の一般的かつ特定の態様は、システム、方法およびコンピュータプログラムを用いて実装され、またはシステム、方法およびコンピュータプログラムの組み合わせを用いて実現され得る。
【発明の効果】
【００２３】
本開示による例示的な不揮発性メモリ装置は、ＩＣに混載されてデータを保存する複数のメモリセルを有している。このメモリセルを用いて、個体識別情報となるディジタルデータを生成することができるため、面積のオーバヘッドが発生しない。ディジタルデータは安全かつ安定的に生成され、かつ複製が極めて困難であるため、近年大きな脅威となっているサイドチャンネル攻撃に対しても強い耐性を持つＰＵＦ技術を提供できる。
【００２４】
本開示にかかる不揮発性メモリ装置を用いることにより、不揮発性メモリ装置が搭載されるＳｏＣ及びマイコンでの個体識別のためのディジタルデータのビット長を容易に多ビット化することができる。さらに、メモリセルの抵抗値とディジタルデータとの関係を予測させることなく、チップの複製を困難たらしめ、セキュリティーを強化できる。
【図面の簡単な説明】

【００２５】
【図１】図１は、本開示の実施形態にかかる抵抗変化型不揮発性メモリ装置１００の概略構成の一例を示すブロック図である。
【図２】図２は、本開示の実施形態にかかる抵抗変化型不揮発性メモリ装置１００が備えるメモリセルの概略構成の一例を示す断面図である。
【図３】図３は、本開示の実施形態にかかる抵抗変化型不揮発性メモリ装置が備えるメモリセルの抵抗値範囲の一例を示すグラフである。
【図４】図４は、可変状態にあるバイポーラ型抵抗変化素子の特性の一例を示す図である。
【図５】図５は、先行技術文献に開示されている、可変状態にあるユニポーラ型抵抗変化素子の特性の一例を示す模式図である。
【図６】図６は、ディジタルIDセット状態の規格化抵抗値情報と、そのメモリセルのばらつきについての標準正規分布の偏差との関係をプロットした図である。
【図７】図７は、ディジタルＩＤデータ状態に推移させるときに様々な電圧パルス条件で推移させたときのばらつき分布を示す図である。
【図８】図８は、フィラメントの発生数が抵抗変化素子ごとに異なることを示す図である。
【図９】図９は、本開示の実施形態において同一の可変抵抗値範囲にあるメモリセルから連続して抵抗値を読み出した例を示す図である。
【図１０Ａ】図１０Ａは、パーコレーションモデル（ｐｅｒｃｏｌａｔｉｏｎ　ｍｏｄｅｌ）を用いて、フォーミング時における抵抗変化層（例えば局所領域）中のフィラメントの形成をシミュレートした結果の一例を示す図である。
【図１０Ｂ】図１０Ｂは、パーコレーションモデル（ｐｅｒｃｏｌａｔｉｏｎ　ｍｏｄｅｌ）を用いて、フォーミング時における抵抗変化層（例えば局所領域）中のフィラメントの形成をシミュレートした結果の一例を示す図である。
【図１１】図１１は、図３に示すようなディジタルＩＤセット状態に書き込まれた所定のビット数のメモリセル群の抵抗値を放置時間ごとに読み出したときのばらつき範囲と抵抗中央値を示す図である。
【図１２】図１２は、書き込まれたディジタルＩＤデータを図１１に示したような初期の抵抗中央値で抽出したときにおける、エラーレートと放置時間との関係を示す図である。
【図１３】図１３は、ディジタルＩＤデータを生成し、不揮発性メモリ装置１０に書き込む処理フローの一具体例を示すフローチャートである。
【図１４】図１４は、ディジタルＩＤデータを再生する処理フローの一具体例を示すフローチャートである。
【図１５】図１５は、ディジタルＩＤデータの例を示す図である。
【図１６】図１６は、誤り訂正前のデータ誤り率の推移を示す図である。
【図１７】図１７は、読み出し回数と累積エラーレートとの関係を示す図である。
【図１８】図１８は、本開示の不揮発性メモリ装置の具体的な構成例を示すブロック図である。
【図１９】図１９は、本開示の不揮発性メモリ装置１０が備える読み出し回路１１の構成例を示す回路図である。
【図２０Ａ】図２０Ａは、選択されたメモリセルを放電方式にて読み出す場合のタイミングチャートである。
【図２０Ｂ】図２０Ｂは、選択されたメモリセルを充電方式にて読み出す場合のタイミングチャートである。
【図２１】図２１は、本開示の不揮発性メモリ装置１０が備える中央値検出回路２５の構成例を示す図である。
【図２２】図２２は、中央値検出回路２５の一変形例を示す図である。
【図２３】図２３は、中央値検出回路２５が実際に抵抗中央値を算出した結果を示す図である。

【図２４】図２４は、中央値検出回路２５の変形例の一例を示すブロック図である。
【図２５】図２５は、本開示の実施形態の変形例を示すブロック図である。
【図２６】図２６は、メモリセルの規格化メモリセル電流と、本開示の読み出し回路で読み出した抵抗値情報の関係を示す図である。
【図２７】図２７は、本開示の応用例にかかる通信システム５００の構成例を示すブロック図である。
【発明を実施するための形態】
【００２６】
以下、添付の図面を参照しながら、本開示にかかる不揮発性メモリ装置等の実施形態を説明する。本開示にかかる不揮発性メモリ装置は少なくとも１つ以上の閾値で抵抗値を判別することによりデータを記憶する抵抗変化型の不揮発性メモリセルを複数有している。
【００２７】
不揮発性メモリ装置は、たとえば、個体識別情報を生成する機能を備えている。不揮発性メモリ装置では、生成した個体識別情報をもとに、データの暗号化・復号化が行われるとともに、相互間の認証も行われ得る。より具体的には、本開示にかかる不揮発性メモリ装置は、抵抗変化メモリ素子の内容を読み出し、少なくとも部分的にその内容からディジタル識別子を導出する個体識別情報用にチップごとにユニークな固有の乱数データを生成する機能を備えている。これにより、電気的、物理的な複製を妨げることが可能になる。
【００２８】
不揮発性メモリ装置は、たとえばモバイル型電子マネーで利用されるＩＣチップを搭載したカードに搭載され得る。ＩＣチップには、他に論理回路、揮発性メモリ装置、およびマイクロプロセッサーを具備する。これらを用いて暗号化機能、ディジタル署名、およびディジタル認証機能などの各種情報セキュリティー機能を実現する。これらの機能が実行されるときには秘密鍵によるデータ暗号が用いられる。集積回路（ＩＣ）カード内においても前述したように秘密鍵を複製できないように安全に保管することが望ましい。
【００２９】
（発明者らによる検討）
上述の秘密鍵の保管を実現するために前述のＰＵＦ技術が用いられる。ＰＵＦ技術で得られた個体識別情報である乱数のディジタルＩＤデータをデバイス暗号鍵として、秘密鍵を暗号化して不揮発性メモリに保存する。ディジタルＩＤデータは、各ＩＣで異なる乱数であるため、それを用いて暗号化されたデータも各ＩＣで固有のデータ列となる。暗号化された秘密鍵がハッキングなどにより別のＩＣにコピーされたとしても複製できないディジタルＩＤデータがコピーされないので、もとの秘密鍵を不正利用されることがない。
【００３０】
しかしながら、ＩＣカードのような超小型機器には、ＰＵＦ技術を具現化したディジタルＩＤデータ生成のための回路も高度に小型化することが要求される。特にＰＵＦ技術にもとづくディジタルＩＤデータはデータに誤りを含んでいるため誤り訂正回路が必要となり、誤り量が多いと回路規模もそれにともなって大きくなる。すなわち、データ誤り率が低くかつ安定化して極力必要な誤り訂正能力を低減して回路規模の削減が求められる。更に、バッテリーが非搭載の一般的なＩＣカードでは、通信時に得られるワイヤレス給電による電力で短時間のうちに各種機能を実行する必要がある。つまり、ディジタルＩＤデータの生成においても超低消費電力化と生成速度の高速化が同時に求められる。そこで本願発明者らは、かかる要求に応えられるようなディジタルＩＤデータの生成器として、いくつかの先行技術を検討した。
【００３１】
非特許文献２では、先行例である各種ＰＵＦ技術のベンチマークがなされている。特にディジタルＩＤデータの誤り率に着目すると、ＳＲＡＭ　ＰＵＦおよびグリッジＰＵＦは環境変化も考慮すると最悪１５％のデータ誤り率まで悪化するとされている。製造上の歩留まりを考えると２０％以上のデータ誤りを許容する誤り訂正回路が必要であり回路規模がＩＣにとって足かせとなってしまう。また、ＳＲＡＭ　ＰＵＦの場合の最新の研究では

非特許文献１のように極めて低誤りのセルが報告されているが、そのときのメモリセルのサイズは２２ｎｍプロセスを用いているにもかかわらず４．６６μｍ^{2}と極めて大きい。さらに特別なＰＵＦ用のＳＲＡＭセルを設けた場合、素子の特定が容易で耐タンパ性の問題となる。

【００３２】

本願発明者らは、ＰＵＦ技術の特徴を以下のように整理した。ＰＵＦ技術の特徴は、主に次の３点にまとめられると考えられる。

特徴（１）：複製できない物理的な現象から固有のディジタルＩＤデータ（個体識別情報）を得る。

特徴（２）：物理的な現象は動的な回路制御によってのみ得られ、プローブによる直接的な読み取りといった静的な解析によっては必要とされる物理的な現象を得ることはできない。

特徴（３）：得られたディジタルＩＤデータには誤りがあり、誤り訂正回路によってのみ真のＩＤデータが得られる。

【００３３】

さらに本願発明者らは、ＰＵＦ技術によって得られるディジタルＩＤデータに求められる主な性能を以下のようにまとめた。

性能（１）：ディジタルＩＤデータに含まれる誤り箇所はランダムに変化し、真のＩＤデータの予測が困難である。

性能（２）：ＰＵＦ技術によって得られるディジタルＩＤデータは高い乱数性がありＩＣごとにユニークな固有データとなる。

性能（３）：ＰＵＦ技術を採用するとしても、そのために付加すべき回路のオーバーヘッドが小さく、ディジタルＩＤデータを生成する際の消費電力が小さい。

性能（４）：各データビットを生成する生成回路の並列処理数を多くすることで、サイドチャンネル攻撃への耐性がある。

性能（５）：データの誤り率が小さく、誤り訂正回路の回路規模を小さくできる。

性能（６）：ディジタルＩＤデータを生成するタイミングに制約が少なく生成速度が高速である。

【００３４】

上述の特徴及び性能に対し、従来例として知られているＳＲＡＭ－ＰＵＦでは、性能（６）に大きな制約がある。ＳＲＡＭ－ＰＵＦは原理上、電源の投入時にしか得られない。ＩＣ内部のＳＲＡＭは、データキャッシュとして利用するため、ＰＵＦによるＩＤデータ生成時には一旦ＳＲＡＭ内のデータを退避するか、破棄しなければならずシステム動作上に大きな制約が発生する。また、この対策として任意のタイミングで生成するようにするためには非特許文献１のようにＰＵＦ専用のセルを別途設ける必要があり回路のオーバーヘッドが増加するような性能（５）の要件を著しく低下させる。

【００３５】

更にＳＲＡＭを用いたＰＵＦの場合、データ誤りを起こすセルは同一となる傾向がある。つまり、動作が安定なセルと不安定なセルが決まっているため誤りを含んだディジタルＩＤデータのパターンが限られる問題があり、真のディジタルＩＤデータが予測しやすいという課題がある。また、アービターＰＵＦでは、生成タイミングの制約、回路規模、および生成速度などの課題はクリアしているものの、配線遅延およびゲート遅延などのばらつきが大きくないことから、ＩＤデータのユニーク性が乏しい。また、非特許文献２において指摘されているように、データ誤り率も１５％と非常に大きいため誤り訂正回路の規模増加が大きな課題となる。

【００３６】

（発明者らが得た知見）

本願発明者らは、以上のような課題を解決できる可能性のある新規なディジタルＩＤデータ生成方法を鋭意検討した。その結果、本願発明者らは、抵抗変化素子の書き込まれた抵抗値が正規分布にばらつく現象を見出し、抵抗値のばらつきから安定的なディジタルＩ

Ｄデータを生成することに想到した。

【００３７】

本開示の限定的ではない例示的な実施形態は、セキュリティー性において、より優れたディジタルＩＤデータを生成するためのＰＵＦ技術を提供する。

【００３８】

抵抗変化型のメモリ素子は、少なくとも第１の抵抗値状態と、第１の抵抗値状態よりも抵抗値の小さい第２の抵抗値状態とを所定の電圧・極性・幅の電気的なパルス印加により変化する。通常は第１の抵抗値状態と第２の抵抗値状態とにディジタルデータ（たとえば「０」と「１」）を割り当て、情報として保存する。

【００３９】

ここで本願発明者らは、上述の第１の抵抗値状態、第２の抵抗値状態、更に後述する初期状態の何れか１つの状態に属するセル群に着目し、そのセル群に含まれる各セルをその抵抗値に応じて２つに分類した。つまり、そのセル群に含まれる各セルを２値化（ディジタルデータ化）した。各セルの抵抗値はばらついており、そのばらつきを利用して各セルをディジタルデータに変換することで、より安全で安定な暗号技術等に応用可能な、従来にないディジタルＩＤデータの生成方法を提供することが可能となった。これが本願発明者らによって得られた知見の一つである。

【００４０】

また、ディジタルＩＤデータの生成を行う多くの回路要素を、通常の不揮発性メモリ装置として搭載される回路と共通化することが可能となる。そのため、ディジタルＩＤデータの生成のために増加する回路規模を大きく抑制することができ高度に小型化し得る。

【００４１】

さらに、不揮発性メモリ装置のデータ読み出しはメモリアレイの構造上、データを並列処理で複数読み出すため、ディジタルＩＤデータの生成スピードも飛躍的に高められる。同時に、サイドチャンネル攻撃においても並列処理により輻射電磁波が並列数の総和で与えられるため攻撃に対する耐性を高められ得る。

【００４２】

本願発明者らによる知見に基づいて、本開示の一態様の概要は以下のとおりである。

【００４３】

（項目１）本開示の一態様である不揮発性メモリ装置は、可変状態では、異なる複数の電気的信号の印加に応じて抵抗値が複数の抵抗値範囲の間を不揮発的かつ可逆的に遷移する性質を有する複数のメモリセルがアレイ状に配置されたメモリセルアレイと、コントロール信号の入力を受け付ける制御回路と、前記制御回路に入力された前記コントロール信号に基づき、前記複数のメモリセルの少なくとも一部の各々の前記抵抗値に関する複数の抵抗値情報を取得する読み出し回路と、前記読み出し回路によって取得された前記複数の抵抗値情報に基づいて２値化基準値を算出する演算回路と、を備え、前記読み出し回路は、前記２値化基準値に基づいて、前記複数の抵抗値情報の各々、および前記複数のメモリセルの前記少なくとも一部と異なる一部の各々の前記抵抗値に関する複数の抵抗値情報の各々の少なくとも一方に対して２つの値から選択的に１つの値を割り当てることにより個体識別情報を生成する。

【００４４】

（項目２）たとえば、上述の項目１に記載の不揮発性メモリ装置において、前記複数の抵抗値範囲は、第１抵抗値範囲、および前記第１抵抗値範囲より抵抗値が小さい第２抵抗値範囲を含み、前記複数のメモリセルの各々は、初期状態では、前記抵抗値が前記第１および第２抵抗値範囲のいずれとも異なる初期抵抗値範囲にあり、前記複数のメモリセルの各々は、電気的ストレスが印加されることにより、前記初期状態から前記可変状態に変化してもよい。

【００４５】

（項目３）たとえば、上述の項目１または２に記載の不揮発性メモリ装置において、前記演算回路は、前記読み出し回路によって取得された、前記複数の抵抗値情報の中央値を

前記２値化基準値として算出してもよい。

【００４６】

（項目４）たとえば、上述の項目３に記載の不揮発性メモリ装置において、前記読み出し回路は、前記複数の抵抗値情報の各々と、前記演算回路が算出する前記２値化基準値との大小関係に基づいて、複数の第１の誤差情報を取得し、前記演算回路は、前記複数の第１の誤差情報と所定の係数とに基づいて複数の第２の誤差情報を算出する感度調整回路と、前記２値化基準値に前記複数の第２の誤差情報を加えることにより、前記２値化基準値を更新する累積加算回路とを含んでいてもよい。

【００４７】

（項目５）たとえば、上述の項目１から４のいずれかに記載の不揮発性メモリ装置において、前記読み出し回路は、前記複数のメモリセルから第１の所定の数の第１の複数のメモリセルを順次選択し、選択した前記第１の複数のメモリセルの各々の抵抗値に関する第１の複数の抵抗値情報を取得し、前記演算回路は、前記第１の複数の抵抗値情報に基づいて第１の２値化基準値を算出し、前記読み出し回路は、前記複数のメモリセルから前記第１の所定の数と同じ又は異なる第２の所定の数の第２の複数のメモリセルを順次選択し、選択した前記第２の複数のメモリセルの各々の抵抗値に関する第２の複数の抵抗値情報を取得し、前記第１の２値化基準値に基づいて、前記第２の複数の抵抗値情報の各々に対して前記２つの値から選択的に１つの値を割り当てることにより、第１の個体識別情報を生成してもよい。

【００４８】

（項目６）たとえば、上述の項目５に記載の不揮発性メモリ装置において、前記演算回路は、前記第１の２値化基準値に所定のオフセット値を加算または減算して第２の２値化基準値を取得し、前記読み出し回路は、前記第２の２値化基準値に基づいて、前記第２の複数の抵抗値情報の各々に対して前記２つの値から選択的に１つの値を割り当てることにより、第２の個体識別情報を生成してもよい。

【００４９】

（項目７）たとえば、上述の項目５に記載の不揮発性メモリ装置は、誤り訂正およびパリティー生成回路をさらに備え、前記制御回路は、予め、前記演算回路に前記第１の２値化基準値を算出させ、前記読み出し回路に前記第１の個体識別情報を生成させ、前記誤り訂正およびパリティー生成回路に前記第１の個体識別情報からパリティーデータを生成させ、前記パリティーデータを前記メモリセルアレイ内に保存させ、使用時に、前記制御回路は、前記演算回路に前記使用時における前記第１の２値化基準値を算出させ、前記読み出し回路に前記使用時における前記第１の個体識別情報を生成させ、前記誤り訂正およびパリティー生成回路に、前記メモリセルアレイ内に保存された前記パリティーデータを用いて前記使用時における前記第１の個体識別情報を訂正させ、第３の個体識別情報を取得してもよい。

【００５０】

（項目８）たとえば、上述の項目５に記載の不揮発性メモリ装置は、データの乱数性を検定する乱数検定回路をさらに備え、前記乱数検定回路は、前記第１の個体識別情報が所定の乱数の基準を満足しているか否かを検定するとともに検定結果を出力してもよい。

【００５１】

（項目９）たとえば、上述の項目２に記載の不揮発性メモリ装置は、暗号化および復号化を行う暗号処理回路をさらに備え、前記暗号処理回路は、前記個体識別情報を暗号鍵として用いて、入力されたデータを暗号化して暗号化データを生成し、前記暗号化データが前記メモリセルアレイに第１種データおよび第２種データの少なくとも一方として記憶され、前記第１種データは、前記複数のメモリセルの各々が前記初期状態にあるか前記可変状態にあるかを示しており、前記第２種データは、前記複数のメモリセルの各々の前記抵抗値が前記第２の抵抗値範囲にあるか第３の抵抗値範囲にあるかを示していてもよい。

【００５２】

（項目１０）たとえば、上述の項目９に記載の不揮発性メモリ装置において、前記読み

出し回路は、記憶された前記暗号化データ、および前記個体識別情報を読み出して前記暗号処理回路に送信し、前記暗号処理回路は、前記個体識別情報を復号鍵として前記暗号化データを復号化してもよい。

【００５３】

（項目１１）たとえば、上述の項目１から１０のいずれかに記載の不揮発性メモリ装置において、前記複数のメモリセルの各々は、第１電極と、第２電極と、前記第１電極および前記第２電極の間に介在する抵抗変化層を有する抵抗変化素子とを備えていてもよい。

【００５４】

（項目１２）たとえば、上述の項目１１に記載の不揮発性メモリ装置において、前記抵抗変化層は、絶縁体で構成された層を含んでいてもよい。

【００５５】

（項目１３）たとえば、上述の項目１２に記載の不揮発性メモリ装置において、前記抵抗変化層は、前記絶縁体で構成された層を貫く導電パスを有していてもよい。

【００５６】

（項目１４）たとえば、上述の項目１１から１３のいずれかに記載の不揮発性メモリ装置において、前記抵抗変化層は、金属酸化物を含む材料によって構成されていてもよい。

【００５７】

（項目１５）たとえば、上述の項目１１から１３のいずれかに記載の不揮発性メモリ装置において、前記抵抗変化層は、酸素不足型の金属酸化物を含む材料によって構成された層を含んでいてもよい。

【００５８】

（項目１６）たとえば、上述の項目１４または１５に記載の不揮発性メモリ装置において、前記金属酸化物は、遷移金属酸化物およびアルミニウム酸化物の少なくとも一方であってもよい。

