(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7573902号
(P7573902)

(45)発行日　令和6年10月28日(2024.10.28)

(24)登録日　令和6年10月18日(2024.10.18)

(51)国際特許分類		FI		
H04L 9/10 (2006.01)		H04L	9/10	Z
G11C 13/00 (2006.01)		G11C	13/00	215
H10B 43/30 (2023.01)		H10B	43/30	
H01L 21/336 (2006.01)		H01L	29/78	371
H01L 29/788 (2006.01)				

請求項の数　7　（全14頁）　最終頁に続く

(21)出願番号　特願2023-65793(P2023-65793)
(22)出願日　令和5年4月13日(2023.4.13)
(65)公開番号　特開2023-181084(P2023-181084A)
(43)公開日　令和5年12月21日(2023.12.21)
審査請求日　令和5年4月13日(2023.4.13)
(31)優先権主張番号　10-2022-0070009
(32)優先日　令和4年6月9日(2022.6.9)
(33)優先権主張国・地域又は機関
韓国(KR)

(73)特許権者　517154199
インハ ユニバーシティ リサーチ アンド ビジネス ファウンデーション
ＩＮＨＡ ＵＮＩＶＥＲＳＩＴＹ ＲＥＳＥＡＲＣＨ ＡＮＤ ＢＵＳＩＮＥＳＳ ＦＯＵＮＤＡＴＩＯＮ
大韓民国 ２２２１２ インチョン、ミチョホルーグ、インハーロ、１００
(74)代理人　110001519
弁理士法人太陽国際特許事務所
(72)発明者　キム・ヒョンジン
大韓民国 ２２２１２ インチョン、ミチョホルーグ、インハーロ、１００
(72)発明者　パク・ジンウ
大韓民国 ２２２１２ インチョン、ミチ
最終頁に続く

(54)【発明の名称】　高信頼性物理的複製困難関数技術

(57)【特許請求の範囲】

【請求項１】

トンネリング基盤のメモリ素子であって、

下部電極（Ｂｏｔｔｏｍ　ｅｌｅｃｔｒｏｄｅ）上にAl_2O_3である伝導層が積層され、

前記伝導層上にTiO_xである酸化物層が積層され、

前記酸化物層上に上部電極（Ｔｏｐ　ｅｌｅｃｔｒｏｄｅ）が積層され、

メモリスタクロスバーアレイの構造を備え、

前記メモリスタクロスバーアレイは、ＡＬＤ（Ａｔｏｍｉｃ　Ｌａｙｅｒ　Ｄｅｐｏｓｉｔｉｏｎ）によるAl_2O_3蒸着時のサイクル回数とTiO_x蒸着時のスパッタリングO_2流量が、ｉ）１０ｃｙｃｌｅｓおよび０．８ｓｃｃｍ、またはｉｉ）１４ｃｙｃｌｅｓおよび０．８ｓｃｃｍである条件下で製造されたものであり、

前記メモリスタクロスバーアレイは、ハードウェアの予測することができない物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ：ＰＵＦ）をメモリ半導体アレイで構成するとき、前記伝導層と前記酸化物層とのトンネリングメカニズムによる外部環境変数である温度に独立的な電流－電圧特性を有し、

前記トンネリング基盤のメモリ素子は、

前記トンネリング基盤のメモリ素子の物理的複製防止のために、

トンネリング基盤の前記メモリスタクロスバーアレイの構造を備えるメモリ素子を利用して物理的複製困難関数を構成するためにチャレンジを印加し、

前記印加されたチャレンジを利用して電圧－電流特性によるレスポンスを抽出し、
予め登録されたレスポンスと前記抽出されたレスポンスとの確認による認証を実行し、
チャレンジ－レスポンスペアを形成するために、前記メモリスタクロスバーアレイの各ワードライン（ｗｏｒｄｌｉｎｅ）にチャレンジのデジタル信号に該当する電圧を印加することでメモリスタ素子の伝導度とベクトル、行列乗算によって各ビットライン（ｂｉｔｌｉｎｅ）に電流が流れるようにし、全体ビットラインから選択された半分のビットラインに流れる電流を加え、選択されなかった半分のビットラインに流れる電流を加えてそれぞれ互いに異なるレジスタに記録するように構成される、
トンネリング基盤のメモリ素子。

【請求項２】
前記伝導層の厚さを調節してトンネリング基盤の伝導メカニズムとして動作するステック構造を備える、
請求項１に記載のトンネリング基盤のメモリ素子。

【請求項３】
前記トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子は、温度に独立的な電流－電圧特性を有することにより、物理的複製困難関数のための保安認証過程でエラーが発生しないようにするＢＥＲ（Ｂｉｔ－Ｅｒｒｏｒ　Ｒａｔｅ）を減少させる、
請求項１に記載のトンネリング基盤のメモリ素子。

【請求項４】
トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子を利用して物理的複製防止関数を構成するためにチャレンジを印加する段階、
前記印加されたチャレンジを利用して電圧－電流特性によるレスポンスを抽出する段階、および
予め登録されたレスポンスと前記抽出されたレスポンスとの確認によって認証を行う段階
を含み、
前記メモリスタクロスバーアレイは、
下部電極（Ｂｏｔｔｏｍ　ｅｌｅｃｔｒｏｄｅ）上にAl_2O_3である伝導層が積層され、前記伝導層上にＴｉＯｘである酸化物層が積層され、前記酸化物層上に上部電極（Ｔｏｐ　ｅｌｅｃｔｒｏｄｅ）が積層され、ＡＬＤ（Ａｔｏｍｉｃ　Ｌａｙｅｒ　Ｄｅｐｏｓｉｔｉｏｎ）によるAl_2O_3蒸着時のサイクル回数とＴｉＯｘ蒸着時のスパッタリングO_2流量が、ｉ）１０ｃｙｃｌｅｓおよび０．８ｓｃｃｍ、またはｉｉ）１４ｃｙｃｌｅｓおよび０．８ｓｃｃｍである条件下で製造されたものであり、
前記トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子を利用して物理的複製防止関数を構成するためにチャレンジを印加する段階は、
チャレンジ－レスポンスペアを形成するために、前記メモリスタクロスバーアレイの各ワードライン（ｗｏｒｄｌｉｎｅ）にチャレンジのデジタル信号に該当する電圧を印加することでメモリスタ素子の伝導度とベクトル、行列乗算によって各ビットライン（ｂｉｔｌｉｎｅ）に電流が流れるようにし、全体ビットラインから選択された半分のビットラインに流れる電流を加え、選択されなかった半分のビットラインに流れる電流を加えてそれぞれ互いに異なるレジスタに記録する、
物理的複製防止方法。

【請求項５】
前記トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子は、メモリスタクロスバーアレイの構造を備え、ハードウェアの予測することができない物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ：ＰＵＦ）をメモリ半導体アレイで構成するとき、トンネリングメカニズムによる外部環境変数である温度に独立的な電流－電圧特性を有することにより、物理的複製困難関数のための保安認証過程でエラーが発生しないようにするＢＥＲ（Ｂｉｔ－Ｅｒｒｏｒ　Ｒａｔｅ）を減少させる、