【００５９】

（項目１７）たとえば、上述の項目１４または１５に記載の不揮発性メモリ装置において、前記金属酸化物は、タンタル酸化物、ハフニウム酸化物およびジルコニウム酸化物の少なくとも一つであってもよい。

【００６０】

（項目１８）たとえば、上述の項目１３に記載の不揮発性メモリ装置において、前記絶縁体は金属酸化物を含み、前記導電パスは、前記金属酸化物よりも酸素含有率が低い酸素不足型の金属酸化物を有していてもよい。

【００６１】

（項目１９）本開示の一態様である集積回路カードは、上述の項目１に記載の不揮発性メモリ装置と、前記コントロール信号が入力され、前記個体識別情報に関する情報が出力される入出力インタフェース部とを備える。なお、ここで、個体識別情報に関連する情報とは、個体識別情報そのものを含むものとする。

【００６２】

（項目２０）本開示の他の一態様である方法は、上述の項目６に記載の不揮発性メモリ装置が正規の装置であることを認証するための認証方法であって、複数の前記所定のオフセット値を用いて、各オフセット値に応じて異なる個体識別情報を生成して外部装置に保持し、出荷後、前記不揮発性メモリ装置が使用されるときに、外部から入力されたオフセット値を特定するチャレンジデータを利用して個体識別情報を生成し、生成した前記個体識別情報を前記外部装置に送信し、生成した前記個体識別情報と、予め前記外部装置に保持されていた個体識別情報とが一致しているか否かを判断し、一致している場合には、前記不揮発性メモリ装置が正規の装置であるとして認証する、不揮発性メモリ装置の認証方法である。

【００６３】

（項目２１）本開示のさらに他の一態様である方法は、上述の項目５に記載の不揮発性メモリ装置を用いた暗号化方法であって、前記不揮発性メモリ装置は、暗号化および復号

化を行う暗号処理回路をさらに備え、前記不揮発性メモリ装置にデータを入力し、入力された前記データを、前記暗号処理回路が、前記個体識別情報を暗号鍵として用いて暗号化して暗号化データを生成し、前記暗号化データを記憶する、暗号化方法である。

【００６４】

（項目２２）本開示のさらに他の一態様である方法は、項目２０に記載の暗号化方法によって暗号化された暗号化データの復号化方法であって、記憶された前記暗号化データを受け取り、前記不揮発性メモリセルのアレイから、前記個体識別情報を読み出し、前記暗号処理回路が、前記個体識別情報を復号鍵として用いて前記暗号化データを復号化する、復号化方法である。

【００６５】

本開示において、ユニット、デバイスの全部又は一部、又は図１、１８、２１、２２、２４、２５および２７に示されるブロック図の機能ブロックの全部又は一部は、半導体装置、半導体集積回路（ＩＣ）、又はＬＳＩ（ｌａｒｇｅ ｓｃａｌｅ ｉｎｔｅｇｒａｔｉｏｎ）を含む一つ又は一つ以上の電子回路によって実行されてもよい。ＬＳＩ又はＩＣは、一つのチップに集積されてもよいし、複数のチップを組み合わせて構成されてもよい。例えば、記憶素子以外の機能ブロックは、一つのチップに集積されてもよい。ここでは、ＬＳＩまたはＩＣと呼んでいるが、集積の度合いによって呼び方が変わり、システムＬＳＩ、ＶＬＳＩ（ｖｅｒｙ ｌａｒｇｅ ｓｃａｌｅ ｉｎｔｅｇｒａｔｉｏｎ）、若しくはＵＬＳＩ（ｕｌｔｒａ ｌａｒｇｅ ｓｃａｌｅ ｉｎｔｅｇｒａｔｉｏｎ） と呼ばれるかもしれない。 ＬＳＩの製造後にプログラムされる、Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ （ＦＰＧＡ）、又はＬＳＩ内部の接合関係の再構成又はＬＳＩ内部の回路区画のセットアップができるｒｅｃｏｎｆｉｇｕｒａｂｌｅ ｌｏｇｉｃ ｄｅｖｉｃｅも同じ目的で使うことができる。

【００６６】

さらに、ユニット、装置、又は装置の一部の、全部又は一部の機能又は操作は、ソフトウエア処理によって実行することが可能である。この場合、ソフトウエアは一つ又は一つ以上のＲＯＭ、光学ディスク、ハードディスクドライブ、などの非一時的記録媒体に記録され、ソフトウエアが、処理装置（ｐｒｏｃｅｓｓｏｒ）によって実行された場合に、ソフトウエアは、ソフトウエア内の特定の機能を、処理装置（ｐｒｏｃｅｓｓｏｒ）と周辺のデバイスに実行させる。システム又は装置は、ソフトウエアが記録されている一つ又は一つ以上の非一時的記録媒体、処理装置（ｐｒｏｃｅｓｓｏｒ）、及び必要とされるハードウエアデバイス、例えばインターフェース、を備えていても良い。

【００６７】

以下、添付図面を参照しながら、これらの知見に基づく本開示の詳細を説明する。

【００６８】

以下で説明する実施形態は、いずれも一具体例を示すものである。以下の実施形態で示される数値、形状、材料、構成要素、構成要素の配置位置および接続形態、ステップ、ステップの順序などは、あくまで一例であり、本開示を限定するものではない。以下の実施形態における構成要素のうち、本開示の最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。また、図面において、同じ符号が付いたものは、説明を省略する場合がある。また、図面は理解しやすくするために、それぞれの構成要素を模式的に示したもので、形状および寸法比等については正確な表示ではない場合がある。また、製造方法においては、必要に応じて、各工程の順序等を変更でき、かつ、他の公知の工程を追加できる。

【００６９】

（実施の形態１）

（本開示で用いる抵抗変化型不揮発性メモリ装置の概要）

図１は、第１実施形態にかかる抵抗変化型不揮発性メモリ装置１００の概略構成の一例を示すブロック図である。また、図２は、第１実施形態にかかる抵抗変化型不揮発性メモリ装置１００が備えるメモリセルの概略構成の一例を示す断面図である。

【００７０】
図１に示す例では、本実施形態の抵抗変化型不揮発性メモリ装置１００は、少なくともメモリセルアレイ９０と、制御装置９３とを備えている。なお、制御装置は必ずしも抵抗変化型不揮発性メモリ装置の一部である必要はなく、装置外に接続された制御装置を用いて、以下に説明する動作が行われてもよい。
【００７１】
メモリセルアレイ９０は、複数のメモリセル９１がアレイ状に配置された構成を有する。
【００７２】
制御装置９３は、抵抗値が同一の抵抗値状態にあるメモリセル９１群から複数の抵抗値情報を取得し、抵抗値情報のばらつきの中央値を検出する。検出された中央値に基づき、同一の抵抗値状態にあるメモリセル群の各メモリセルに更に０または１のディジタルデータのいずれの値を割り当てるかを判定し、ディジタルＩＤデータを生成する。同一の抵抗値状態とは、ディジタル情報の１状態を割り当てるために用いる１つの抵抗値範囲のことをいう。
【００７３】
一般に、不揮発性メモリ装置において、メモリセルがもつ物理量に、例えばディジタル量の最小単位である２値情報を割り当てるとき、その物理量が、所定の閾値以上のある範囲に属するか、または所定の閾値未満のある範囲に属するかによって、２値情報のいずれを割り当てるかを変える。近年の不揮発性メモリ装置には誤り訂正回路が具備される。誤り訂正回路の誤り訂正処理によれば、一部のメモリセルの物理量が２値情報を割り当てるために予め想定された範囲に入らない場合であっても、その物理量から得られる２値情報は正しく復元される。これは、ディジタルＩＤデータをなすメモリセル群のうちの一部が同一の抵抗値範囲になくても良いことを意味する。本明細書の定義として、ディジタルＩＤデータをなすメモリセル群の少なくとも半数より多いメモリセルが同一の抵抗値状態にあれば、本開示における諸機能を達成できるものとする。
【００７４】
抵抗変化型不揮発性メモリ装置１００の個体識別情報として利用されるディジタルＩＤデータを生成する際には、各抵抗値が、同一の抵抗値範囲に属している複数の不揮発性メモリセルを利用する。当該複数の不揮発性メモリセルにはユーザデータは書き込まれない。つまり、抵抗値の書換えは行われない。各不揮発性メモリセルの抵抗値は、予め定められた抵抗値範囲に固定化されている。各抵抗値は同一の抵抗値範囲内でばらついており、そのばらつきが、抵抗変化型不揮発性メモリ装置１００の固有の情報になる。「抵抗値範囲」の詳細は、後述する図３を参照しながら詳細に説明する。
【００７５】
「抵抗値情報」とは、抵抗値と相関関係を有する情報であり、抵抗値そのものであってもよいし、抵抗値に応じて増減する値であってもよい。抵抗値に応じて増減する値としては、例えば後述するような、メモリセルに並列に接続されたコンデンサに蓄積された電荷が選択されたメモリセルを介して放電される放電時間、または逆にディスチャージされたコンデンサに所定の定電流を流し所定のレベルまでチャージされる充電時間でもよい。該放電時間または充電時間は、所定のクロック周期でカウントされたカウント値等であってもよい。なお、コンデンサは素子であることには限定されず、例えば配線などの寄生容量でもよい。
【００７６】
抵抗値情報は、所定の分解能のセンスアンプによって測定された値であってもよい。あるいは、抵抗値情報は、センスアンプによって測定された値が、閾値によって区分けされた複数の抵抗値範囲のいずれに該当するかを判定することによって得られた値であってもよい。その場合、複数の抵抗値範囲のそれぞれは、一部の抵抗値範囲が、さらに細かく区分けされたものであってもよい。
【００７７】

図２に示す例では、メモリセル９１が備える抵抗変化素子１２０が、下地層１２２と、第１電極１２４と、抵抗変化層１２６と、第２電極１２８とを備えている。それぞれのメモリセルには、特定のメモリセルを選択するためのトランジスタまたはダイオードなどの選択素子が接続されてもよいが、図２においては図示せずに省略した。

【００７８】

メモリセル９１は、異なる複数の電気的信号が印加されることによって、抵抗値が複数の可変抵抗値範囲の間を可逆的に遷移する可変状態を取りうる性質を有する。

【００７９】

図３は、第１実施形態にかかる抵抗変化型不揮発性メモリ装置が備えるメモリセルの抵抗値範囲の一例を示すグラフである。図３に例示するように、メモリセル９１は、少なくとも可変状態と初期状態の２つの状態を備えてもよい。

【００８０】

「初期状態」とは、抵抗値が可変抵抗値範囲のいずれとも重複しない初期抵抗値範囲にある状態をいう。初期状態にあるメモリセルは、フォーミングが行われない限り可変状態とならない。「フォーミング」とは、所定の電気的ストレスをメモリセルに印加して、メモリセルの抵抗値が複数の可変抵抗値範囲の間を可逆的に遷移する状態へと、メモリセルを変化させることをいう。

【００８１】

フォーミングのために印加される電気的ストレス（フォーミングストレス）は、例えば、所定の電圧と時間幅を有する電気的パルスである場合もあるし、複数の電気的パルスを組み合わせたものである場合もある。フォーミングストレスは累積的なストレスであってもよい。その場合、ストレスの累積量が所定量を超えたときに、メモリセル９１（図１）は初期状態から可変状態に遷移する。

【００８２】

本実施の形態では、メモリセル９１は、製造後、フォーミングをしなければ抵抗値が複数の可変抵抗値範囲の間を可逆的に遷移する状態とならないような性質を有しているとする。つまり、半導体プロセス等により製造した後、フォーミングストレスが印加される前の抵抗変化素子は、初期状態にあるとして説明する。

【００８３】

しかしながら、この性質は一例であり必須ではない。メモリセル９１は、初期状態を取りうる素子でなくてもよく、たとえば、可変状態のみを有する、いわゆるフォーミングレスの素子であってもよい。

【００８４】

［抵抗変化素子の構成］

図２に示す例において、抵抗変化素子１２０は、第１電極１２４と第２電極１２８との間に抵抗変化層１２６が介在する構成を有する。抵抗変化層１２６は、例えば金属酸化物、より詳細には例えば遷移金属酸化物で構成することができる。可変状態にあるメモリセル９１の抵抗変化素子１２０は、第１電極１２４と第２電極１２８との間に電気的信号が印加されることによって、第１電極１２４と第２電極１２８との間の抵抗値が複数の可変抵抗値範囲の間を可逆的に遷移する性質を有する。

【００８５】

初期状態にあるメモリセル９１の抵抗変化素子１２０の抵抗変化層１２６は、第１電極１２４と第２電極１２８との間を絶縁していてもよい。絶縁とは、具体的には２ＭΩ以上とすることができる。抵抗変化素子１２０の抵抗変化層１２６は、絶縁体から構成された層を備えていてもよい。絶縁体とは、具体的には抵抗率が３０Ω・ｍ以上の材料とすることができる。抵抗変化素子１２０の抵抗変化層１２６が絶縁体から構成されることにより、初期状態のメモリセルの抵抗特性を安定して維持することができる。

【００８６】

電気的信号の印加によって抵抗値が変化する可変状態の抵抗変化素子と異なり、初期抵抗値範囲は、抵抗変化素子の材料、大きさ、形状、及び製造条件等によってある程度調整

することができる。例えば、特に抵抗変化層１２６が積層構造である場合、酸素濃度の高い層の厚み、形成時の酸素濃度によって任意に調整可能であるが、個別のメモリセルごとには調整できない。

【００８７】

上記のような初期状態は、電気的信号の印加によって抵抗値が遷移する可変状態に比べて、安定している。そのため、初期状態と可変状態との差異を利用して、データを安定して保持することができる。

【００８８】

初期抵抗値範囲は、例えば、初期状態にある素子に、可変状態にある素子の抵抗値を複数の可変抵抗値範囲の間で変化させる電気的信号およびフォーミングストレスのいずれよりも小さな電圧を素子に印加して読み出したときに得られる抵抗値の範囲としうる。

【００８９】

なお、フォーミングストレスは、メモリセル９１に印加する電圧振幅の量、パルスの幅、および累積印加時間等で決定され、それぞれの値はメモリセルアレイ９０内のメモリセル９１毎に異なりうる。なお、累積印加時間とは、例えば、抵抗状態が初期状態から可変状態に変化するまでに印加される電気的パルスのパルス幅の合計を意味する。このためフォーミングストレスとして最低限必要となる電気的ストレスを規定するパラメータの具体的な値は、対象となるメモリセル９１毎に素子が可変状態へと変化するまでに印加された電気的ストレスの電圧、パルス幅、および累積印加時間等の値であって、絶対的な固定値ではなく所定のばらつきをもつ値である。そして、このような素子ごとのフォーミングにおける電気的ストレスのばらつきは、その後の可変抵抗値範囲にある各セルの抵抗値のばらつきの要因となると推察され、素子ごとに人為的に制御することが困難である。

【００９０】

なお、フォーミングストレスは、可変状態にあるメモリセルの抵抗値を複数の可変抵抗値範囲の間で可逆的に変化させるために印加される電気的信号よりも強いのが一般的である。具体的には、フォーミングストレスは、電圧の絶対値、パルス幅、および累積印加時間の少なくともいずれかにおいて、可変状態にあるメモリセルの抵抗値を変化させるために印加される電気的信号よりも大きいものとしうる。

【００９１】

可変状態において、電圧およびパルス幅等は異なるが同極性の電気的信号を印加することにより抵抗値が変化するものをユニポーラ型抵抗変化素子とよぶ。より具体的には、例えば、第２電極１２８から第１電極１２４に電流が流れる向きに＋２Ｖで１μＳｅｃの幅の電気的信号（電気的パルス）を印加すると抵抗変化素子の抵抗値が所定の高抵抗レベル（第１抵抗値範囲：ＨＲレベルともいう）に変化し、同様に第２電極１２８から第１電極１２４に電流が流れる向きに＋４Ｖで５０ｎＳｅｃの幅の電気的信号を印加すると抵抗変化素子の抵抗値が所定の低抵抗レベル（第２抵抗値範囲：ＬＲレベルともいう）に変化する。このような、同極性の電気的信号を印加することにより抵抗値が可逆的に変化するものを、ユニポーラ型抵抗変化素子という。

【００９２】

一方、可変状態において、異なる極性の電気的信号を印加することで抵抗値が変化するものをバイポーラ型抵抗変化素子とよぶ。より具体的には第２電極１２８から第１電極１２４に電流が流れる向きに＋２Ｖで５０ｎＳｅｃの幅の電気的信号を印加すると抵抗変化素子の抵抗値が所定の高抵抗レベル（第１抵抗値範囲：ＨＲレベルともいう）に変化し、逆に第１電極１２４から第２電極１２８に電流が流れる向きに＋２Ｖで５０ｎＳｅｃの幅の電気的信号を印加すると抵抗変化素子の抵抗値が所定の低抵抗レベル（第２抵抗値範囲：ＬＲレベルともいう）に変化する。このような、逆極性の電気的信号を印加することにより抵抗値が可逆的に変化するものを、バイポーラ型抵抗変化素子という。

【００９３】

当然であるが、バイポーラ型抵抗変化素子において、例えば動作を安定にするために、極性のみならず、ＨＲレベルに変化させる場合（高抵抗化ともいう）に印加する電気的信

号と、ＬＲレベルに変化させる場合（低抵抗化ともいう）に印加する電気的信号とで、パルス幅または電圧の絶対値を異ならせてもよい。

【００９４】

抵抗変化層１２６は金属酸化物から構成されてもよい。抵抗変化層１２６は、酸素不足型の金属酸化物から構成された層を備えてもよい。抵抗変化層１２６を構成する金属酸化物は、遷移金属酸化物およびアルミニウム酸化物の少なくともいずれか一方であってもよいし、タンタル酸化物、鉄酸化物、ハフニウム酸化物およびジルコニウム酸化物の少なくともいずれかであってもよい。

【００９５】

ユニポーラ型抵抗変化素子の抵抗変化層の材料には、チタン（Ｔｉ）酸化物、ニッケル（Ｎｉ）酸化物、アルミニウム（Ａｌ）酸化物等を用いることができる。一方、バイポーラ型抵抗変化素子の抵抗変化層の材料には、タンタル（Ｔａ）酸化物、ハフニウム（Ｈｆ）酸化物、アルミニウム（Ａｌ）酸化物、鉄（Ｆｅ）酸化物等を用いることができる。

【００９６】

同じ材料の酸化物を用いた場合でも、電極材料との組合せおよび酸化物の積層構造等により、ユニポーラ型抵抗変化素子およびバイポーラ型抵抗変化素子の両方が得られる場合もある。なお、抵抗変化層の材料にタンタル酸化物を用いると、抵抗変化素子が良好な特性を示すので、本実施形態において特に詳細に例示する。

【００９７】

第１電極１２４および第２電極１２８の材料には、例えば、イリジウム（Ｉｒ）、白金（Ｐｔ）、タングステン（Ｗ）、銅（Ｃｕ）、アルミニウム（Ａｌ）、窒化チタン（ＴｉＮ）、窒化タンタル（ＴａＮ）および窒化チタンアルミニウム（ＴｉＡｌＮ）等を用いることができる。

【００９８】

なお、図２に示す例では、第１電極１２４が第２電極１２８に比べ大面積となっているが、これに限定されるものでない。例えば、第１電極１２４を配線の一部に適用するなど、半導体プロセスにあわせ適宜、最適な形状にされうる。下地層１２２も同様に半導体プロセスに応じて適宜に省略または変更されうる。

【００９９】

抵抗変化層１２６は、第１電極１２４に接続する第１抵抗変化層と、第２電極１２８に接続する第２抵抗変化層の少なくとも２層を積層して構成されてもよい。

【０１００】

第１抵抗変化層は、酸素不足型の第１金属酸化物で構成され、第２抵抗変化層は、第１金属酸化物よりも酸素不足度が小さい第２金属酸化物で構成されうる。第２抵抗変化層は、絶縁体から構成された層であってもよい。第２抵抗変化層中には、電気パルスの印加に応じて酸素不足度が可逆的に変化する微小な局所領域が形成されている。局所領域は、酸素欠陥サイトから構成されるフィラメントを含むと考えられる。局所領域は、第２抵抗変化層を貫く導電パスであってもよい。絶縁体が金属酸化物から構成され、導電パスは、絶縁体よりも酸素含有率が低い酸素不足型の金属酸化物から構成されていてもよい。

【０１０１】

「酸素不足度」とは、金属酸化物において、その化学量論的組成（複数の化学量論的組成が存在する場合は、そのなかで最も抵抗値が高い化学量論的組成）の酸化物を構成する酸素の量に対し、不足している酸素の割合をいう。化学量論的組成の金属酸化物は、他の組成の金属酸化物と比べて、より安定でありかつより高い抵抗値を有している。

【０１０２】

例えば、金属がタンタル（Ｔａ）の場合、上述の定義による化学量論的組成の酸化物はTa_2O_5であるので、$TaO_{2.5}$と表現できる。$TaO_{2.5}$の酸素不足度は０％であり、$TaO_{1.5}$の酸素不足度は、酸素不足度＝（２．５－１．５）／２．５＝４０％となる。また、酸素過剰の金属酸化物は、酸素不足度が負の値となる。なお、本明細書中では、特に断りのない限り、酸素不足度は正の値、０、負の値も含むものとして説明する。