請求項４に記載の物理的複製防止方法。
【請求項６】
前記印加されたチャレンジを利用して電圧－電流特性によるレスポンスを抽出する段階は、
前記選択されなかったワードラインとビットラインはフローティング（ｆｌｏａｔｉｎｇ）またはグラウンド（ｇｒｏｕｎｄ）に連結され、選択されなかった半分のビットラインに流れる電流を加える場合、選択された残りのビットラインはビットラインまたはグラウンドに連結され、
互いに異なるレジスタに記録された電流は電圧に換算され、比較器によって大小の比較を判断した後、０または１の１－ｂｉｔレスポンスを生成する、
請求項４に記載の物理的複製防止方法。
【請求項７】
前記予め登録されたレスポンスと前記抽出されたレスポンスとの確認によって認証を行う段階は、
メモリ半導体素子の駆動原理によって電圧－電流特性が決定され、製造上の工程偏差および素子間偏差により、同じ電圧が印加されたとしても同じ量の電流が流れる特徴を固有のレスポンスに活用して保安機能を実現する、
請求項４に記載の物理的複製防止方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、高信頼性物理的複製防止方法およびメモリアレイに関する。
【背景技術】
【０００２】
スマートフォンの大衆化に伴うユビキタス化によって情報が相互連結するようになりながら、敏感な情報や作業を処理する保安および認証などの分野ではソフトウェア保安方式によって暗号化を実現してきた。しかし、ＩｏＴ環境の拡散によってハッキングの危険性が高まりを見せ、個人情報の漏洩のように多くの保安事故が起こるようになりながら、安全な保安に対する要求が高まるようになった。
【０００３】
ディープラーニングやマシンラーニングなどの人工知能によってサーバに記録されたデータを予測できないようにするために、ハードウェア的に予測することができない製造工程偏差や本質的特性などを活用する物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ Ｕｎｃｌｏｎａｂｌｅ Ｆｕｎｃｔｉｏｎ：ＰＵＦ）の研究が活発に行われている。特に、メモリ半導体アレイを活用したＰＵＦの場合は、高い集積度と保安鍵の書き直しの可能性のために、近年は活発に研究がなされている。
【０００４】
メモリ素子の電圧－電流特性が素子間の散布および工程散布によってすべて異なる値を有し、隣接するメモリ素子の電流大小関係の予測は不可能であるということが、メモリアレイ基盤のＰＵＦの核心的な動作原理である。しかし、メモリ素子の電流－電圧関係が温度に大きく影響を受けるようになれば電流大小関係は逆転するようになり、これによって保安認証過程でエラーが発生することがある。通常はこのようなエラーをＢＥＲ（Ｂｉｔ－Ｅｒｒｏｒ Ｒａｔｅ）と言うが、高信頼性のＰＵＦ動作のためには、理想的にはこのＢＥＲが０でなければならない。本発明では、０に近いＢＥＲ動作を行うＰＵＦを実現するために、温度に独立的な電流－電圧特性を有するトンネリング基盤のメモリ素子、アレイで実現されるＰＵＦ技術を提案する。
【先行技術文献】
【特許文献】
【０００５】
【文献】韓国公開特許第１０－２０２０－００７５７２２号公報（２０２１年８月２０日）

【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明が達成しようとする技術的課題は、変化する外部環境要素である温度に対して脆弱なダイオードやトランジスタのような能動素子だけでなく、自由キャリアの伝導メカニズムが温度に影響を受ける素子のビットエラー率に対する誤差を大きく減らし、メモリアレイの並列演算とともに極めて信頼性のある動作実行を保障することができる、トンネリング基盤のメモリ半導体アレイ基盤の高信頼性物理的複製防止技術を提供することにある。
【課題を解決するための手段】
【０００７】
一側面において、本発明で提案するトンネリング基盤のメモリ素子は、下部電極（Ｂｏｔｔｏｍ ｅｌｅｃｔｒｏｄｅ）上に伝導層（例えば、Al_2O_3）が積層され、前記伝導層上に酸化物層（例えば、ＴｉＯｘ）が積層され、前記酸化物層上に上部電極（Ｔｏｐ ｅｌｅｃｔｒｏｄｅ）が積層され、メモリスタクロスバーアレイの構造を備え、ハードウェアの予測することができない物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ Ｕｎｃｌｏｎａｂｌｅ Ｆｕｎｃｔｉｏｎ：ＰＵＦ）をメモリ半導体アレイで構成するとき、トンネリングメカニズムによる外部環境変数である温度に独立的な電流－電圧特性を有する。
【０００８】
前記伝導層の厚さを調節してトンネリング基盤の伝導メカニズムとして動作するステック構造を備える。
【０００９】
前記トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子は、温度に独立的な電流－電圧特性を有することにより、物理的複製困難関数のための保安認証過程でエラーが発生しないようにするＢＥＲ（Ｂｉｔ－Ｅｒｒｏｒ Ｒａｔｅ）を減少させる。
【００１０】
また他の側面において、本発明で提案するトンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子の物理的複製防止方法は、トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子を利用して物理的複製防止関数を構成するためのチャレンジを印加する段階、前記印加されたチャレンジを利用して電圧－電流特性によるレスポンスを抽出する段階、および予め登録されたレスポンスと前記抽出されたレスポンスとの確認によって認証を行う段階を含む。
【００１１】
前記トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子は、メモリスタクロスバーアレイの構造を備え、ハードウェアの予測することができない物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ Ｕｎｃｌｏｎａｂｌｅ Ｆｕｎｃｔｉｏｎ：ＰＵＦ）をメモリ半導体アレイで構成するとき、トンネリングメカニズムによる外部環境変数である温度に独立的な電流－電圧特性を有することにより、物理的複製困難関数のための保安認証過程でエラーが発生しないようにするＢＥＲ（Ｂｉｔ－Ｅｒｒｏｒ Ｒａｔｅ）を減少させる。
【００１２】
前記トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子を利用して物理的複製防止関数を構成するためにチャレンジを印加する段階は、チャレンジ－レスポンスペアを形成するために前記メモリスタクロスバーアレイの各ワードライン（ｗｏｒｄｌｉｎｅ）にチャレンジのデジタル信号に該当する電圧を印加し、メモリスタ素子の伝導度とベクトル、および行列乗算によって各ビットライン（ｂｉｔｌｉｎｅ）に電流が流れるようにし、全体ビットラインから選択された半分のビットラインに流れる電流を加え、選択されなかった半分のビットラインに流れる電流を加えてそれぞれ互いに異なるレジスタに記録する。
【００１３】