【０１０３】
酸素不足度の小さい酸化物は化学量論的組成の酸化物により近いため抵抗値が高く、酸素不足度の大きい酸化物は酸化物を構成する金属により近いため抵抗値が低い。
【０１０４】
「酸素含有率」とは、総原子数に占める酸素原子の比率である。例えば、Ta_2O_5の酸素含有率は、総原子数に占める酸素原子の比率（Ｏ／（Ｔａ＋Ｏ））であり、７１．４ａｔｍ％となる。したがって、酸素不足型のタンタル酸化物は、酸素含有率は０より大きく、７１．４ａｔｍ％より小さいことになる。例えば、第１金属酸化物を構成する金属と、第２金属酸化物を構成する金属とが同種である場合、酸素含有率は酸素不足度と対応関係にある。すなわち、第２金属酸化物の酸素含有率が第１金属酸化物の酸素含有率よりも大きいとき、第２金属酸化物の酸素不足度は第１金属酸化物の酸素不足度より小さい。
【０１０５】
抵抗変化層を構成する金属は、タンタル以外の金属を用いてもよい。抵抗変化層を構成する金属としては、遷移金属、およびアルミニウム（Ａｌ）の少なくともいずれかを用いることができる。遷移金属としては、タンタル（Ｔａ）、チタン（Ｔｉ）、ハフニウム（Ｈｆ）、ジルコニウム（Ｚｒ）、ニオブ（Ｎｂ）、タングステン（Ｗ）、ニッケル（Ｎｉ）、鉄（Ｆｅ）等を用いることができる。遷移金属は複数の酸化状態をとることができるため、異なる抵抗状態を酸化還元反応により実現することが可能である。
【０１０６】
例えば、ハフニウム酸化物を用いる場合、第１金属酸化物の組成をHfO_xとした場合にｘが０．９以上１．６以下であり、かつ、第２金属酸化物の組成をHfO_yとした場合にｙがｘの値よりも大である場合に、抵抗変化層の抵抗値を安定して高速に変化させることができる。この場合、第２金属酸化物の膜厚は、３～４ｎｍとしてもよい。
【０１０７】
また、ジルコニウム酸化物を用いる場合、第１金属酸化物の組成をZrO_xとした場合にｘが０．９以上１．４以下であり、かつ、第２金属酸化物の組成をZrO_yとした場合にｙがｘの値よりも大である場合に、抵抗変化層の抵抗値を安定して高速に変化させることができる。この場合、第２金属酸化物の膜厚は、１～５ｎｍとしてもよい。
【０１０８】
第１金属酸化物を構成する第１金属と、第２金属酸化物を構成する第２金属とは、異なる金属を用いてもよい。この場合、第２金属酸化物は、第１金属酸化物よりも酸素不足度が小さい、つまり抵抗が高くてもよい。このような構成とすることにより、抵抗変化時に第１電極１２４と第２電極１２８との間に印加された電圧は、第２金属酸化物に、より多くの電圧が分配され、第２金属酸化物中で発生する酸化還元反応をより起こしやすくすることができる。
【０１０９】
また、第１抵抗変化層となる第１金属酸化物を構成する第１金属と、第２抵抗変化層となる第２金属酸化物を構成する第２金属とを、互いに異なる材料を用いる場合、第２金属の標準電極電位は、第１金属の標準電極電位より低くてもよい。標準電極電位は、その値が高いほど酸化しにくい特性を表す。これにより、標準電極電位が相対的に低い第２金属酸化物において、酸化還元反応が起こりやすくなる。なお、抵抗変化現象は、抵抗が高い第２金属酸化物中に形成された微小な局所領域中で酸化還元反応が起こってフィラメント（導電パス）が変化することにより、その抵抗値（酸素不足度）が変化することにより発現すると考えられる。
【０１１０】
例えば、第１金属酸化物に酸素不足型のタンタル酸化物（TaO_x）を用い、第２金属酸化物にチタン酸化物（TiO_2）を用いることにより、安定した抵抗変化動作が得られる。チタン（標準電極電位＝－１．６３ｅＶ）はタンタル（標準電極電位＝－０．６ｅＶ）より標準電極電位が低い材料である。このように、第２金属酸化物に第１金属酸化物より標準電極電位が低い金属の酸化物を用いることにより、第２金属酸化物中でより酸化還

元反応が発生しやすくなる。その他の組み合わせとして、高抵抗層となる第２金属酸化物にアルミニウム酸化物（Al_2O_3）を用いることができる。例えば、第１金属酸化物に酸素不足型のタンタル酸化物（TaO_x）を用い、第２金属酸化物にアルミニウム酸化物（Al_2O_3）を用いてもよい。

【０１１１】

積層構造の抵抗変化層における抵抗変化現象は、いずれも抵抗が高い第２金属酸化物中に形成された微小な局所領域中で酸化還元反応が起こって、局所領域中のフィラメント（導電パス）が変化することにより、その抵抗値が変化すると考えられる。

【０１１２】

つまり、第２金属酸化物に接続する第２電極１２８に、第１電極１２４を基準にして正の電圧を印加したとき、抵抗変化層中の酸素イオンが第２金属酸化物側に引き寄せられる。これによって、第２金属酸化物中に形成された微小な局所領域中で酸化反応が発生し、酸素不足度が減少する。その結果、局所領域中のフィラメントが繋がりにくくなり、抵抗値が増大すると考えられる。

【０１１３】

逆に、第２金属酸化物に接続する第２電極１２８に、第１電極１２４を基準にして負の電圧を印加したとき、第２金属酸化物中の酸素イオンが第１金属酸化物側に押しやられる。これによって、第２金属酸化物中に形成された微小な局所領域中で還元反応が発生し、酸素不足度が増加する。その結果、局所領域中のフィラメントが繋がりやすくなり、抵抗値が減少すると考えられる。

【０１１４】

酸素不足度がより小さい第２金属酸化物に接続されている第２電極１２８は、例えば、白金（Ｐｔ）、イリジウム（Ｉｒ）、パラジウム（Ｐｄ）など、第２金属酸化物を構成する金属および第１電極１２４を構成する材料と比べて標準電極電位が高い材料で構成する。また、酸素不足度がより高い第１金属酸化物に接続されている第１電極１２４は、例えば、タングステン（Ｗ）、ニッケル（Ｎｉ）、タンタル（Ｔａ）、チタン（Ｔｉ）、アルミニウム（Ａｌ）、窒化タンタル（ＴａＮ）、窒化チタン（ＴｉＮ）など、第１金属酸化物を構成する金属と比べて標準電極電位が低い材料で構成してもよい。標準電極電位は、その値が高いほど酸化しにくい特性を表す。

【０１１５】

すなわち、第２電極１２８の標準電極電位Ｖ２、第２金属酸化物を構成する金属の標準電極電位Ｖｒ２、第１金属酸化物を構成する金属の標準電極電位Ｖｒ１、および、第１電極１２４の標準電極電位Ｖ１は、Ｖｒ２＜Ｖ２、およびＶ１＜Ｖ２なる関係を満足してもよい。さらには、Ｖ２＞Ｖｒ２、およびＶｒ１≧Ｖ１の関係を満足してもよい。

【０１１６】

上記の構成とすることにより、第２電極１２８と第２金属酸化物の界面近傍の第２金属酸化物中において、選択的に酸化還元反応が発生し、安定した抵抗変化現象が得られる。

【０１１７】

より好適には、抵抗変化層１２６は、TaO_x（但し、$0 \leqq x < 2.5$）で表される組成を有する第１抵抗変化層と、TaO_y（但し、$x < y < 2.5$）で表される組成を有する第２抵抗変化層とが積層された積層構造を少なくとも有している。他の層、例えばタンタル酸化物以外の金属酸化物で構成される第３抵抗変化層等を適宜配置しうることは言うまでもない。

【０１１８】

ここで、TaO_xは、$0.8 \leqq x < 1.9$を満足してもよく、TaO_yは、$2.1 \leqq y < 2.5$を満足してもよい。第２タンタル含有層の厚みは、１ｎｍ以上８ｎｍ以下であってもよい。酸素不足度の異なる層を積層することにより、バイポーラ型における抵抗変化の方向が決定できる。例えば、第２抵抗変化層を第２電極１２８側に、第１抵抗変化層を第１電極１２４側に配置する。かかる構成によれば、第２電極１２８側から第１電極１２４側に電流を流す向きの電圧印加で高抵抗化し、逆向きに電流を流す向きの電圧印加で低抵

抗化する。当然ながら第２抵抗変化層を第１電極１２４に接し、第１抵抗変化層を第２電極１２８に接するように構成すると、抵抗変化と電圧印加の向きの関係が逆転する。

【０１１９】

［可変状態における抵抗変化素子の特性］

図４は、可変状態にあるバイポーラ型抵抗変化素子の特性の一例を示す図である。図４の素子の構成は、第１電極１２４の材料がＴａＮ、第２電極１２８の材料がＩｒ、抵抗変化層１２６の材料がTaO_x（但し、０＜ｘ＜２．５）で表される組成を有する第１タンタル含有層と、TaO_y（但し、ｘ＜ｙ）で表される組成を有する第２タンタル含有層とが積層された積層構造を少なくとも有して、第１タンタル含有層が第１電極１２４に接し、第２タンタル含有層が第２電極１２８に接している。TaO_xは、０．８≦ｘ≦１．９を満足し、TaO_yは、２．１≦ｙ≦２．５を満足するように製造されている。第２タンタル含有層の厚みは、８ｎｍ以下であり、抵抗変化層１２６全体の厚みは５０ｎｍ以下である。各電極への接触面積は図３の測定に用いた抵抗変化素子と等しい。

【０１２０】

図４の横軸は印加する電気的信号の電圧を示し、縦軸に電気的信号を印加した後の抵抗変化素子の抵抗値（抵抗値は読み出し電圧ＶＲを印加したときの電流から算出）を示している。図中のスタートの位置から、正極性側に電圧レベルを徐々にあげて行くと、印加電圧が＋１．１Ｖを超えたときから徐々に抵抗値が上昇し、印加電圧が＋２．０Ｖでは約１００ｋΩに達している。逆に負極性側に電圧レベルを徐々に下げて行き、－１．１Ｖを超えると約１０ｋΩ程度に低抵抗化して、スタートの抵抗値に戻っていることがわかる。このとき抵抗変化層１２６は、第２抵抗変化層を第２電極１２８側に、第１抵抗変化層を第１電極１２４側に配置している。第２電極１２８から第１電極１２４に電流が流れるような電気的信号の印加を正極性印加と定義する。正極性印加では、抵抗変化素子１２０はＨＲレベルに変化する。また、逆向きに電流が流れる印加を負極性印加と定義する。負極性印加では、抵抗変化素子１２０はＬＲレベルに変化する。ＬＲからＨＲに変化せしめる電圧レベルを高抵抗化電圧（ＶＨ）とし、ＨＲからＬＲに変化せしめる電圧レベルを低抵抗化電圧（ＶＬ）とすると、図４の場合では、その絶対値が｜ＶＨ｜＝｜ＶＬ｜＝２．０Ｖ程度あれば、共通の電源電圧を用いて十分に低抵抗状態と高抵抗状態を可逆的に推移できることがわかる。

【０１２１】

図５は、IEDM Technical Digest. 13-15 Dec. 2004, p.587に開示されている、可変状態にあるユニポーラ型抵抗変化素子の特性の一例を示す模式図である。当該論文に示される通り、ＮｉＯ、TiO_2、HfO_2、ZrO_2から構成された抵抗変化層を有する抵抗変化素子がユニポーラ特性を示すこと、及び、それらの遷移金属酸化物から構成された抵抗変化層が、製造直後には絶縁体であって、かつフォーミングストレスを与えるプロセスによって導電パスが形成されて可変状態に遷移することが知られている。

【０１２２】

抵抗変化層の材料と電極の組合せ、および抵抗変化材料にドープする不純物の材料等によっては、正電圧側でも負電圧側でも対称的にユニポーラ型で抵抗変化する素子が得られる。図５は、かかる素子の特性を例示する。

【０１２３】

図に示す例では、バイアス電圧の絶対値が０．５Ｖを超えると素子がリセット状態、つまりＨＲレベルへと推移し、バイアス電圧の絶対値１．０Ｖを超えると素子がセット状態、つまりＬＲレベルへと推移する。かかる素子では、同じ極性で電圧の異なる電気的信号を印加することで、２個の抵抗状態の間を可逆的に遷移させることが可能である。しかし、図５のような特性のユニポーラ型抵抗変化素子であれば、＋０．５Ｖ以上＋１Ｖ未満の正極性の電気的信号を印加することで高抵抗化させ、－１Ｖ以下（絶対値が１Ｖ以上）の負極性の電気的信号を印加することで低抵抗化させるように制御すれば、バイポーラ型抵抗変化素子として利用することもできる。本実施形態では、バイポーラ型もユニポーラ型も、いずれのタイプでも使用可能である。

【０１２４】
抵抗変化素子は、印加する電気的信号の電圧（絶対値）、幅、および回数等の組合せにより、抵抗値が３以上の可変抵抗値範囲の間を可逆的に遷移する多値メモリとして利用されてもよい。例えば、抵抗変化層としてタンタル酸化物を用いた素子は、良好な特性を示し、多値メモリへ応用されうる。
【０１２５】
このような抵抗変化素子（ＲｅＲＡＭ素子）の抵抗変化は、第２電極１２８と第１電極１２４とを電気的に接続する導電性パスが抵抗変化層１２６内に発生することによって発生することを断面解析によって観察した。このとき導電性パスは直径３０～１０ｎｍ以下であり、最先端の微細な半導体プロセスで作製される配線幅より更に小さいことを見出した。すなわち上記で説明した抵抗変化素子の特性は、リソグラフィーによる加工の限界とされる超微細半導体プロセスで製造されても同様な安定した抵抗変化の特性を維持できる。
【０１２６】
また、抵抗変化素子（ＲｅＲＡＭ素子）の抵抗変化層を形成するプロセスには数百℃を超えるような高温処理が必要ない。このため、加熱プロセスによってＣ－ＭＯＳトランジスタへの特性を劣化させることがない。すなわち抵抗変化素子は、フラッシュメモリなどのフローティングゲート型トランジスタを用いるメモリ素子に比べ半導体プロセスとの親和性が非常に優れ、製造プロセスの微細化が進んでも抵抗変化の信頼性が低下することがない特徴を有している。そのため、例えば、コントローラ等のロジック回路と抵抗変化素子とが同一チップ上に形成される場合であっても、ロジック回路の特性への影響を抑えつつ抵抗変化素子を形成することができる。また、ロジック回路とプロセスを共通化することにより、製造コストを低減することができる。
【０１２７】
可変状態とは、異なる複数の電気的信号が印加されることによって、抵抗値が複数の可変抵抗範囲の間を可逆的に遷移できる状態をいう。
【０１２８】
メモリセルアレイ９０が備える複数のメモリセル９１は、可変状態のメモリセルと、初期状態のメモリセルと、を含んでもよい。メモリセルアレイ９０では、各メモリセル９１が初期状態にあるか可変状態にあるかの違いを利用してデータが記録されていてもよい。
【０１２９】
メモリセルアレイ９０では、後述する第１種データ、第２種データおよび第３種データの何れかを利用してデータが各メモリセル９１に記録されうる。メモリセルアレイ９０は、第３種データが記録されたメモリセル９１と、第１種データおよび第２種データの何れか、または両方が記録されたメモリセル９１を含んでいてもよい。
【０１３０】
製造直後のメモリセル９１の抵抗値が、初期抵抗値範囲に入る一方で可変抵抗値範囲に入ることがないように、初期抵抗値範囲および可変抵抗値範囲は設定されうる。可変状態に変化した後のメモリセル９１の抵抗値が、可変抵抗値範囲に入る一方で初期抵抗値範囲には入ることがないように、初期抵抗値範囲および可変抵抗値範囲は設定されうる。抵抗変化素子の不揮発性記憶素子を備えるメモリセルが、かかる特性を備え得ることは周知である。公知の様々な材料を用いて、かかる特性を備えるメモリセル９１を製造することができる。
【０１３１】
初期状態のメモリセル９１は、可変状態に変化させるような電気的ストレスであるフォーミングストレスではない何らかの電気的ストレスを受けた状態を含む。初期状態のメモリセル９１は、製造直後の抵抗値から、フォーミングストレスではない何等かの電気的ストレスを受ける等して抵抗値が、初期抵抗値範囲内で変化した状態を含む。
【０１３２】
制御装置９３は、選択されたメモリセル９１が初期状態にあるか可変状態にあるかを判

定することによって記録されたデータを読み出すことができるように構成されていてもよい。

【０１３３】

図３に示した例における素子の構成は、第１電極１２４の材料がＴａＮ（窒化タンタル）、第２電極１２８の材料がＩｒ（イリジウム）、抵抗変化層１２６の材料がタンタル酸化物、抵抗変化層１２６全体の厚さが５０ｎｍ以下で、酸素濃度の異なる２層の積層構造を有する。第１電極１２４に接する層が酸素濃度の低い層であって、組成をTaO_xとすると$0<x<2.5$である。第２電極１２８に接する層が酸素濃度の高い層であって、組成をTaO_yとすると$y \geqq 2.1$であり、厚さが５．５ｎｍ程度である。第１電極１２４と抵抗変化層１２６との接触面および第２電極１２８と抵抗変化層１２６との接触面の面積が$0.25\mu m^2$以下である。

【０１３４】

次に、メモリセルの状態の変化を具体的に説明する。以下では「ＨＲ状態」および「ＬＲ状態」という語を用いる。「ＨＲ状態」とは、ＨＲパルス（高抵抗化パルス）を印加されたメモリセルの状態をいう。「ＬＲ状態」とは、ＬＲパルス（低抵抗化パルス）を印加されたメモリセルの状態をいう。

【０１３５】

フォーミングストレスは、電圧が＋３．５Ｖ、パルス幅が５μＳｅｃのパルスを累積的に印加する。セルごとに適切な累積パルスを印加することで、図３の（１）初期状態にあったメモリセルは、（２）初回ＨＲ状態に推移する。初回ＨＲ状態に推移した後は、低抵抗化パルス（素子の抵抗値を第１抵抗値範囲から第２抵抗値範囲へと変化させるためのパルス：第２電気的信号）は、電圧が－２．４Ｖ、パルス幅が５０ｎＳｅｃを印加する。これにより（３）ディジタルＩＤセット状態に推移する。ディジタルＩＤセット状態にあるセルに更に高抵抗化パルス（素子の抵抗値を第２抵抗値範囲から第１抵抗値範囲へと変化させるためのパルス：第１電気的信号）である電圧が＋１．８Ｖ、パルス幅が５０ｎＳｅｃのパルスを印加することで第１抵抗値範囲へと変化する。これ以降のメモリセルは可変状態のセルとなる。すなわち、本開示のディジタルＩＤデータに用いる場合は図３の（３）ディジタルＩＤセット状態でとどめて利用する。なお、本開示の例では図３（３）の状態をディジタルＩＤデータとして利用することを例示するが、（１）の初期状態にも複製のできない製造上のばらつきがもたらす抵抗値のばらつきがあるので、後述する方式を応用して利用可能である。

【０１３６】

なお、パルス印加の工程は上述の手順に限定されない。例えば（３）のディジタルＩＤセット状態は、メモリ素子が可変状態となった以降に複数回第１電気的信号と第２電気的信号を交互に繰返しＨＲ状態とＬＲ状態を複数回遷移させ、最終的にＬＲ状態にして工程を終了し最後にセットされた状態を（３）のディジタルＩＤセット状態としてもよい。

【０１３７】

図６を参照しながら、図３の（３）ディジタルＩＤセット状態の抵抗値ばらつきの特性を説明する。

【０１３８】

図６は、（３）ディジタルＩＤセット状態の規格化抵抗値情報と、そのメモリセルのばらつきについての標準正規分布の偏差との関係をプロットした図である。

【０１３９】

図６に示すように、メモリセルの正規分布は抵抗値情報に対してほぼ直線に分布している。このことから、分布のばらつきは極めてランダムな分布現象であることが示される。図６で示すようにばらつき分布の中央値の抵抗値情報（中央抵抗値または２値化基準値ともいう）を検出し、中央抵抗値との大小関係を比較してディジタルデータの１または０に割り当てる。そして抵抗値ばらつきのランダム性を用いることで、不揮発性メモリ装置ごとに、ユニークかつランダムなディジタルＩＤデータを作成することができる。

【０１４０】

図７を参照しながら、本開示のディジタルＩＤデータが複製できない理由について説明する。図７は上述の（３）ディジタルＩＤデータ状態に推移させるときに様々な電圧パルス条件で推移させたときのばらつき分布を示す。トランジスタ耐圧の上限である３．３Ｖかつパルス幅も通常の１０万倍の１０ｍｓの強力なエネルギーをもつ条件から、２Ｖといった通常よりも弱いパルス条件まで含んでばらつきを見たものである。一般にパルスエネルギーが弱い印加条件と、強い印加条件とで、書き込まれた抵抗値の分布間に明確なウインドウがあるとき、２つの印加条件を用いて任意のデータを書き込むことができる。しかしながら、図からわかるように分布の偏りおよび最大/最小値の若干の差はあるものの、総じて全ての条件の分布の中央値が他の条件の分布と重なっている。つまり、中央値を基準に人為的に書き込み条件を変えて、書き分け、任意のデータを書き込むといった複製が、原理的にできないばらつき現象であることが分かる。

【０１４１】

図７のように同じ抵抗値範囲にあるメモリセル群の中で更に抵抗値が低いものと高いものとに分布する理由としては、抵抗変化素子のプロセスばらつきおよび形状ばらつきの他に、例えば、フォーミングが完了するメモリセルがランダムに発生することが考えられる。

【０１４２】

上述のとおり、金属酸化物中の欠陥サイトはメモリセル毎にランダムに配置され、フォーミングによってこれらの欠陥サイト間を繋いでフィラメントが形成される。そのため、仮に初期状態にある複数のメモリセルに一定の電気的ストレスを印加した場合であっても、フォーミングが完了するメモリセルは統計的にばらついて発生することを、本願発明者らは事前実験によって確認している。そのため、仮に複数のメモリセルに対して一様なストレスを印加する場合であっても、確率的にフィラメントが形成され、上述の（２）初回ＨＲ状態に変化する時間が素子ごとに異なる。このため抵抗変化素子内の金属酸化物中の欠陥サイトの数または密度が素子ごとにばらつく。欠陥サイトの密度および個数のばらつきは、素子ごとに固有であり、そこからもたらされる抵抗値の大小も素子ごとに固有となる。

【０１４３】

図８は、フィラメントの発生数が抵抗変化素子ごとに異なることを示す。初期化パルス印加（Ｆｏｒｍｉｎｇ）により、酸素欠陥サイトの発生箇所と密度は素子ごとにランダムである。また、欠陥が相対的に多く発生した素子の抵抗は低くなり、欠陥が相対的に少ない素子の抵抗は高くなっており、ばらつきが生じている。そしてこのようなばらつきは制御不可である。

【０１４４】

図８のように、酸素欠陥サイトの形成が多く、フィラメントパスが形成されやすい場合は、その抵抗変化素子の抵抗値はより低くなる。一方、酸素欠陥サイトの密度が一部でも低いところがある場合はフィラメントパスが形成されにくいため、その抵抗変化素子の抵抗値はより高くなる。各素子の抵抗値はばらついており、このようなばらつきを人為的に制御することはできない。なお、酸素欠陥サイト等が繋がることによってフィラメントパスが形成される材料であれば、同様のメカニズムによって説明できると推察される。

【０１４５】

なお、図２のメモリセル構造において、電圧は第１電極１２４を基準として第２電極１２８に正の電圧を印加する場合を正極性とする。

【０１４６】

その他の例として、第１電極１２４及び第２電極１２８の材料が白金（Ｐｔ）、抵抗変化層１２６の材料がハフニウム酸化物、抵抗変化層１２６の厚さが３０ｎｍ、素子領域の直径を３μｍの円形としてもよい。なお、抵抗変化層１２６が$HfO_{1.6}$の場合、初期抵抗値は数ＭΩ程度であり、高抵抗値範囲が１０００～３０００Ω程度、低抵抗値範囲が１００～３００Ω程度となる。この場合、フォーミングストレスは、例えば、電圧が２～３Ｖ、パルス幅が１００ｎＳｅｃのパルスを累積的に印加する。低抵抗化パルスは、電圧が

＋１．０Ｖ、パルス幅が１００ｎＳｅｃであり、高抵抗化パルスは、電圧が－１．３Ｖ、パルス幅が１００ｎＳｅｃである。

【０１４７】

［閾値について］

図３に示す例では、初期抵抗値範囲の下限が、全ての可変抵抗値範囲の上限以上である。具体的には、初期抵抗値範囲の下限が、複数の可変抵抗値範囲のうち抵抗値が最も大きいものの上限以上であってもよい。さらに具体的には、初期抵抗値範囲の下限は、２個の可変抵抗値範囲のうち抵抗値が最も大きい第１抵抗値範囲の上限に等しくてもよい。

【０１４８】

図３に示す例では、第１閾値は、初期抵抗値範囲の下限以下であり、かつ、複数の可変抵抗値範囲のうち抵抗値が最も大きいものの上限以上である値である。具体的には、第１閾値は、初期抵抗値範囲の下限であり、複数の可変抵抗値範囲のうち抵抗値が最も大きいものの上限である値であってもよい。さらに具体的には、第１閾値は、２個の可変抵抗値範囲のうち抵抗値が最も大きい第１抵抗値範囲の上限に等しくてもよい。なお、第１閾値と等しい値を有する抵抗値は、初期抵抗値範囲に属するものとしてもよいし、複数の可変抵抗値範囲のうち抵抗値が最も大きいものに属するものとしてもよい。

【０１４９】

図３に示す例では、第２閾値は、複数の可変抵抗値範囲のうち抵抗値が最も大きいものの下限以下であり、かつ複数の可変抵抗値範囲のうち抵抗値が最も小さいものの上限以上である値である。具体的には、第２閾値は、２個の可変抵抗値範囲のうち抵抗値が最も大きい第１抵抗値範囲の下限以下であり、かつ２個の可変抵抗値範囲のうち抵抗値が最も小さい第２抵抗値範囲の上限以上である値であってもよい。さらに具体的には、第２閾値は、第１抵抗値範囲の下限または第２抵抗値範囲の上限に等しくてもよい。また、第１抵抗低範囲と第２抵抗値範囲とが隣接していてもよい。すなわち、第１抵抗値範囲を規定する２つの端点のうち小さい方の値と、第２抵抗値範囲を規定する２つの端点のうち大きい方の値とが一致していてもよい。なお、第２閾値と等しい値を有する抵抗値は、複数の可変抵抗値範囲のうち、第２閾値よりも大きな抵抗値を含む抵抗値範囲に属するものとしてもよいし、第２閾値よりも小さな抵抗値を含む抵抗値範囲に属するものとしてもよい。

【０１５０】

メモリセル９１の構成によっては、製造直後のメモリセル９１の抵抗値が、いずれの可変抵抗値範囲よりも小さい場合もある。すなわち、初期抵抗値範囲が可変抵抗値範囲よりも小さい場合がある。具体的には例えば、メモリセル９１が鉄酸化物を抵抗変化層に用いた抵抗変化素子を備える場合に、かかる特性が実現される。

【０１５１】

より具体的には、鉄酸化物において抵抗率は、Fe_3O_4、ＦｅＯ、Fe_2O_3の順に高い。例えば、素子構造として第１電極１２４の材料がＰｔ（白金）、第２電極１２８の材料がＰｔ（白金）、抵抗変化層１２６の材料がFe_3O_4、抵抗変化層１２６全体の厚さが５０ｎｍ以下としうる。

【０１５２】

第１電極１２４と抵抗変化層１２６との接触面および第２電極１２８と抵抗変化層１２６との接触面の面積を０．２５μm^2以下とするとき、初期抵抗値は概ね２００Ωと非常に低抵抗にある。この初期状態のメモリセルに１０μＳｅｃのパルス幅で第１電気的信号と同じ極性で電圧の絶対値が３．５Ｖのパルスを所定の回数を印加することによって、初期抵抗値よりも抵抗値の大きい状態（２Ｋ～８ＫΩの高抵抗状態）に推移する。これは、第２電極１２８と抵抗変化層１２６の接触界面の酸化が進行し、Fe_2O_3の絶縁状態にある抵抗層が形成されるためと考えられる。

【０１５３】

その後、電圧の絶対値が２．４Ｖの第２電気的信号の印加により３００Ωから５００Ωの第２抵抗値範囲と、第２電気的信号と極性の異なる電圧の絶対値が２．４Ｖの第１電気的信号の印加により２Ｋから８ＫΩの第１抵抗値範囲を推移できるようになる。この場合

、初期抵抗のばらつきをディジタルＩＤデータとして利用することが容易であり好ましい。

【０１５４】

制御装置９３は、選択されたメモリセル９１の抵抗値が、第１閾値よりも大きいか否かを判定する第１読み出しモードと、選択されたメモリセル９１の抵抗値が、第２閾値よりも大きいか否かを判定する第２読み出しモードとを選択的に実行することによって、記録されたデータを読み出すことができるように構成されていてもよく、第１閾値および第２閾値は、固定の値ではなく、任意に可変できるように構成されてよい。

【０１５５】

本開示の不揮発性メモリ装置に記録されたデータは、第１種データと第２種データとのいずれか、または両方を含んでよい。第１種データは、各メモリセル９１の抵抗値が初期抵抗値範囲にあるか否かの違いを利用して記録されており、第２種データは、各メモリセル９１の抵抗値が初期抵抗値範囲にあるか否かの違いを利用せずに、各メモリセル９１の抵抗値が少なくとも一つの可変抵抗値範囲にあるか否かの違いを利用して記録されていてもよい。そして、本開示は、上述の何れか同一の抵抗値範囲にあるメモリセルの抵抗値ばらつきを用いてディジタルＩＤデータを生成する３種データを備える。

【０１５６】

この場合において、メモリセルアレイ９０が、第１書き込みアドレス領域と、第２書き込みアドレス領域とを備え、第１書き込みアドレス領域に第１種または第２種のデータのいずれか、または両方が記録されており、第２書き込みアドレス領域にディジタルＩＤデータのもととなる抵抗値状態のメモリセルが保管されていてもよい。第１書き込みアドレス領域と、第２書き込みアドレス領域とは、必ずしも物理的な領域として分離していなくてもよい。例えば、各メモリセル９１がアドレスごとに所定の規則によって第１書き込みアドレス領域と第２書き込みアドレス領域とに振り分けられていてもよく、これによりディジタルＩＤデータの物理的な場所が特定されにくくなり耐タンパ性が向上する。

【０１５７】

メモリセルアレイ９０を構成する複数のメモリセルにフォーミングストレスを印加する工程は選択的に自由に行えるため、第１書き込みアドレス領域と第２書き込みアドレス領域との容量配分および配置を自由に変更し選択することができる。

【０１５８】

図９は、第１実施形態において同一の可変抵抗値範囲にあるメモリセルから連続して抵抗値を読み出した例を示す。「抵抗値が少なくとも１つの可変抵抗値範囲にある」とは、メモリセルが同一の抵抗状態にあることをいう。すなわち二値型のメモリセルである場合には、例えば、メモリセルが低抵抗状態にあって高抵抗状態にないことをいう。つまり、この場合は図３の（３）ディジタルＩＤセット状態と等しい。

【０１５９】

高抵抗化パルスと低抵抗化パルスを交互に印加することで素子が高抵抗状態と低抵抗状態とを可逆的に遷移することを確認した。その後、低抵抗状態にある素子に高抵抗化パルスを１回だけ印加して高抵抗状態とし、その後は低抵抗化パルスも高抵抗化パルスも印加することなく、読み出し動作を連続して１０００回実行し、それぞれの抵抗値情報の読み出しを行った。読み出しの時間間隔は５μＳｅｃとした。

【０１６０】

図９では、横軸が読み出し回数、縦軸が規格化された抵抗値情報であり、同じ構成を有する３つの素子の抵抗値の揺らぎが示されている。ここでいう抵抗値情報とは、後述する放電方式の読み出し回路で得られるもので、値が大きければ高い抵抗値を示し、小さければ低い抵抗値を示す。図９によれば、同一の抵抗状態にある素子を繰り返して読み出すと、抵抗値がランダムに増減する様子が確認できる。

【０１６１】

ここで述べる抵抗値変動または抵抗値揺らぎとは、抵抗状態を変化させる電気的パルスが印加されない状態、すなわち同一の抵抗状態、にある同一メモリセルから読み出される

抵抗値が時間の経過と共に変動する現象を指す。

【０１６２】

図１０Ａ、図１０Ｂは、パーコレーションモデル（ｐｅｒｃｏｌａｔｉｏｎ ｍｏｄｅｌ）を用いて、フォーミング時における抵抗変化層（例えば局所領域）中のフィラメントの形成をシミュレートした結果の一例を示す図である。

【０１６３】

パーコレーションモデルとは、抵抗変化層中にランダムに分布した欠陥サイトに対して、欠陥サイト等の密度がある閾値を超えると欠陥サイト等の繋がりが形成される確率が増加するという理論に基づくモデルである。ここで「欠陥」とは、例えば、金属酸化物中で酸素が欠損していることを意味し、「欠陥サイトの密度」とは酸素不足度とも対応している。すなわち、酸素不足度が大きくなると、欠陥サイトの密度も大きくなる。

【０１６４】

図１０Ａ、図１０Ｂに示されるシミュレーションでは、抵抗変化層の酸素イオンサイトを、格子状に仕切られた領域（サイト）として近似的に仮定し、確率的に形成される欠陥サイトによって形成されるフィラメントをシミュレーションで求めている。図１０Ａおよび図１０Ｂにおいて、“０”が含まれているサイトは抵抗変化層中に形成される欠陥サイトを表している。他方、空白となっているサイトは酸素イオンが占有しているサイトを表しており、導電パスのない高抵抗な領域を意味している。また、矢印で示される欠陥サイトのクラスター（上下、左右及び斜め方向に１個のサイトの範囲内で互いに接続された欠陥サイトの集合体）は、図中の上下方向に電圧が印加された場合に抵抗変化層内に形成されるフィラメント、すなわち電流が流れるパスを示している。

【０１６５】

図１０Ａに示されるように、抵抗変化層の下面と上面との間に電流を流すフィラメントは、ランダムに分布する欠陥サイトの内の上端から下端までを接続する欠陥サイトのクラスターで構成される。このパーコレーションモデルに基づくと、フィラメントの本数及び形状は確率的に形成されることになる。フィラメントの本数及び形状の分布は、抵抗変化層の抵抗値のばらつきとなる。

【０１６６】

また、フィラメントは、上述した高抵抗化パルスにより酸素イオンがフィラメントに導入され欠陥サイトと結合し、幾つかのフィラメントパスを切断することにより高抵抗状態へと推移する。逆に、低抵抗化パルスを印加すると、再び酸素イオンの離脱が起こり、欠陥サイトが生成されフィラメントパスが再現され、低抵抗状態へと推移する。各抵抗状態の間でフィラメントパスの本数に充分な差があれば、抵抗値の差分が大きくなり、抵抗値の判定マージンが増加する。

【０１６７】

次に、図９のように同一の抵抗状態にある素子において抵抗値が揺らぐ現象のメカニズムについて説明する。

【０１６８】

各抵抗状態の抵抗値を決定するフィラメントパスの形状、本数および太さは、時間的に安定ではない。つまり、酸素サイトから酸素イオンが抜け出ることによって欠陥サイトが生成されたり、欠陥サイトへ酸素イオンが供給されることによって欠陥サイトが消滅したりすることにより、フィラメントパスの形状、本数および太さが微妙に増減する。これが時間的な抵抗値の揺らぎとして観測される。図１０Ｂは、その一例を示す説明図で、たった一つの欠陥サイトが隣接サイトと入れ替わっただけで、図１０Ａにあったフィラメントパスのうち、一つのパスが断絶されることになる。この場合、抵抗値が僅かに増加することになる。図による説明は省略するが、逆に欠陥サイトが隣接サイトと入れ替わることにより新たなフィラメントパスが発生することもある。この場合は、僅かに抵抗値が減少する。図９のような抵抗値の揺らぎ現象は、かかるメカニズムにより発生すると考えられる。実際には、図のようなフィラメントパスの数は多数あり、その一部が増減するもののフィラメントパスの総数は大きくは変化しないと考えられる。すなわち、揺らぎ現象におい

ては、メモリセルの抵抗状態が別の抵抗状態に変化してしまうほどの大きなフィラメントパスの変化は生じないと考えられる。

【０１６９】

上記メカニズムにより抵抗値が揺らぐ現象は、酸化物中の酸素イオンの移動により抵抗値が変動するあらゆる抵抗変化素子に当てはまると考えられる。具体的には例えば、かかる性質を有するメモリセルとして、第１電極と金属酸化物と第２電極とをこの順で積層した素子を用いることができる。あるいは例えば、第１電極と遷移金属酸化物と第２電極とをこの順で積層した素子を用いることができる。

【０１７０】

このように抵抗変化型メモリ装置に用いられるメモリセルは書き込まれた抵抗値に対して若干であるが抵抗値の揺らぎ現象が存在する。図６に示す中央抵抗値を用いて抵抗値の大小関係からディジタルデータの１または０に判別して得られるディジタルＩＤデータには、抵抗値揺らぎが原因の誤りデータが発生する。中央抵抗値付近は、抵抗値のばらつき分布の中央であるため、その抵抗値付近にあるメモリセルの分布数が最も多いことになる。これら中央付近のメモリセルが前述のとおりランダムに抵抗値が揺らぐため多くのビットがランダムに誤ることになる。

【０１７１】

本願発明者らは、書き込まれた抵抗値が、放置時間および温度環境、更には装置の電源環境などにより、中央抵抗値の最適値が変動し、誤り率が安定せず、ディジタルＩＤデータを安定的に生成することができないという課題を見出した。この課題について図１１を用いて説明する。

【０１７２】

図１１は図３に示すようなディジタルＩＤセット状態に書き込まれた所定のビット数のメモリセル群の抵抗値を放置時間ごとに読み出したときのばらつき範囲と抵抗中央値を示す。

【０１７３】

測定に使用したビット数は１Ｋｂｉｔで、放置時間に対する劣化を加速するために放置温度は１７５℃とした。図からわかるように、放置時間とともに、ばらつき範囲が広がっている。さらに、破線で囲んだように抵抗中央値が徐々に上昇していることが分かる。つまり、放置時間が増加するに従って、抵抗値の分布が高抵抗側にシフトしていると言える。

【０１７４】

図１２は、書き込まれたディジタルＩＤデータを図１１に示したような初期の抵抗中央値（１４３）で抽出したときにおける、エラーレートと放置時間との関係を示す。エラーレートは抽出したデータと初回ＩＤデータとが相違する割合を示す。図１２から分かるように放置時間とともに最適な抵抗中央値がずれるためエラーレートが急速に増大していることが分かる。この現象は、放置時間だけでなく周辺温度の変化、または装置電源電圧の変化によっても大きく変動する。

【０１７５】

そこで発明者らは図１３および図１４に示すフローを考案した。

【０１７６】

図１３は、ディジタルＩＤデータを生成し、不揮発性メモリ装置１０に書き込む処理フローの一具体例を示す。このフローは、たとえば不揮発性メモリ装置１０が工場から出荷される前の検査工程時に実行される。

【０１７７】

一方、図１４は、ディジタルＩＤデータを再生する処理フローの一具体例を示す。このフローは、たとえば工場から出荷された後の不揮発性メモリ装置１０が市場において使用される都度実行される。

【０１７８】

前述したように、生成されるディジタルＩＤデータには誤りデータが含まれるため真の

正しいＩＤデータを常に得るためには誤り訂正を行う必要がある。従って、図１３および図１４のように、装置の出荷前の検査工程時と、市場で装置が使用されるフィールド使用時とでは処理のフローが異なる。

【０１７９】

出荷前検査時は図のように不揮発性メモリ装置の各メモリセルは可変状態ではなく絶縁抵抗に近い抵抗値を示す初期状態にある。図１３のフローのＳ１ステップにおいて、図３に関連して説明したようなフォーミングストレスを印加するフォーミング処理が実行され、各メモリセルを図３の（２）初回ＨＲ状態に推移せしめる。次にＳ２ステップにおいて低抵抗化パルスが印加され図３の（３）ディジタルＩＤセット状態にセットされる。そしてＳ３ステップにおいて複数のディジタルＩＤセット状態にあるメモリセルの抵抗値情報を読み出し、Ｓ４ステップにて読み出した抵抗値情報から抵抗値ばらつきの分布の中央値を演算して保持する。Ｓ５ステップでは再度、（３）ディジタルＩＤセット状態にあるメモリセルから抵抗値情報を読み出し、上述の保持された中央値との関係からディジタルＩＤデータを生成する。

【０１８０】

図１５は、ディジタルＩＤデータの例を示す。上述したように、ディジタルＩＤセット状態にあるメモリセルの抵抗値情報と、閾値である抵抗値ばらつきの分布の中央値を比較して、抵抗値情報がより小さい場合にはそのメモリセルにデータ「１」を割り当て、抵抗値情報がより大きい場合にはそのメモリセルにデータ「０」を割り当てる。これにより、人為的に制御できないメモリセルの抵抗値を利用した、不揮発性メモリ装置１０を一意に識別可能なディジタルＩＤデータを得ることができる。

【０１８１】

再び図１３を参照する。Ｓ６ステップではディジタルＩＤデータをもとにデータ誤りを訂正するために用いるパリティーデータを演算し、Ｓ７ステップにてパリティーデータを別の異なるメモリセルに記録する。

【０１８２】

次に、図１４を参照する。フィールドにおいて装置が使用される際、Ｓ８ステップにおいて、検査時のＳ３およびＳ４ステップと同様に複数のディジタルＩＤセット状態にあるメモリセルの抵抗値情報を読み出し、Ｓ９ステップにて読み出した抵抗値情報から抵抗値ばらつきの分布の中央値を演算して保持する。さらにＳ１０ステップでは再度、（３）ディジタルＩＤセット状態にあるメモリセルから抵抗値情報を読み出し、上述の保持された中央値との関係からディジタルＩＤデータを生成する。Ｓ１１ステップにおいて検査時に予め保存されたパリティーデータを読み出し、Ｓ１２ステップでパリティーデータを用いてＳ１０で得たディジタルＩＤデータの誤りデータを訂正する。その結果、Ｓ１３ステップにて常に同じ真のディジタルＩＤデータを得る。

【０１８３】

図１６は、誤り訂正前のデータ誤り率の推移を示す。この推移は、図１４のフローによりフィールド使用時に最適な抵抗中央値を検出し、検出した抵抗中央値でディジタルＩＤデータを生成したときの誤り訂正前のデータ誤り率の推移である。前述した誤り訂正前のディジタルＩＤデータを生のディジタルＩＤデータ（Raw Digital ID Data）と呼ぶ。図１６は横軸にディジタルＩＤデータの読み出し回数を示し、縦軸にそのときのディジタルＩＤデータの誤り率（エラーレート）を示した。図からわかるようにエラーレート上昇が抑制され２％～３％の誤り率で良好な結果が得られている。

【０１８４】

更に、本開示の特徴的な点として、累積エラーレートがあげられる。図１７は読み出し回数と累積エラーレートとの関係を示す。累積エラーレートとは、複数回、生のディジタルＩＤデータを読み出し新たな異なるビットに誤りが発生した場合は順次加算していき、累計でエラーしたビット数から誤り率を求めたものである。図１６で各読み出しごとのエラーレートは２～３％で低いものの、異なるビットが入替わり立代りするため累積エラーレートは読み出し回数に従って上昇する。図では２５００回のディジタルＩＤデータの生

成では１４％ものビットが誤りを起こしたことがわかる。つまり、読み出すたびにエラーするビットが異なり、エラー訂正前のＩＤデータは刻一刻と変化していることが理解できる。この特長により、前述したような機械学習攻撃を受けた場合であっても学習結果が定まらず真のディジタルＩＤデータが解析できないため、ハッキングに対して極めて耐性があるといえる。

【０１８５】

では、次に本開示の方式を実現するための具体的な構成例について説明する。

【０１８６】

図１８は、本開示の不揮発性メモリ装置の具体的な構成例を示すブロック図である。なお、図１８はあくまで一例であり、第１実施形態の不揮発性メモリ装置の具体的構成が図１８に示される構成に限定されるものではない。

【０１８７】

図１８に示すように、実施例の不揮発性メモリ装置１０は、半導体基板上に、メモリ本体部２２を備えている。また不揮発性メモリ装置１０は、さらにデータ入出力回路６と、制御回路１５と、アドレス入力回路１６と、誤り訂正およびパリティー生成回路４００とを備えている。

【０１８８】

メモリ本体部２２は、読み出し回路１１と、書き込み回路１４と、カラムデコーダ回路１７と、ロウデコーダ回路１８と、メモリセルアレイ２０と、中央値検出回路２５とを備えている。

【０１８９】

書き込み回路１４は、選択されたメモリセル２１へ各動作における所定の電圧を印加してデータを書き込む。

【０１９０】

読み出し回路１１は、ビット線に流れる電流の変化を、後述する読み出し方式により検知し、選択メモリセルの抵抗値情報をディジタルカウント値として取得する。

【０１９１】

ロウデコーダ回路１８は、メモリセルアレイ２０に接続されている複数のｍ本のワード線ＷＬの中から１つのワード線ＷＬを選択する。

【０１９２】

カラムデコーダ回路１７は、複数のｎ本のビット線ＢＬと複数のソース線ＳＬの中から並列読み出し数であるＳ本のビット線ＢＬと、それに対応するＳ本のソース線ＳＬとを選択し、書き込み回路および読み出し回路へ接続する。

【０１９３】

これらは並列的に読み出しおよび／または書き込みが行われる行および／または列の数に応じて動作可能である。

【０１９４】

不揮発性メモリ装置１０の読み出し回路１１は、出力端子ＡおよびＢと、入力端子Ａとを有する。読み出し回路１１は、入力端子Ａを介して閾値を受け取る。この閾値は、読み出し回路１１が、カラムデコーダ回路１７から得られた信号を０または１のデータとして二値化するために利用される。

【０１９５】

また、読み出し回路１１は、出力端子Ｂを介して、カラムデコーダ回路１７から得られた信号を中央値検出回路２５に出力する。この信号は、ディジタルＩＤデータを生成するために必要な中央値を算出するために中央値検出回路２５によって利用される。

【０１９６】

さらに、読み出し回路１１は、出力端子Ａを介して、ユーザデータである０または１のデータ、および、ディジタルＩＤデータである０または１のデータを出力する。ユーザデータを生成する際に利用される閾値と、ディジタルＩＤデータを生成する際に利用される閾値とは異なっていてもよい。

【０１９７】
図１３で説明したように、検査工程時にディジタルＩＤデータに応じた誤り訂正のためのパリティーデータを生成する場合は、上述の出力端子Ａから出力されるディジタルＩＤデータをデータ入出力回路６が受け取り、誤り訂正およびパリティー生成回路４００に送る。
【０１９８】
誤り訂正およびパリティー生成回路４００は、ディジタルＩＤデータに応じた誤り訂正用のパリティーデータを演算し、演算結果をデータ入出力回路６に戻す。
【０１９９】
なお誤り訂正およびパリティー生成回路４００は、機能的には、誤り訂正を行う回路要素と、パリティーを生成する回路要素とに分けることが可能である。本実施の形態では、誤り訂正およびパリティー生成回路４００は１つの回路として説明されているが、誤り訂正回路およびパリティー生成回路という別個の２つの回路として設けられてもよい。
【０２００】
データ入出力回路６は、パリティーデータを書き込み回路１４に出力し、書き込み回路１４は、ディジタルＩＤデータに応じた冗長のメモリセルにパリティーデータを書き込む。なお、これらの制御は制御回路１５を介して実行される。
【０２０１】
引き続き、中央値検出回路２５の動作について、より詳しく説明する。読み出し回路１１は抵抗値情報のディジタルカウント値を入力端子Ａに入力される閾値と比較して、１または－１の中央値誤差信号を出力端子Ｂから出力する。出力端子Ｂから出力される中央値誤差信号は並列的に読み出されるチャンネル数（ｓ）だけ同時に出力される。ｓ個の中央値誤差信号は、中央値検出回路２５に入力される。
【０２０２】
中央値検出回路２５は演算回路であり、たとえば半導体集積回路を用いて実現され得る。中央値検出回路２５は中央値誤差信号が小さくなるようにフィードバック制御されて算出した抵抗中央値を読み出し回路１１の入力端子Ａに出力する。
【０２０３】
一般に不揮発性メモリ装置にユーザがデータを書き込む場合は、外部からアドレス信号、データ信号、コントロール信号を装置に入力することで実行される。このため外部から入力されるアドレス信号を受け取るアドレス入力回路１６と、外部から入力されるコントロール信号に基づいてメモリ本体部２２の動作を制御する制御回路１５が、書き込むアドレスを選択するとともに書き込みパルスを印加する様に制御する。そして、データ入出力回路６は外部から入力されるデータ信号（外部データ）を受け取り、その外部データに基づいて書き込みデータを生成して書き込み回路１４に送る。書き込み回路１４は、その書き込みデータを選択されたアドレスに対応するメモリセルに書き込む。
【０２０４】
この書き込みデータは、データ入出力回路６により誤り訂正のためのパリティーデータが付加されたデータである。以下、パリティーデータに関連する処理を説明する。
【０２０５】
書き込みデータの生成のために、データ入出力回路６は、取り込んだ外部データを、図１８に示す誤り訂正およびパリティー生成回路４００に送る。誤り訂正およびパリティー生成回路４００は、入力された外部データに応じた誤り訂正を行うためのパリティーデータを演算してデータ入出力回路６に戻す。データ入出力回路６は、外部データと誤り訂正用パリティーをあわせた書き込みデータを書き込み回路１４に送り、そのデータに従って選択されたメモリセルにデータが書き込まれる。このとき、パリティーデータは外部から指定されたアドレス情報に応じて予め決められた冗長のメモリセルに書き込まれる。
【０２０６】
また、不揮発性メモリ装置１０に書き込まれたユーザデータを読み出す際には、アドレス信号を受け取るアドレス入力回路１６と、外部から入力されるコントロール信号に基づ

いてメモリ本体部２２の動作を制御する制御回路１５とが利用される。具体的には、制御回路１５は、アドレス入力回路１６に入力されたアドレス信号に基づいて読み出すアドレスを選択するとともに選択されたメモリセルを読み出すように読み出し回路１１を制御する。また、外部から入力されたアドレスに応じたパリティーデータを読み出すため予め決められた冗長のメモリセルも順次選択され読み出すように読み出し回路１１を制御する。読み出し回路１１は、入力端子Ａに入力される閾値に従い１／０判定をした結果であるディジタルデータを出力端子Ａから出力する。アドレス信号に応じたユーザデータと、そのユーザデータに対応したパリティーデータは、データ入出力回路６を介して誤り訂正およびパリティー生成回路４００に送られ、データ誤りがあれば訂正されたのち、データ入出力回路６に戻され、更に装置外部に出力される。

【０２０７】

このとき、読み出し回路１１の入力端子Ａに入力される閾値は中央値検出回路２５からのものではなく、図３の第１閾値および第２閾値に相当する値である。なお、図には、入力端子Ａに入力される閾値を、中央値検出回路２５から出力された中央値にするか、図３の第１閾値および第２閾値に相当する値にするかを切り替えるための切替回路の記載は省略している。第１閾値および第２閾値に相当する値は、たとえば図示されないレジスタに記憶されている。なお、第１閾値および第２閾値で読み出す際には、後述するセンスアンプの判定レベルＶＲＥＦ値またはＬＯＡＤ電位を変更しても良い。

【０２０８】

以下に、パリティーデータを用いてディジタルＩＤデータの誤りを訂正する例を説明する。以下では、各構成要素がどのように動作するかの観点で説明しているが、それらの動作は、制御回路１５からの指示によって制御されていることに留意されたい。

【０２０９】

まず、工場出荷前の検査工程時に、読み出し回路１１および中央値検出回路２５は予めディジタルＩＤデータを生成する。誤り訂正およびパリティー生成回路４００は、そのディジタルＩＤデータをもとにパリティーデータを生成する。生成されたパリティーデータは、たとえば予め定められたアドレスの不揮発性メモリセル内に、ユーザデータとして記録される。

【０２１０】

次に、不揮発性メモリ装置１０のフィールド使用時の動作を説明する。パリティーデータは、予め検査時にユーザデータとして記録されているため図３の第１閾値および第２閾値で判定される。すなわち、読み出し回路１１は、ディジタルＩＤデータを前述した工程により読み出し、データ入出力回路６に出力する。その後、読み出し回路１１は、閾値を所定の値に切り替えて、ディジタルＩＤデータに応じた冗長のメモリセルに保存されたパリティーデータを読み出し、データ入出力回路６に出力する。データ入出力回路６は、ディジタルＩＤデータとパリティーデータを誤り訂正およびパリティー生成回路４００に送信する。誤り訂正およびパリティー生成回路４００は、誤りを訂正した後のデータを、データ入出力回路６に戻す。データ入出力回路６はそのデータを装置外部に出力する。

【０２１１】

なお、上述の例では、ユーザデータおよびディジタルＩＤデータの両方の誤りが、同じ誤り訂正およびパリティー生成回路４００によって訂正されるとして説明したが、これは一例である。ディジタルＩＤデータの誤りを訂正するための誤り訂正およびパリティー生成回路は、例えば装置外部に具備されても良い。このような構成にすれば、装置外に送られるディジタルＩＤデータは、データ誤りを含んでおり、装置外部との通信路においてハッキングなどの脅威に対してセキュリティーが向上できるという利点がある。

【０２１２】

図に示すように、メモリ本体部２２は、記憶領域として、ユーザデータ領域７とＰＵＦデータ領域８とを有する。ユーザデータ領域７にはユーザの任意のデータ（ユーザデータ）が記憶される。ユーザデータの書き込みおよび読み出しはユーザデータ領域７のアドレスが選択される。ＰＵＦデータ領域８には、ディジタルＩＤデータとして用いられる個体

識別情報を導き出すための、フォーミングストレスが印加される。その結果、ＰＵＦデータ領域８のメモリセル群は同一の抵抗値状態を取る。ディジタルＩＤデータは、各メモリセルの抵抗値の揺らぎを利用して導出されるデータである。

【０２１３】

なお、ユーザデータ領域７とＰＵＦデータ領域８は図のようにワード線単位に分けられる必要はなく、アレイ上の任意の領域で区分けしても良い。物理的な領域区分の規則性を複雑にするほどハッキングなどの攻撃への耐性を高めることができる。

【０２１４】

メモリセルアレイ２０は、ワード線単位で、ＷＬ０、ＷＬ１、ＷＬ２、・・・ＷＬｍ－１をユーザデータ領域７と、ＷＬｍ、・・・ＷＬｎをＰＵＦデータ領域８として切り分けられ、互いに平行に延びるように形成された複数のワード線ＷＬ０、ＷＬ１、ＷＬ２、・・・ＷＬｍ－ｋ－１、ＷＬｍ－ｋ、・・・ＷＬｍと、複数のワード線と交差し、かつ互いに平行に延びるようにして形成された複数のビット線ＢＬ０、ＢＬ１、・・・ＢＬｎと、複数のワード線と交差し、かつ互いに平行に、かつビット線と平行に延びるようにして形成されたソース線ＳＬ０、ＳＬ１、ＳＬ２、・・・ＳＬｎと、を備える。複数のワード線と複数のビット線の立体交差点には、それぞれメモリセル２１が配置されている。

【０２１５】

それぞれのメモリセル２１は抵抗変化素子２３とトランジスタ２４とを備える。ワード線ＷＬ０、ＷＬ１、ＷＬ２、・・・ＷＬm-k－１、ＷＬm-k、・・・ＷＬｍはそれぞれのトランジスタ２４のゲート端子に接続され、ビット線ＢＬ０、ＢＬ１、・・・ＢＬｎは、それぞれのメモリセル２１が備える抵抗変化素子２３の第２電極に接続され、抵抗変化素子の第１電極はトランジスタ２４の第２主端子に各々接続され、ソース線ＳＬ０、ＳＬ１、ＳＬ２、・・・ＳＬｎは、トランジスタ２４の第１主端子にそれぞれ接続されている。

【０２１６】

抵抗変化素子２３はメモリセル２１において不揮発性メモリ素子として動作する。不揮発性メモリ装置１０は、各メモリセル２１が１個のトランジスタ２４と１個の抵抗変化素子２３とから構成される、いわゆる１Ｔ１Ｒ型の抵抗変化型不揮発性メモリ装置である。メモリセルの選択素子は前述のトランジスタに限定されない。例えばダイオードなどの２端子素子を用いても良い。

【０２１７】

制御回路１５はコントロール信号に基づき、カラムデコーダ回路１７に対し、ビット線あるいはソース線のいずれか一方を選択し、書き込み時は書き込み回路１４、読み出し時は読み出し回路１１に接続させる。その上で、書き込み回路１４あるいは読み出し回路１１を動作させる。

【０２１８】

抵抗変化素子２３については、実施形態において上述した抵抗変化素子１２０と同様の構成とすることができるので、詳細な説明を省略する。

【０２１９】

図１８に示す例では、メモリセルアレイ２０の選択トランジスタとしてＮＭＯＳトランジスタが用いられているが、これに限定されず、ＰＭＯＳトランジスタを用いても良い。

【０２２０】

図１９は本開示の不揮発性メモリ装置１０が備える読み出し回路１１の構成例を示す回路図である。

【０２２１】

読み出し回路１１は放電方式のセンスアンプ回路３０を有している。当該センスアンプ回路は、コンパレータ３１と、抵抗値カウンタ３２と、プリチャージ用のＰＭＯＳトランジスタ３３と、ロード電流用のＰＭＯＳトランジスタ３４と、クランプ電圧印加用のＮＭＯＳトランジスタ３５で構成されたクランプ回路とを備えている。

【０２２２】

抵抗値カウンタ３２は、コンパレータ３１の出力先に接続されている。抵抗値カウンタ

３２は、リセット信号ＲＳＴがロウレベルとなることで、抵抗値カウンタ内のカウント値が初期化された後、クロック信号ＣＬＫによるカウントを開始する。クロック信号ＣＬＫは、制御回路１５から出力される信号であって、抵抗変化素子２３の抵抗値によって変化する放電時間をカウント値に変換する際の基準となる信号である。クロック信号ＣＬＫは、例えば一定の周波数を維持する矩形波である。このクロック信号ＣＬＫが立ち上がる毎に、抵抗値カウンタのカウント値が１つ加算され、ノードＳＥＮがＶＲＥＦを下回ると抵抗値カウンタのカウントアップが停止し、そのときのカウント値がＣＯＵＮＴ＿ＯＵＴに維持される。このとき、入力Ａからは閾値が入力される。比較器１３５はＣＯＵＮＴ＿ＯＵＴと入力Ａの閾値とを比較し、閾値以上であれば１を、閾値未満であれば０を出力Ａから出力する。また、閾値以上であれば１を、閾値未満であれば－１を出力Ｂから出力する。プリチャージＰＭＯＳトランジスタ３３は、ゲート端子にプリチャージ制御信号ＰＲＥが入力され、ソース端子にＶＤＤが入力され、ドレイン端子にノードＳＥＮが接続されている。

【０２２３】

ロードＰＭＯＳトランジスタ３４は、ゲート端子にロード制御信号ＬＯＡＤが入力され、ソース端子にＶＤＤが入力され、ドレイン端子にノードＳＥＮが接続されている。

【０２２４】

クランプＮＭＯＳトランジスタ３５は、ゲートにクランプ制御信号ＣＬＭＰが入力され、ソース端子もしくはドレイン端子の何れか一方にノードＳＥＮが接続され、他端にはカラムデコーダ回路を介して選択されたメモリセルが接続されている。なお、図１９ではカラムデコーダ回路は省略している。

【０２２５】

ここで、読み出し回路１１がカウント値（抵抗カウント値の一例）を出力する動作について、読み出し回路の構成図（図１９）と図２０Ａおよび図２０Ｂのタイミングチャートを用いて、具体的に説明する。

【０２２６】

図２０Ａは、選択されたメモリセルを放電方式にて読み出す場合のタイミングチャートである。

【０２２７】

Ｔ１のプリチャージ期間では、制御信号ＰＲＥはロウレベルとなり、プリチャージ用ＰＭＯＳトランジスタ３３はオン状態になる一方で、制御信号ＬＯＡＤはハイレベルとなり、ロード用ＰＭＯＳトランジスタ３４はオフ状態となる。選択ワード線ＷＬｓの電位はロウレベルでトランジスタ２４はオフ状態となっている。

【０２２８】

クランプ回路のクランプＮＭＯＳトランジスタ３５のゲート端子にＶＣＬＭＰの電圧が印加されることで、選択ビット線ＢＬｓの電位はＶＣＬＭＰからＶＴ（クランプＮＭＯＳトランジスタ３５の閾値）を引いた電位までプリチャージされる。選択ソース線ＳＬｓはＧＮＤに固定される。ノードＳＥＮはＶＤＤまでプリチャージされる。また、コンパレータの出力に接続されている抵抗値カウンタの制御信号ＲＳＴはハイレベルとなっているため、抵抗値カウンタ出力端子ＣＯＵＮＴ＿ＯＵＴは０の固定値が出力される。

【０２２９】

Ｔ２のセンス期間では、制御信号ＰＲＥをハイレベルとすることで、プリチャージＰＭＯＳトランジスタ３３がオフ状態となり、制御信号ＬＯＡＤがロウレベルになることで、ロードＰＭＯＳトランジスタ３４はオン状態になる。また選択ワード線ＷＬｓの電位をハイレベルにすることで、ＮＭＯＳトランジスタ２４はオン状態となる。

【０２３０】

そして選択ビット線ＢＬｓから選択されたメモリセル２１を介して選択ソース線ＳＬｓへと電圧が印加され、放電が開始される。放電開始と同時に抵抗値カウンタ３２の制御信号ＲＳＴがロウレベルとなり、カウントが始まる。そして、１カウント毎に、コンパレータ３１によって、ノードＳＥＮの電位と参照電圧ＶＲＥＦの電圧が比較され、ノードＳＥ

Ｎが参照電圧ＶＲＥＦを下回るまで、カウント値が加算され続ける。読み出し時の抵抗変化素子２３の抵抗値が高いほど放電時間は長くなり、カウント値は大きくなる。

【０２３１】

また、コンデンサ３６の容量を調整することで、放電時間を調整することも可能である。コンデンサ３６の容量が大きければ、ノードＳＥＮの放電時間も遅くなるため、カウント値は長くなり、容量が小さければ、ノードＳＥＮの放電時間は速くなり、カウント値は短くなる。コンデンサ３６は、例えば、放電時間が速い低抵抗レベルの検出精度を向上させたいとき、効果的である。カウントの間隔はクロック信号ＣＬＫで決定されるため、その動作周波数が抵抗カウント値の分解能となる。しかし、低い抵抗値の場合、放電時間がカウント値の分解能を上回る可能性があるため、区別できなくなる場合がある。そこで、ノードＳＥＮに容量負荷を上乗せし、遅延させることで、意図的に分解能で検出できるレベルの放電特性に調整することが可能となる。しかしながら、原理上放電方式の場合は高抵抗になればなるほど放電時間が長くなり、それにともなって放電の傾斜が緩やかに変化するため、カウンタ値に対する抵抗値情報の分解能が向上する。つまり放電方式の場合は高抵抗側が高精度な抵抗値情報を得ることのできる方式である。

【０２３２】

Ｔ３のラッチ期間では、放電が開始された後、ノードＳＥＮが参照電圧ＶＲＥＦを下回ったときの抵抗値カウンタ３２のカウント値がラッチされる。ラッチされたカウント値は、ＣＯＵＮＴ＿ＯＵＴに出力され、マスクデータ修正回路１２に格納されて、抵抗変化素子２３の抵抗値情報を表すカウント値として扱われる。

【０２３３】

Ｔ４のリセット期間においては、データ出力が完了すると、選択ワード線ＷＬｓの電位がロウレベルとされ、選択されたメモリセル２１のトランジスタ２４がオフとなり、読み出し動作が終了する。

【０２３４】

図２０Ｂは、選択されたメモリセルを充電方式にて読み出す場合のタイミングチャートである。

【０２３５】

Ｔ１のディスチャージ期間であり、制御信号ＰＲＥ、ＬＯＡＤ共にハイレベルとなり、プリチャージ用ＰＭＯＳトランジスタ３３とロード用ＰＭＯＳトランジスタ３４は何れもオフ状態となる。また選択ワード線ＷＬｓの電位はロウレベルでトランジスタ２４もオフ状態となっている。

【０２３６】

クランプ回路のクランプ用ＮＭＯＳトランジスタ３５のゲート端子にＶＣＬＭＰの電圧が印加され、選択ワード線ＷＬｓの電位をハイレベルにすることで、ＮＭＯＳトランジスタ２４はオン状態となるため、ノードＳＥＮ、選択ビット線ＢＬｓは抵抗変化素子２３を介してＧＮＤへ接続され、ＧＮＤレベルまでディスチャージされる。また、コンパレータの出力に接続されている抵抗値カウンタの制御信号ＲＳＴはハイレベルとなっているため、抵抗値カウンタ出力端子ＣＯＵＮＴ＿ＯＵＴは０の固定値が出力される。

【０２３７】

Ｔ２のセンス期間では、制御信号ＬＯＡＤがロウレベルになることで、ロードＰＭＯＳトランジスタ３４はオン状態になり、ロードＰＭＯＳトランジスタ３４、クランプＮＭＯＳトランジスタ３５、選択メモリセル２１ｓの電流パスが形成され、ノードＳＥＮ、選択ビット線ＢＬｓへ充電が開始される。充電開始と同時に、抵抗値カウンタ３２の制御信号ＲＳＴがロウレベルとなり、カウントが始まる。そして、１カウント毎に、コンパレータ３１によって、ノードＳＥＮの電位と参照電圧ＶＲＥＦの電圧が比較され、ノードＳＥＮが参照電圧ＶＲＥＦを上回るまで、カウント値が加算され続ける。読み出し時の抵抗変化素子２３の抵抗値が低いほど充電時間は長くなり、カウント値は大きくなる。

【０２３８】

また、コンデンサ３６は放電方式の方で時間のときと同様に、充電方式も充電時間を調

整することも可能である。詳細な説明は放電方式での説明と同様であるため割愛する。原理上充電方式の場合は低抵抗になればなるほど充電時間が長くなり、それにともなって充電の傾斜が緩やかに変化するため、カウンタ値に対する抵抗値情報の分解能が向上する。つまり充電方式の場合は低抵抗側が高精度な抵抗値情報を得ることのできる方式である。

【０２３９】

Ｔ３のラッチ期間では、充電が開始された後、ノードＳＥＮが参照電圧ＶＲＥＦを上回ったときの抵抗値カウンタ３２のカウント値がホールドされる。ホールドされたカウント値は、ＣＯＵＮＴ＿ＯＵＴに出力され、抵抗変化素子２３の抵抗値情報を表すカウント値として扱われる。

【０２４０】

Ｔ４のリセット期間においては、データ出力が完了すると、選択ワード線ＷＬｓの電位がロウレベルとされ、選択されたメモリセル２１のトランジスタ２４がオフとなり、読み出し動作が終了する。

【０２４１】

図１９の構成であれば、放電方式と充電方式の両方を用いることができる。しかし、図１９の比較器１３５で例示した出力Ａおよび出力Ｂの論理例は放電方式の読み出し回路における例である。高抵抗状態と低抵抗状態に夫々対応するディジタルデータの論理を同じにする場合は、検出方向が逆になるために充電方式では反転する必要がある。具体的には、出力Ａへの論理はａ≧ｂの場合は１とし、ａ＜ｂの場合は０となる。出力Ｂへの論理は放電方式と充電方式で等しい。

【０２４２】

このように読み出しの方式によって抵抗値情報に対する分解能が異なるため、高精度に抵抗値情報を得たい場合は、放電方式はディジタルＩＤデータが高い抵抗値範囲を用いて保存される場合に用いるのが好ましい。逆に充電方式はディジタルＩＤデータが低い抵抗値範囲を用いて保存される場合に用いることが好ましい。しかしながら、一方で図１９に示した抵抗値カウンタ３２のカウンタ幅はハードウェアの制約上有限な量である。つまり前述したような放電時間または充電時間が長すぎる場合はカウンタのレンジをオーバーしてしまい正確な抵抗値情報が得られない問題がある。このため必要なカウンタのビット幅を節約して回路規模の縮小を図る場合は、放電方式はディジタルＩＤデータが低い抗値範囲を用いて保存される場合に用いるのが好ましい。逆に充電方式はディジタルＩＤデータが高い抵抗値範囲を用いて保存される場合に用いることが好ましい。

【０２４３】

図２１は、本開示の不揮発性メモリ装置１０が備える中央値検出回路２５の構成例を示している。

【０２４４】

図２１に示すように、中央値検出回路２５は、選択回路２００と、アップダウンカウンタ２０１と、乗算器２０２とを備える。

【０２４５】

選択回路２００は、読み出し回路１１から入力される中央値誤差信号の何れかのチャンネルを制御回路から入力される制御信号Ａに従い選択する。アップダウンカウンタ２０１は、選択回路２００により選択された中央値誤差信号の論理（図１９の出力Ｂの値である「１」または「－１」）に従いカウンタ値を増減する。つまり、アップダウンカウンタ２０１は中央値誤差信号の累積加算回路をなしている。

【０２４６】

乗算器２０２は、アップダウンカウンタ２０１の出力に所定の係数αを乗算して出力する。乗算器２０２の係数αは１より小さい値、例えば１／２，１／４，１／８などとすることで、中央値誤差信号の積算感度を変えることができる。なお、本明細書で言う「感度」とは、変化の程度、または変化率を言う。乗算器２０２は、感度調整回路と言うことができる。α値が大きいと抵抗中央値の検出の感度が増加し、上下動が大きく検出精度が悪化する。逆にα値が小さいと感度が下がり抵抗中央値の検出精度が増すものの検出にかか

る時間（読み出し回数）が増加する。α値はシステムによって最適に選択される。なお、アップダウンカウンタ２０１の初期値を、目標となる抵抗中央値にαを掛けた値にセットすることにより、検出時間が短縮化され得る。

【０２４７】

上述の処理を簡潔に説明すると、アップダウンカウンタ２０１は、選択されたメモリセルから取得した抵抗値情報と、演算途中の中央値（本明細書において「暫定中央値」と称することもある。）との差分を誤差として累積する。乗算器２０２は、カウンタの出力に所定の係数を乗算した値を新たな暫定中央値として更新する。これにより、適切な中央値を得ることができる。

【０２４８】

乗算器２０２から出力された中央値は、抵抗中央値として読み出し回路１１の入力端子Ａに出力される。

【０２４９】

なお、図２１に示されるような、誤差信号の累積加算回路をなすアップダウンカウンタ２０１と、誤差信号の累積における感度を調整する感度調整回路をなす乗算器２０２は一例である。また、累積加算回路の出力に感度調整回路が接続されるような接続関係についても限定されない。たとえば図２２に示される構成を採用することも可能である。

【０２５０】

図２２は、中央値検出回路２５の一変形例を示す。

【０２５１】

図２２に示す中央値検出回路２５は、選択回路２００に代わる全チャンネル加算器４０１と、乗算器２０２と、加算器４０２と、データラッチ回路４０３とを備えている。乗算器２０２は、全チャンネル加算器４０１と接続され、全チャンネル加算器４０１から出力される信号を受け取る。加算器４０２は、乗算器２０２の出力およびデータラッチ回路４０３の出力および入力と接続されている。加算器４０２は、乗算器２０２の出力およびデータラッチ回路４０３の出力を受け取って加算し、その加算結果をデータラッチ回路４０３に送る。

【０２５２】

データラッチ回路４０３は、加算器４０２の出力を受け取り、制御信号Ｂが指定するタイミングで受け取っていたデータをラッチする。なお、データラッチ回路４０３は、１ビットのラッチ回路を複数組み合わせることによって複数ビットの情報を記憶することが可能な回路である。ビット数は、その出力として必要とされるビット数に依存する。次に説明するように、本例ではデータラッチ回路４０３の出力は読み出し回路１１において抵抗中央値として利用される。データラッチ回路４０３は、少なくとも抵抗中央値を表現するために必要とされるビット数分の１ビットのラッチ回路を実装していればよい。

【０２５３】

この中央値検出回路２５の動作をより具体的に説明する。

【０２５４】

全チャンネル加算器４０１は、読み出し回路１１から入力されるＳチャンネルの抵抗値誤差信号を全て合算し、トータル誤差信号として出力する。乗算器２０２は、トータル誤差信号を受け取って、その信号に係数αを乗じる。乗算器２０２は、係数αにより、例えば１／２，１／４，１／８などのように誤差信号の感度を調整する。加算器４０２は、データラッチ回路４０３の出力と、乗算器２０２から出力された、感度が調節された誤差信号とを加算して、データラッチ回路４０３に出力する。

【０２５５】

データラッチ回路４０３は、制御信号Ｂによって指定されたタイミングで、加算器４０２から受け取った信号（データ）をラッチする。データラッチ回路４０３は、直前にラッチしたデータを、加算器４０２に送るとともに、読み出し回路１１の入力Ａにも送る。このデータは、読み出し回路１１において抵抗中央値として利用される。

【０２５６】

上述の動作から理解されるように、全チャンネル加算器４０１および乗算器２０２は、抵抗値誤差信号を累積する際の感度を調整する感度調整回路をなす。また、加算器４０２およびデータラッチ回路４０３は制御信号Ｂから入力されるタイミングに従って、１つ前の抵抗中央値と、感度が調節された抵抗値誤差信号とを加算して累積する累積加算回路をなす。

【０２５７】

図２１および図２２の例から明らかなように、感度調整回路と、抵抗値誤差信号の累積加算回路とを設けることに関し、各回路の具体的な構成、および各回路の接続関係は種々考えられる。上述の開示を踏まえると、当業者であればそのような変形例を設計することができる。本開示の趣旨に鑑みれば、現時点における抵抗中央値と、読み出された抵抗値情報との差分を抵抗値誤差信号として得て、その抵抗値誤差信号を累積する際の感度が調整でき、抵抗値誤差信号の累積結果を新たな抵抗中央値として更新する、１つの回路または組み合わされた複数の回路は、本開示の範疇である。

【０２５８】

図２３は、中央値検出回路２５が実際に抵抗中央値を算出した結果を示す。横軸にＰＵＦデータ領域８を読み出した回数、縦軸にアップダウンカウンタの値を示している。ＰＵＦデータ領域８の抵抗値情報を予め読み出しておき、計算機により中央値を算出した場合の理論値が１７であった。図からわかるように、読み出し回数が３０回あたりで、ほぼ理論値である１７に収束している様子が分かる。このように本開示の提案方式であれば抵抗値ばらつきの中央値を安定的に検出でき、中央値でもってディジタルＩＤデータ（ＰＵＦデータ）が良好に生成できる。

【０２５９】

抵抗値のばらつきから、中央値検出回路２５がその中央値を得るフローを第１のステップとする。この第１のステップは図１３のＳ４ステップと図１４のＳ９ステップに相当する。そして中央値の演算が完了した後、読み出し回路１１が再度各メモリセルの抵抗値情報を読み出し、中央値との関係からディジタルＩＤデータを生成する。これを第２のステップとすると、第２のステップは図１３のＳ５および図１４のＳ１０に相当する。なお、第２のステップには図１４のＳ１１，Ｓ１２，Ｓ１３を含んでも良い。

【０２６０】

上述の処理は、主として制御回路１５の制御および動作によって実現され得る。制御回路１５は、上述の処理が行われるよう各構成要素を制御することにより、ディジタルＩＤデータを更新する。より具体的には以下のとおりである。

【０２６１】

読み出し回路１１が個体識別情報を生成する際、読み出し回路１１は、新たに選択した予め定められた所定の数のメモリセルから抵抗値情報を取得する。中央値検出回路２５は、新たに取得された抵抗値情報を利用して新たに２値化基準値を算出する。その後、読み出し回路１１は、新たに選択した所定の数の異なるメモリセルから抵抗値情報を取得する。制御回路は、各抵抗値情報と２値化基準値の情報とを取得し、抵抗値情報と新たに算出された２値化基準値との関係に応じて個体識別情報を生成する。読み出し回路１１によって得られる抵抗値情報は、周辺の温度、装置電源電圧の変動、更には経年劣化によって逐次相対的に変動する。前述のように、ＰＵＦデータ領域８の抵抗値情報が読み出される度に、中央値を再取得することで、現在の最適な値に追従させることが可能になる。

【０２６２】

（中央値のオフセットによる複数のディジタルＩＤデータを得る方法の変形例）

次に中央値検出回路２５の変形例を説明する。

【０２６３】

図２４は、中央値検出回路２５の変形例の一例を示すブロック図である。図２４の構成要素のうち、図２１に記載されている構成要素と同じ構造および／または機能を有するものには同じ参照符号を付して、その説明は省略する。図２１の構成と比較して、図２４の中央値検出回路２５には、新たに加算器３００と切替器３０１とが追加されている。

【０２６４】
加算器３００には制御回路１５を介してオフセットが入力される。オフセットは、装置外部から入力され、または装置内部で生成される。加算器３００は、オフセットと乗算器２０２の出力とを加算し、加算結果を切替器３０１のｂ端子に出力する。
【０２６５】
切替器３０１のａ端子には乗算器２０２の出力が接続されている。切替器３０１は、制御回路１５から入力される制御信号Ｃに従って端子ａの信号を出力するか、端子ｂの信号を出力するかを選択的に切り替える。
【０２６６】
図２４において、前述した第１のステップでは、制御信号Ｃの設定により切替器３０１はａ端子に切り替える。つまり、第１のステップにおいては図２１と等しい動作が行われる。
【０２６７】
次に第２のステップ（図１３のＳ５および図１４のＳ１０）では、制御信号Ｃの設定により切替器３０１はｂ端子に切り替える。ｂ端子からは第１のステップで演算された抵抗中央値に制御回路１５から入力されるオフセットを加算した結果を示す信号が出力される。
【０２６８】
読み出し回路１１は、切替器３０１によって選択された端子からの出力である中央抵抗値を受け取り、ディジタルＩＤデータを生成する。ａ端子から出力された中央抵抗値を用いて生成されるディジタルＩＤデータと、ｂ端子から出力された、オフセットが加算された中央抵抗値を用いて生成されるディジタルＩＤデータとは、オフセットの有無に起因する差が存在し得る。
【０２６９】
オフセットが加算されないＩＤデータを第１のディジタルＩＤデータとし、オフセットが加算されたＩＤデータを第２のディジタルＩＤデータとする。第１ディジタルＩＤデータと第２ディジタルＩＤデータはデータパターンが異なり、更にそれらはいずれも装置固有のデータとして利用可能である。
【０２７０】
オフセットは、可変の値として中央値検出回路２５に入力することができる。すなわち、オフセット量を正負に変化させるだけでデータパターンの異なる複数のディジタルＩＤデータが複数生成できることになる。
【０２７１】
オフセット量が装置外部から入力されるならば、装置外部からの入力に対して異なるディジタルＩＤデータを返すことができる。これは、ＰＵＦ技術におけるチャレンジ・レスポンス認証に相当する。複数のＩＤデータはオフセット量に対して固有のデータとなり、そのレスポンスは物理的に複製できない関数であるＰＵＦに当たる。具体的なチャレンジ・レスポンス認証の例示は後述する。
【０２７２】
（ディジタルＩＤデータの乱数性を検定する変形例）
図２５は、本開示の実施形態の変形例を示す。図２５の構成要素のうち、図１８に記載されている構成要素と同じ構造および／または機能を有するものには同じ参照符号を付して、その説明は省略する。
【０２７３】
図２５に示される不揮発性メモリ装置１０には、新たに乱数検定回路３１０が追加されている。乱数検定回路３１０は、得られたディジタルＩＤデータの乱数性を検定するために設けられている。
【０２７４】
ディジタルＩＤデータの乱数性を検定する理由は、ハッキングにおけるフォルト攻撃（Fault Analysis Attack）対策のためである。フォルト攻撃とはＩＣのセキュアブロック

に対して強い電磁波またはレーザーを与え、回路に強制的な欠陥(fault)を与えて暗号器のアルゴリズムおよび鍵データを解析する攻撃である。例えばフォルト攻撃によりディジタルＩＤデータが全て１、または全て０のデータに変えられ、それを鍵データとして暗号化されると暗号データの解析が容易になる。または、正しいディジタルＩＤデータをデバイス鍵として利用して秘密鍵が暗号化されている場合に、フォルト攻撃によって得られたディジタルＩＤデータを用いて秘密鍵を復号化すると、その復号化プロセスが推測される恐れもある。その結果、秘密鍵が割り出される可能性がある。このような問題を未然に防ぐために、乱数検定回路による乱数性の検定が有効である。

【０２７５】

乱数検定回路３１０にはディジタルＩＤデータがｓビット単位で入力される。乱数検定にはχ二乗（カイ二乗）検定が用いられる。χ二乗検定とはｓビットのディジタルデータのうち４ビット単位で取り出し、４ビットで表される１６のディジタルデータパターンの頻度を累積する。０から１５のディジタル値の出現個数をカウントし、理論値の差分を積算し、積算値がゼロに近いほど乱数性が高いとされる。

【０２７６】

一般化したχ二乗演算について述べると、データパターンの取得個数をＡとしたときＤ＝Ａ÷ｎ（ｎはデータパターン数）となるＤが、各データパターンの取得個数の理想値となり、このとき（$X_n-D)^2\div D$（X_nは各データパターン毎の取得数）を、データパターン数ｎ分だけ累積した値がχ二乗値となる。具体的には例えば、４ビットで表されるデータパターンのχ二乗値を演算するとき、データパターンの種類は０～１５の１６通りある。ｓが３２ビットとのき、ｓビットを１６回取得すると合計５１２ビットのデータ数となる。５１２÷４＝１２８であることから、取得されるデータパターン数は１２８個となる。１２８個のデータパターンが均一に０～１５のパターンに分かれるのであれば、１２８÷１６＝８となり、各データパターンの取得個数の理想値Ｄは８となる。つまり、データパターン毎の取得個数がX_n（ｎは０から１５の整数）であるとき、全てのデータパターンごとに$(X_n-8)^2\div 8$を求め、全てを合計したものが、取得した５１２ビット分のχ二乗値となる。

【０２７７】

このように演算されたχ二乗値は、図２５のデータ入出力回路６に送られ、更に装置外に出力される。装置外ではχ二乗値が所定の値以下であることを検定し、得られたディジタルＩＤデータが暗号鍵等に用いられるレベルの乱数性があるかを確認し、問題なければ利用する。

【０２７８】

なお、不揮発性メモリ装置１０が、乱数検定回路３１０から得られた検定結果をもとに、たとえば制御回路１５などを用いて、生成した個体識別情報が利用可能か否かを装置外に通知してもよい。

【０２７９】

上述のように、乱数検定回路３１０を設けてデータの乱数性を検定することにより、フォルト攻撃等を受けた場合であっても、秘密鍵の窃取を未然に防ぐことができる。

【０２８０】

図２６は、メモリセルの規格化メモリセル電流と、本開示の読み出し回路で読み出した抵抗値情報の関係を示す。このときのメモリセル電流とは所定の読み出し電圧を印加したときのＤＣ電流を一般的なテスター装置で測定したものである。つまり、全てのメモリセルに対して値が等しければ等しい抵抗値であることを示している。図にプロットされた点は、同一チップ内にある１４４個のセンスアンプにより得られた抵抗値情報をまとめてプロットしたものである。図からわかるようにメモリセル電流と回路で得た抵抗値情報には明確な相関がない。つまり、チャンネルごとに、更にはＩＣごとにセンスアンプの特性がばらつき、絶対的な抵抗値と、回路により計測される抵抗情報との関係は、センスアンプごとに異なることを示している。センスアンプの特性は、アンプを構成するトランジスタのＶｔなどのばらつきにより発生する。通常であれば、このようなばらつきは抑制して均

一なセンスアンプにすることが望まれるが、ＰＵＦ技術に応用する場合は回路ばらつきをエンハンスするような設計が好ましい。例えば、図１９のＬＯＡＤ用トランジスタ３４のランダムばらつきが多くなるようなトランジスタサイズを用いるなどがあげられる。なお、ランダムばらつきを増やす手法は、種々考えられ設計事項であり割愛する。このようにセンスアンプのランダムばらつきが大きいと抵抗値の絶対値と、回路で得られる抵抗値情報とに明確な相関がなくなり、プローブなのでメモリセルを直接読み取られた場合であってもディジタルＩＤデータを予測することは困難になる。

【０２８１】

このように、本開示の構成によれば、ＰＵＦ技術の特徴である以下が満足できる。

特徴（１）：本開示の抵抗変化型不揮発性メモリ装置において、同一の抵抗値範囲にあるメモリセルの抵抗値のばらつきは、人為的に故意のデータパターンで書き込むことができないため、このような複製できない物理的な現象から固有のディジタルＩＤデータ（個体識別情報）得ることができる。

特徴（２）：本開示の抵抗変化型不揮発性メモリ装置において、ディジタルＩＤデータ（個体識別情報）に用いる抵抗値ばらつきはセンスアンプにより読み出される。センスアンプを構成するトランジスタには微細プロセス特有のランダムばらつきがあり、並列に読み出す各センスアンプごとのメモリセルの抵抗値情報は絶対値が異なる。従って、物理的に抵抗値を読み取ったとしてもセンスアンプを介して得た抵抗値情報と異なり、物理的には正しいディジタルＩＤデータを予測できない。すなわち、抵抗値ばらつきの物理的な現象は内部に搭載されているセンスアンプの動的な回路制御によってのみ得られる。

特徴（３）：メモリ素子である抵抗変化型メモリセルはパーコレーションモデルに基づく抵抗値揺らぎを備えており、得られたＩＤデータには誤りがあり、誤り訂正回路によってのみ真のＩＤデータが得られる。

【０２８２】

そして、本開示のＰＵＦ技術に基づいたディジタルＩＤデータには次の良好な性能がある。

性能（１）：前述の特徴（３）であるデータ誤り現象は、本開示の構成によれば、一回ごとの誤り率は２～３％と低いものの、累積の誤り率は読み出し回数に応じて１４％以上にも増加するため機械学習攻撃に対して極めて強いという良好な特徴をもつ。

性能（２）：抵抗値のばらつき分布が標準偏差の正規分布に従ってばらついている為、そこから得られるディジタルＩＤデータは良好な乱数性を示す。

性能（３）：本開示はＩＣおよびＳｏＣに搭載される不揮発性メモリ装置の回路を大部分共用しているため、回路増加が僅かであり、回路オーバーヘッドが小さくかつ、読み出し電流も小さい。

性能（４）：本開示はＩＣおよびＳｏＣに搭載される不揮発性メモリ装置を用いているため、並列読み出し数が多い。実施例では３２ｂｉｔ並列制御のメモリアレイでデータを取得したが、一回の読み出しが５００ｎｓ程度であり、生成速度は６４Ｍｂｐｓと非常に高速である。並列読み出し数が多いため、サイドチャネルアタックなどの電磁解析では各ビット状態を特定することが困難でハッキングに対する耐性が高い。

性能（５）：専用のメモリセルを用いないＳＲＡＭ-ＰＵＦ、およびグリッジＰＵＦのようにデータ誤り率が１５％に比べ、本開示の構成によれば誤り率が２～３％と小さい。このため誤り訂正回路の回路規模を小さくできる。

性能（６）：専用のメモリセルを用いないＳＲＡＭ－ＰＵＦのように、電源オン時のみ生成タイミングが制限されず、前述したように並列数によるが、一般的な並列数でも６４Ｍｂｐｓと非常に高速に生成できる。

【０２８３】

以上のように、本開示のＰＵＦ技術によって得られるディジタルＩＤデータは、一長一短ある従来のＰＵＦ技術とは異なり、必要な特徴と性能要件を全て満足する良好なディジタルＩＤデータを得ることができる。本願のディジタルＩＤデータを用いれば、前述した秘密鍵の安全な保管、および認証におけるセキュリティー性を向上できるとともに、ＩＣ

の複製などの脅威からユーザを確実に保護できる。

【０２８４】

（ＩＣカードへの応用例）

一つの応用例は、本開示により生成されるディジタルＩＤデータによる秘密鍵の暗号と、暗号化秘密鍵のフォーミングによる書き込みによるデータ隠蔽、さらに認証方法を開示する。

【０２８５】

図２７は、本開示の応用例にかかる通信システム５００の構成例を示すブロック図である。図２７において、通信システム５００は、リーダライタおよびデータサーバー５０１（以降、リーダライタと略す）と、ＩＣカード５０２とを備えている。リーダライタ５０１と、ＩＣカード５０２とは、例えば、それぞれが有するアンテナなどを介して無線による通信を行う。

【０２８６】

（リーダライタ側）

リーダライタ５０１は、ＲＡＭ５０３と、入出力インタフェース（Ｉ／Ｆ）部５０４と、ＣＰＵ５０５と、暗号処理回路５０６と、不揮発性メモリ装置５１５とを有している。

【０２８７】

リーダライタ５０１の入出力Ｉ／Ｆ部５０４は、外部との無線通信を行ってデータを送受信するためのインタフェースであり、たとえば無線通信回路として実現され得る。入出力Ｉ／Ｆ部５０４は、ＲＦアンテナを有している。入出力Ｉ／Ｆ部５０４は、所定の電磁波を輻射し、負荷の変化を利用して、ＩＣカード５０２が近づけられたか否かを検出する。また、入出力Ｉ／Ｆ部５０４は、例えば、発振回路（図示せず）から供給される所定の周波数の搬送波を、ＣＰＵ５０５から供給されるデータに基づいて変調する。入出力Ｉ／Ｆ部５０４は、該生成された変調波を、電磁波としてアンテナ（図示せず）から出力することで、近傍に配置されたＩＣカード５０２へと各種のデータを送信する。また、アンテナを介してＩＣカード５０２から送られた変調波を受信して復調し、得られたデータをＣＰＵ５０５に供給する。不揮発性メモリ装置５１５は、上述の不揮発性メモリ装置１０に対応する。不揮発性メモリ装置５１５は、秘密鍵記憶部５０８と、データ記憶部５０９と、ＲＯＭ部５１０と、固有ＩＤ記憶部５１１と、全ＩＣカード固有ＩＤ記憶部５４０とを備えている。

【０２８８】

ＲＯＭ部５１０は、本開示の不揮発性メモリ装置５１５が備える第２種データ記憶用メモリセル群のうちの所定のアドレス領域に相当する。リーダライタ５０１のＣＰＵ５０５は、ＲＯＭ部５１０に記憶されているプログラムをＲＡＭ５０３にロードし、該プログラムを用いて各種の処理を実行する。ＲＡＭ５０３にはＣＰＵ５０５が各種の処理を実行するために必要なデータなども一時的に記憶される。ＲＡＭ５０３は、ＳＲＡＭ（Static Random Access Memory）またはＤＲＡＭ（Dynamic Random Access Memory）などの揮発性記憶装置が用いられてもよい。あるいは、ＲＡＭ５０３は、本開示の不揮発性メモリ装置の第２種データ記憶用メモリセル群の一部で構成されていてもよい。

【０２８９】

固有ＩＤ記憶部５１１は本開示のディジタルＩＤデータの生成に用いるメモリセル群であり、リーダライタに固有のＩＤデータが本開示の方式により生成できる。さらに全ＩＣカード固有ＩＤ記憶部は、第１種データまたは第２種データで記憶されるメモリセル群で構成されており、運用される複数のＩＣカード５０２で異なるディジタルＩＤデータの全てが記憶されている。なお、全ＩＣカードのディジタルＩＤデータは、リーダライタ固有のディジタルＩＤデータを暗号鍵として暗号化されたデータで記憶されることが望ましい。

【０２９０】

ＣＰＵ５０５は、暗号処理回路５０６を制御することにより、予め定められた暗号アルゴリズムに基づいて、データの暗号化と復号化を行う。暗号アルゴリズムとしては、トリ

プルＤＥＳ（Data Encryption Standard）、ＡＥＳ（Advanced Encryption Standard）などが例示できる。これらは、いわゆる１つの秘密鍵を用いて暗号と復号を行う共通鍵暗号方式の暗号アルゴリズムである。また、ＲＳＡ暗号といった秘密鍵と公開鍵の２つの異なる鍵を用い、暗号化時の鍵と、復号化時の鍵を異ならせることで暗号通信を行う公開鍵方式でもよい。この場合は、後述する秘密鍵記憶部５０８に通信相手の公開鍵と、通信者自身の秘密鍵の両方を格納してもよい。これらの重要な鍵データは、固有ＩＤ記憶部５１１から生成される本開示のディジタルＩＤデータを暗号鍵として暗号化して、暗号化秘密鍵または暗号化公開鍵として格納することが望ましい。前述したようにＰＵＦ技術を用いて生成されたディジタルＩＤデータはリーダライタに固有であり、複製およびハッキングが困難である。従って、それを用いて暗号化された暗号化秘密鍵または暗号化公開鍵がコピーされてもディジタルＩＤデータがコピーできないＩＣ固有のデータであるため安全である。

【０２９１】

リーダライタ５０１においてデータの暗号化または復号化を行う場合、例えば、ＣＰＵ５０５は、不揮発性メモリ装置５１５内の所定のアドレス領域である秘密鍵記憶部５０８に記憶された暗号化秘密鍵を、本開示のディジタルＩＤデータを鍵として復号化し、元の秘密鍵を得て、暗号化または復号化すべきデータとともに、暗号処理回路５０６に供給する。暗号処理回路５０６は、供給された秘密鍵を用いてデータの暗号化または復号化を実行する。

【０２９２】

データ記憶部５０９は、ＣＰＵ５０５がプログラムを実行する上で必要なデータが記憶されている。データ記憶部５０９において、所定のデータは、本開示のディジタルＩＤデータを鍵として暗号化して記憶されていてもよい。なお、所定のデータは、初期状態のメモリセルを利用して記憶されていてもよいし、可変状態のメモリセルを利用して記憶されていてもよい。

【０２９３】

秘密鍵記憶部５０８としては、前述した第１種データ記憶用メモリセルを用いてもよいし、第２種データ記憶用メモリセルを用いてもよい。第２種データ記憶用メモリセル群９７を用いる場合は、他の一般的な不揮発性メモリを用いるのと大きな違いはない。第１種データ記憶用メモリセルを用いる場合は、抵抗変化素子の初期状態と可変状態との違いでデータを記憶するため、通常の読み出し閾値のコマンドではデータを読み出すことができない。よって、鍵情報の隠蔽が行える。第１実施形態で述べたように、可変状態にあるメモリセルから“０”と“１”のディジタルデータを読み出すためには、第２閾値を用いて“０”と“１”の判定が行なわれる。第２閾値で第１種データ記憶用メモリセル群９６を読み出すと、ほとんどのメモリセルが“０”にデコードされ、正規のデータを読み出せない。なお、秘密鍵記憶部５０８において、秘密鍵は、前述の暗号化秘密鍵として記憶されることが望ましい。

【０２９４】

また、メモリセルアレイ内の自由なアドレスに第１種データ記憶用メモリセル群９６と第２種データ記憶用メモリセル群９７とを配置できる。よって、プローブを用いて物理的に抵抗値を直接読み出すような解析を行おうとしても、そのメモリセルが第１種データ記憶用メモリセル群９６および第２種データ記憶用メモリセル群９７のいずれに属するのかを特定が困難である。更にディジタルＩＤデータで暗号化されたデータか、非暗号のデータかの区別が困難であるため、更に解析を複雑にせしめる。

【０２９５】

以上のように、図２７に示す通信システム５００は、秘密鍵の漏洩に対し強い耐タンパ性（tamper resistant）があるといえる。さらに第１種データ記憶用メモリセル、および本開示のディジタルＩＤデータは、高温においてのデータ信頼性にも優れ、データ誤りが許容されない秘密鍵の記憶および暗号化にも最適である。

【０２９６】

秘密鍵記憶部５０８に記憶される秘密鍵は、ＩＣカード５０２の秘密鍵記憶部５２６に記憶されている秘密鍵と同じものとされてもよい。ＩＣカード５０２に対応するリーダライタ５０１であって、ＩＣカード５０２に固有のディジタルＩＤデータであるカードＩＤの読み出しを許可されたリーダライタ５０１のみに、予め秘密鍵が記憶されていてもよい。

【０２９７】

固有のディジタルＩＤデータは、本開示の実施の形態で説明したＰＵＦ技術に基づき固有ＩＤ記憶部５２５にデータ誤りを内在した状態で記憶されている。

【０２９８】

固有ディジタルＩＤデータは前述したようにＩＣカードごとに固有の乱数になりうる。このため、ＩＣ固有の各種暗号化に用いることができる。

【０２９９】

（ＩＣカード側）

ＩＣカード５０２は、入出力インタフェース（Ｉ／Ｆ）部５２０と、ＣＰＵ５２１と、暗号処理回路５２２と、ＲＡＭ５２３と、不揮発性メモリ装置５３０とを有している。

【０３００】

ＩＣカード５０２の入出力Ｉ／Ｆ部５２０は、外部との無線通信を行ってデータを送受信するためのインタフェースであり、たとえば無線通信回路として実現され得る。入出力Ｉ／Ｆ部５２０は、例えば、コイル状のアンテナとコンデンサにより構成されるＬＣ回路が一般的に用いられる。ＩＣカードのアンテナがリーダライタ５０１に近づけられると、リーダライタ５０１から輻射される所定の周波数の電磁波と共振するようになっている。また、入出力Ｉ／Ｆ部５２０は、アンテナにおいて交流磁界により励起された電流を整流化および安定化し、ＩＣカード５０２の各部に直流電源として供給する。

【０３０１】

入出力Ｉ／Ｆ部５２０は、アンテナを介して受信した変調波を検波して復調し、復調後のデータをデコードしてディジタルデータに復元しＣＰＵ５２１に供給する。また、デコードしたディジタルデータに周波数と位相をロック（ＰＬＬと呼ばれるクロック再生技術：装置内部に電圧可変のオシレータが搭載されており、入力されたディジタルデータにあわせて、位相誤差を検出および積分して制御用の電圧を生成し、オシレータの制御電圧として入力することで入力されたデータのサンプリング周波数を一致させ、かつ位相も固定したクロックを得る。）させた受信用のクロック信号（図示せず）が発生し、ディジタルデータのデータラッチ用のクロック信号として供給される。

【０３０２】

さらに、入出力Ｉ／Ｆ部５２０は、所定の情報をリーダライタ５０１に送信する場合、ＣＰＵ５２１から入力されエンコードされたデータにしたがってアンテナの負荷に変動を発生させ変調し、アンテナを介してリーダライタ５０１に送信する。

【０３０３】

ＩＣカード５０２は本開示の不揮発性メモリ装置５３０を備える。不揮発性メモリ装置５３０は本実施形態の上述の不揮発性メモリ装置１０に対応する。よって以下の説明では、共通する要素については同一の符号および名称を付して適宜参照する。なお、本応用例では、不揮発性メモリ装置５３０が不揮発性記憶装置としても機能する。

【０３０４】

不揮発性メモリ装置５３０は、ＩＣカードごとに固有のディジタルＩＤデータを記憶する固有ＩＤ記憶部５２５と、秘密鍵データを記憶する秘密鍵記憶部５２６と、ＣＰＵ５２１がプログラムを実行する上で必要なデータが記憶されたデータ記憶部５２７と、ＣＰＵ５２１が実行するプログラムが記憶されたＲＯＭ部５２８とを備える。それらの全てが１個のメモリセルアレイ（図１のメモリセルアレイ９０、図１８および図２５のメモリセルアレイ２０）に包含されている。そして、ＣＰＵ５２１はＲＯＭ部５２８に記憶されているプログラムをＲＡＭ５２３にロードし、実行するなどして各種の処理を行う。ＲＯＭ部５２８に記憶されたプログラムデータは、固有ＩＤ記憶部にあるメモリセル群をもとに生

成される本開示のディジタルＩＤデータを鍵として用いて暗号化されて記憶されても良い。

【０３０５】

ＣＰＵ５２１は、暗号処理回路５２２を制御することにより、予め定められた暗号アルゴリズムに基づいて、データの暗号化と復号化を行う。上述したように、典型的な暗号方式には、送信側と受信側で同じ秘密鍵で暗号化と復号化を行う共通鍵方式と、異なる公開鍵と秘密鍵で暗号化と復号化を行う公開鍵方式がある。以下の説明では、共通鍵方式を採用した場合について説明する。

【０３０６】

なお、公開鍵方式では、ＩＣカード側が暗号化した暗号文データをＩＣカード５０２がリーダライタ５０１側に送信する場合は、予めリーダライタ５０１側から入手した公開鍵で暗号化する。逆に、リーダライタ５０１側から送られてきた暗号文データは、ＩＣカード５０２側で予め記憶してある秘密鍵にて復号する。以上の点以外は、公開鍵方式も共通鍵方式と同様である。公開鍵方式における公開鍵と秘密鍵は、互いに唯一のペアの鍵であるため、互いに暗号化されたデータを復号することで同時に相互認証もできることになる。

【０３０７】

ＩＣカード５０２においても、カードリーダでの説明と同様に秘密鍵記憶部５２６へ記憶する鍵データは、本開示のＰＵＦ技術に基づき固有ＩＤ記憶部５２５にあるディジタルＩＤデータにより暗号化された暗号化秘密鍵または暗号化公開鍵として保存される。更に、その記憶は第１種データ記憶用メモリセルにより記憶されうる。ＩＣカード５０２において、データの暗号化または復号化を行う場合、ＣＰＵ５２１が、不揮発性メモリ装置５３０内の第１種データ記憶用メモリセル群９６の一部である秘密鍵記憶部５２６に記憶された暗号化秘密鍵データを、図３の第１の閾値で読み出す特殊なリードコマンドにて読み出す。読み出された暗号化秘密鍵データは、本開示のディジタルＩＤデータにより復号化され元の秘密鍵データとされる。ＣＰＵ５２１は、秘密鍵データを、暗号化または復号化すべきデータとともに、暗号処理回路５２２に供給する。暗号処理回路５２２は、供給された秘密鍵を用いて、供給されたデータの暗号化または復号化を実行する。

【０３０８】

データ記憶部５２７は、ＣＰＵ５２１がプログラムを実行する上で必要なデータが記憶されている。データ記憶部５２７において、所定のデータが平文のまま記憶されていてもよいし、秘密鍵で暗号化されて記憶されていてもよいし、ディジタルＩＤデータを鍵として暗号化されて記憶されてもよい。なお、所定のデータは、初期状態のメモリセルを利用して記憶されていてもよいし、可変状態のメモリセルを利用して記憶されていてもよい。

【０３０９】

このような暗号化と復号化の機能を備えたＩＣカードシステムにおいて、ＩＣカード５０２とリーダライタ５０１との通信の第１ステップについて以下に述べる。

【０３１０】

ＩＣカード５０２において各ＩＣカード固有のディジタルＩＤデータは、本開示の実施の形態で説明したＰＵＦ技術に基づき固有ＩＤ記憶部５２５にデータ誤りを内在した状態で存在している。

【０３１１】

ＣＰＵ５２１は、各ＩＣカード固有のディジタルＩＤデータを固有ＩＤ記憶部５２５から生成する。ＣＰＵ５２１は、読み出した暗号化秘密鍵データとディジタルＩＤデータを鍵として暗号処理回路５２２に供給する。暗号処理回路５２２は供給されたディジタルＩＤデータを鍵として暗号化秘密鍵を元の秘密鍵に復号化する。そして、今度は元の秘密鍵を用いてディジタルＩＤデータを暗号化する。暗号化された暗号化ディジタルＩＤデータは入出力Ｉ／Ｆ部５２０、５０４を介して、リーダライタ側のＣＰＵ５０５に供給される。

【０３１２】

ＣＰＵ５０５は、リーダライタ５０１内の不揮発性メモリ装置５１５の秘密鍵記憶部５０８から、秘密鍵データを読み出す。ＣＰＵ５０５は、秘密鍵データと、受信した暗号化ディジタルＩＤデータを、暗号処理回路５０６に供給する。暗号処理回路５０６は、供給された秘密鍵データを用いて、暗号化ディジタルＩＤデータを復号化する。復号化されたディジタルＩＤデータは固有ＩＤ記憶部５１１が記憶している各ＩＤデータと照合される。各ＩＤデータの中に復号化されたＩＤデータと一致するものがあれば、通信したＩＣカード５０２がデータ通信を行う資格のある正規のＩＣカード５０２であると認証される。そして、その後のデータ通信が継続して実行される。

【０３１３】

リーダライタ５０１とＩＣカード５０２との相互認証において別の変形例を示す。

【０３１４】

リーダライタ５０１の全ＩＣカード固有ＩＤ記憶部５４０は、前述した中央値のオフセット量を変更して得られる複数のディジタルＩＤデータをＩＣカードごとに保管している。リーダライタ５０１は、オフセット量と、受け取りたいディジタルＩＤデータのアドレス情報を暗号化し、チャレンジデータとして、ＩＣカード５０２に送信する。ＩＣカード５０２は受け取ったチャレンジデータを復号化してオフセット量とアドレス情報を得て、それに応じたディジタルＩＤデータを暗号化し、レスポンスデータとしてリーダライタ５０１に返信する。

【０３１５】

リーダライタ５０１は受け取ったレスポンスデータを復号化して、ＩＣカード５０２ごとに固有のディジタルＩＤデータを、予め全ＩＣカード固有ＩＤ記憶部に登録されているＩＤデータと検索・照合を行い。所定のビット数以上が一致していることを確認してＩＣカードを認証する。

【０３１６】

レスポンスデータであるディジタルＩＤデータには、前述したような誤りデータを含んだ状態で送られるため、ハッキングに対して耐性が高い。ディジタルＩＤデータは、各ＩＣで異なる乱数でありデータ間に十分なハミング距離があれば所定のビット数の誤りデータがあったとしても何れのＩＣカードのＩＤデータかを特定することができる。このため、チャレンジデータの送信と、レスポンスデータの受信を繰り返すことで、ＩＣカードが正規のカードであることを特定できる。さらに認証に用いられているデータがＩＣカードごとに固有かつ誤りのあるデータであるためデータの解析が困難であり非常に高いセキュリティーが担保された認証が実現できる。

【０３１７】

以上のように、通信システム５００によれば、固有ディジタルＩＤデータ生成、秘密鍵記憶、データ記憶、プログラムデータ記憶の機能を、ただ一つの不揮発性メモリ装置で実現できる。別途ＰＵＦ技術に基づくＩＤ生成用の回路を搭載する必要がなく、回路規模の増加を極力抑制したＩＣカードのようなモバイル型アプリケーションが提供できる。

【０３１８】

ＲＡＭ５０３の機能を不揮発性メモリ装置５１５が備えるメモリセルアレイで実現してもよい。ＲＡＭ５２３の機能を不揮発性メモリ装置５３０が備えるメモリセルアレイで実現してもよい。

【０３１９】

情報の記憶手段として第１種データ記憶用メモリセルと第２種データ記憶用メモリセルとを任意に混在させて各種データを保存できるため、どのエリアのメモリセルが何れの状態で情報が記憶されているかを第三者に対し秘匿することができる。さらに、物理的なプローブを用いてメモリ内のデータを直接読み出すようなハッキングからもディジタルＩＤデータを防衛でき、極めて耐タンパ性の優れたアプリケーションが提供できる。

【０３２０】

なお、ディジタルＩＤデータを暗号鍵として用いて暗号化されたデータ（暗号化データ）が、ＩＣカード５０２に記憶されることは必須ではない。たとえば、リーダライタ５０

１が暗号化データを読み取り、リーダライタ５０１のデータ記憶部５０９が暗号化データを記憶してもよい。さらにリーダライタ５０１が暗号化データを外部に設けられたサーバ（図示せず）に送信し、そのサーバの記憶装置が記憶してもよい。暗号化データがＩＣカード５０２に記憶されていない場合には、復号化の手順は以下のとおりである。すなわち、ＩＣカード５０２のＣＰＵ５２１は、入出力Ｉ／Ｆ部５２０を介して外部に記憶されている暗号化データを受信する。またＣＰＵ５２１は、各ＩＣカード固有のディジタルＩＤデータを固有ＩＤ記憶部５２５から生成する。その後、暗号処理回路５２２が、ディジタルＩＤデータを復号鍵として用いて当該暗号化データを復号化する。

【０３２１】

上記説明から、当業者にとっては、本開示の多くの改良および他の実施形態が明らかである。従って、上記説明は、例示としてのみ解釈されるべきであり、本開示を具体化する最良の態様を当業者に教示する目的で提供されたものである。本開示の精神を逸脱することなく、その構造および／又は機能の詳細を実質的に変更できる。

【産業上の利用可能性】

【０３２２】

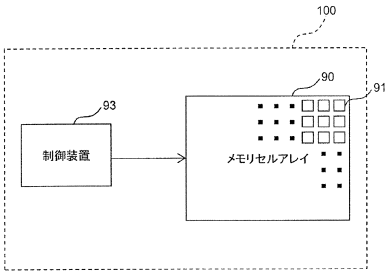
本開示にかかる不揮発性メモリ装置は、メモリ装置内部に含まれる抵抗変化型メモリ素子の抵抗値のばらつきから複製できない固有のディジタルＩＤデータを、安定かつ高セキュアに生成し、ディジタルＩＤデータを用いたデータ暗号及びホストコンピュータ及びサーバに認証を伴うアクセスを行うＩＣやＳｏＣなどへの搭載として有用である。

【符号の説明】

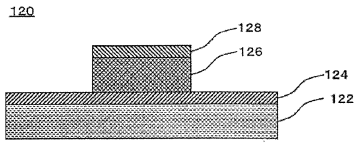
【０３２３】

６　データ入出力回路
１０　不揮発性メモリ装置
１１　読み出し回路
１４　書き込み回路
１５　制御回路
１６　アドレス入力回路
１７　カラムデコーダ回路
１８　ロウデコーダ回路
２０　メモリセルアレイ
２２　メモリ本体部
２５　中央値検出回路（演算回路）
３１０　乱数検定回路

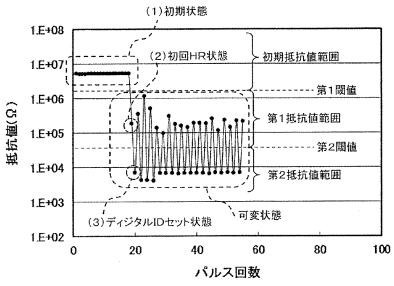
【図１】



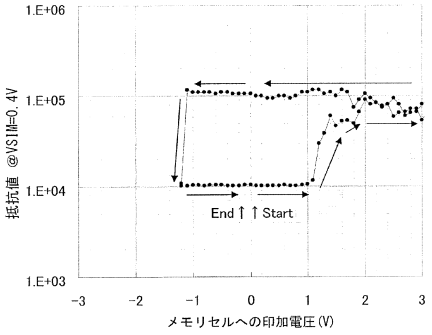
【図２】



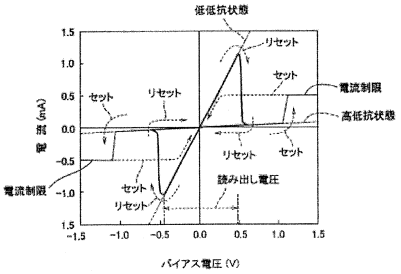
【図３】



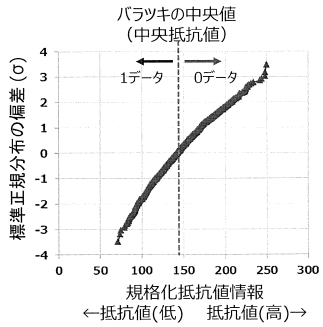
【図４】



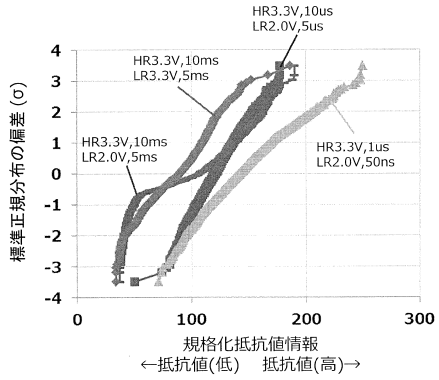
【図５】



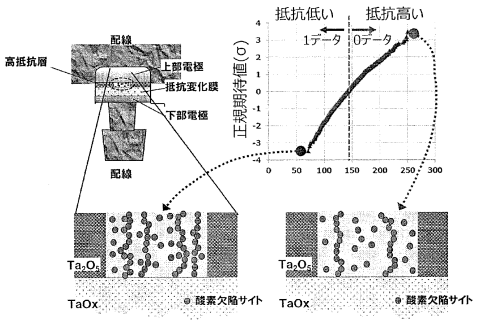
【図６】



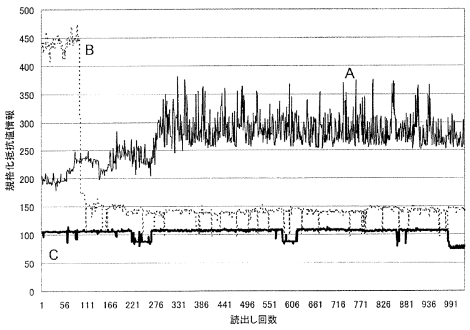
【図７】



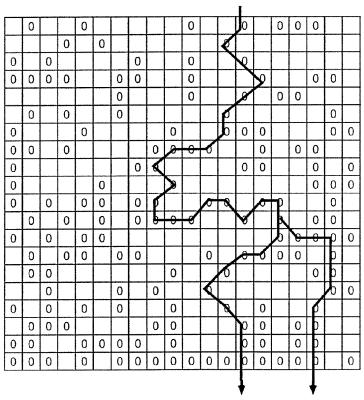
【図８】



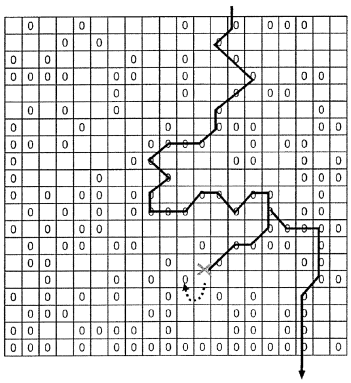
【図９】



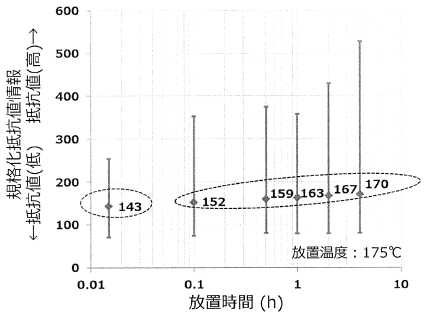
【図１０Ａ】



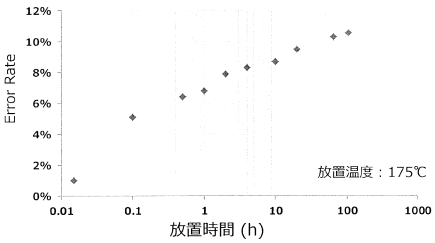
【図１０Ｂ】



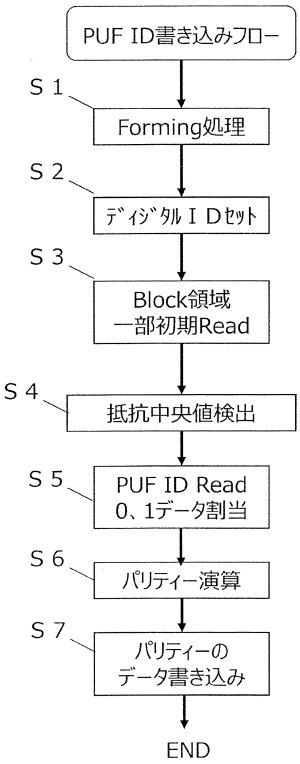
【図１１】



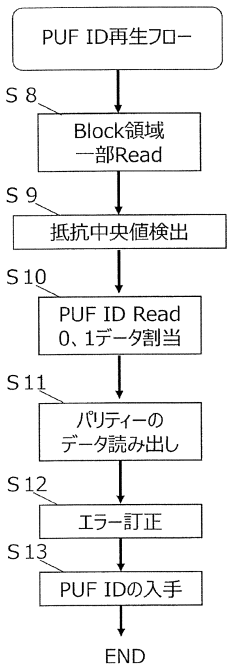
【図１２】



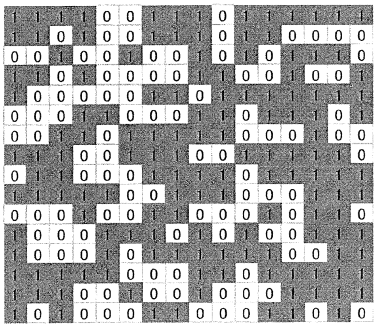
【図１３】



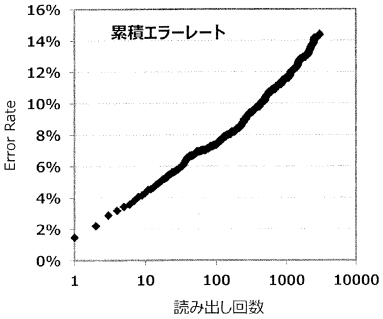
【図１４】



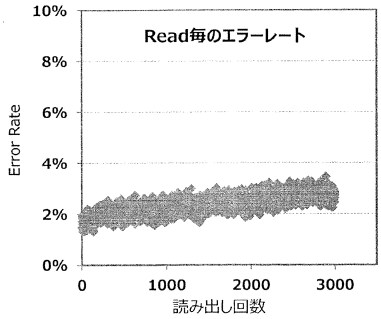
【図１５】



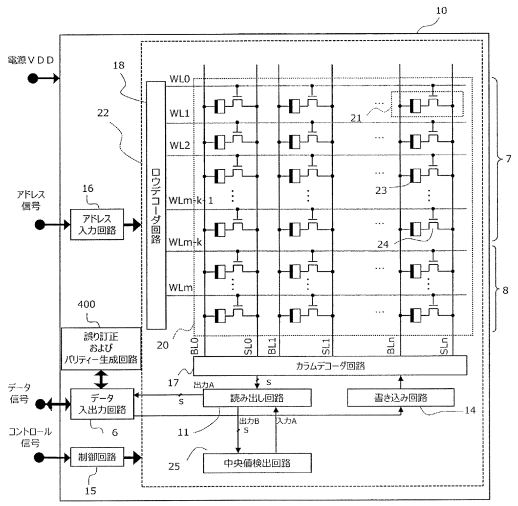
【図１７】



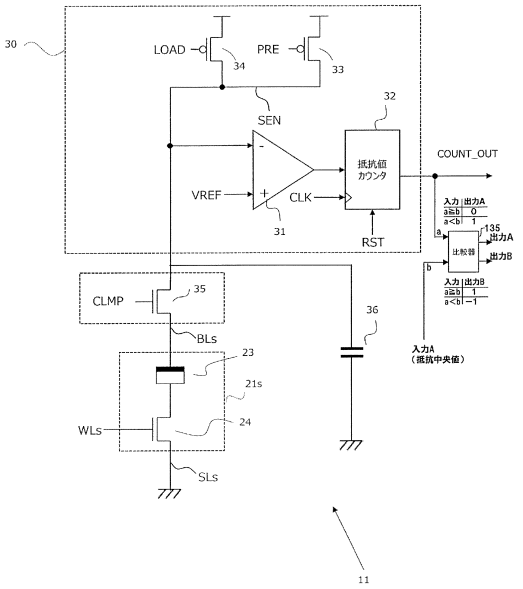
【図１６】



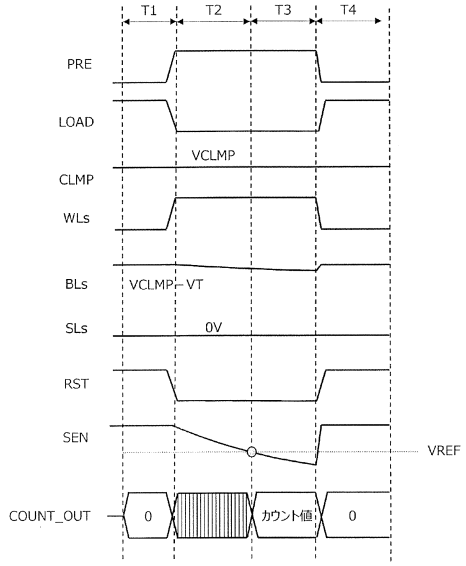
【図１８】



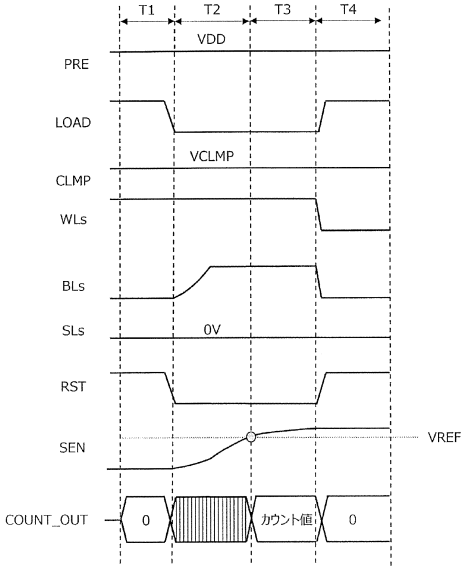
【図１９】



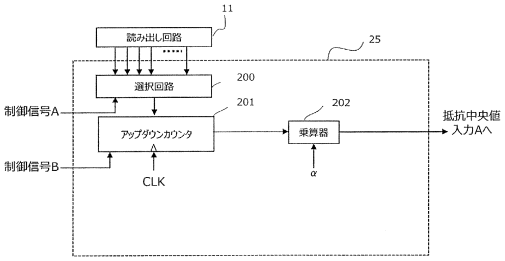
【図２０Ａ】



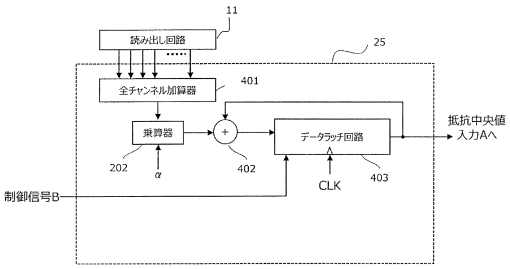
【図２０Ｂ】



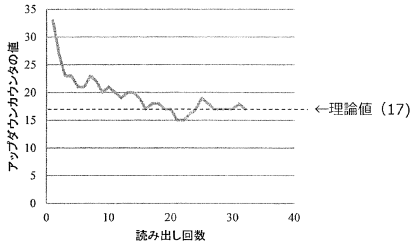
【図２１】



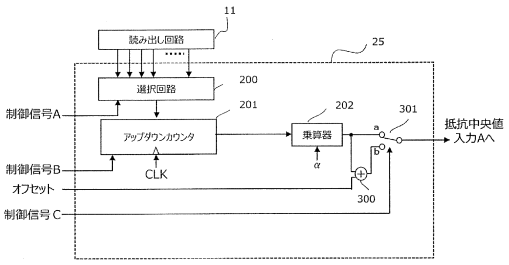
【図２２】



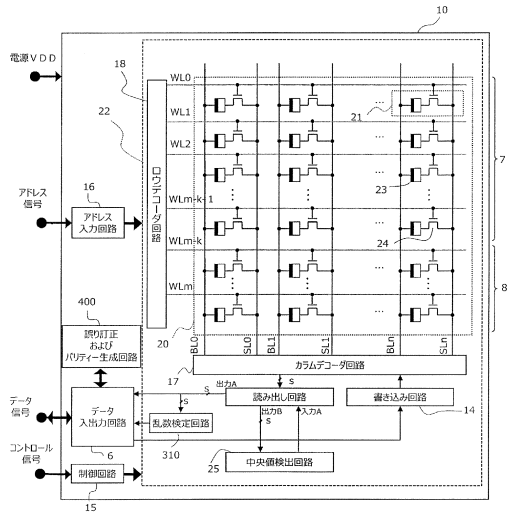
【図２３】



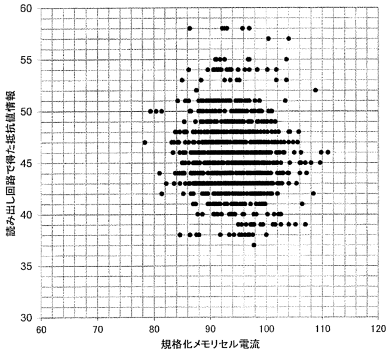
【図２４】



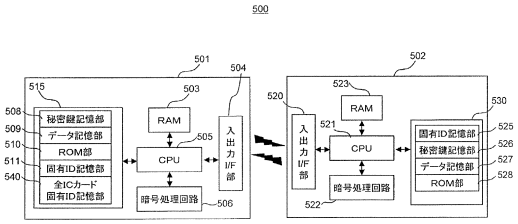
【図２５】


10
電源ＶＤＤ
18
22
WL0
WL1
WL2
WLm-k-1
WLm-k
WLm
21
23
24
7
8
アドレス信号
16
アドレス入力回路
ロウデコーダ回路
400
誤り訂正および パリティー生成回路
20
BL0
SL0
BL1
SL1
BLn
SLn
カラムデコーダ回路
17
出力A
S
データ信号
データ入出力回路
乱数検定回路
読み出し回路
書き込み回路
14
出力B
入力A
コントロール信号
制御回路
6
310
25
中央値検出回路
15

【図２６】


読み出し回路で得た抵抗値情報
規格化メモリセル電流
60
55
50
45
40
35
30
60
70
80
90
100
110
120

【図２７】


500
501
502
504
515
503
523
520
530
508
秘密鍵記憶部
RAM
RAM
509
データ記憶部
505
521
525
510
ROM部
CPU
入出力I/F部
CPU
固有ID記憶部
526
511
固有ID記憶部
秘密鍵記憶部
527
540
全ICカード固有ID記憶部
暗号処理回路
506
入出力I/F部
暗号処理回路
データ記憶部
528
ROM部
522

フロントページの続き

(74)代理人　100184985
　　弁理士　田中　悠
(72)発明者　加藤　佳一
　　京都府長岡京市神足焼町１番地　パナソニックセミコンダクターソリューションズ株式会社内
(72)発明者　吉本　裕平
　　京都府長岡京市神足焼町１番地　パナソニックセミコンダクターソリューションズ株式会社内
(72)発明者　小笠原　悟
　　京都府長岡京市神足焼町１番地　パナソニックセミコンダクターソリューションズ株式会社内

審査官　中里　裕正

(56)参考文献　国際公開第２０１４／１３２６６４（WO，Ａ１）
　　特開２０１３－２１８４８３（ＪＰ，Ａ）
　　特開２０１３－１０１４４２（ＪＰ，Ａ）
　　特開２０１２－０４３５１７（ＪＰ，Ａ）
　　特表２０１０－５２７２１９（ＪＰ，Ａ）
　　特開２０１０－２２６６０３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｌ　　９／１０
　　Ｇ１１Ｃ　　１３／００