前記印加されたチャレンジを利用して電圧－電流特性によるレスポンスを抽出する段階は、前記選択されなかったワードラインとビットラインはフローティング（ｆｌｏａｔｉｎｇ）またはグラウンド（ｇｒｏｕｎｄ）に連結され、選択されなかった半分のビットラインに流れる電流を加える場合、選択された残りのビットラインはビットラインまたはグラウンドに連結され、互いに異なるレジスタに記録された電流は電圧に換算され、比較器によって大小比較を判断した後、０または１の１－ｂｉｔレスポンスを生成する。

【００１４】

前記予め登録されたレスポンスと前記抽出されたレスポンスとの確認によって認証を行う段階は、メモリ半導体素子の駆動原理によって電圧－電流特性が決定され、製造上の工程偏差および素子間偏差により、同じ電圧が印加されたとしても異なる量の電流が流れる特徴を固有のレスポンスに活用して保安機能を実現する。

【発明の効果】

【００１５】

本発明の実施形態に係るトンネリング基盤のメモリ半導体アレイによって物理的複製防止機能を実行するようになれば、変化する外部環境要素である温度に対して脆弱なダイオードやトランジスタのような能動素子だけでなく、自由キャリアの伝導メカニズムが温度に影響を受ける素子に比べてビットエラー率に対する誤差を大きく減らすことができ、メモリアレイの並列演算とともに極めて信頼性のある動作実行を保障することができる。

【００１６】

本発明は、従来の保安方式として広く使用されているソフトウェア基盤の方式とは異なり、予測することのできないハードウェア物理的複製防止機能をメモリ半導体アレイで構成するとき、トンネリングメカニズムによって外部環境変数である温度に対して堅固な特性を有することができる信頼性を高め、物理的複製防止機能の活用先である暗号化鍵の生成または認証などにおいて安定的な動作に応用することができる。

【図面の簡単な説明】

【００１７】

【図１】本発明の一実施形態における、高信頼性物理的複製防止のためのトンネリング基盤のメモリ構造を示した図である。

【図１ｂ】本発明の一実施形態における、高信頼性物理的複製防止のためのトンネリング基盤のメモリ構造を示した図である。

【図２】本発明の一実施形態における、高信頼性物理的複製防止方法を説明するためのフローチャートである。

【図３ａ】本発明の一実施形態における、メモリスタクロスバーアレイ素子の温度特性を説明するための図である。

【図３ｂ】本発明の一実施形態における、メモリスタクロスバーアレイ素子の温度特性を説明するための図である。

【図３ｃ】本発明の一実施形態における、メモリスタクロスバーアレイ素子の温度特性を説明するための図である。

【図３ｄ】本発明の一実施形態における、メモリスタクロスバーアレイ素子の温度特性を説明するための図である。

【図４ａ】本発明の一実施形態における、トンネリング基盤のメモリスタクロスバーアレイ素子の特性を説明するための図である。

【図４ｂ】本発明の一実施形態における、トンネリング基盤のメモリスタクロスバーアレイ素子の特性を説明するための図である。

【図４ｃ】本発明の一実施形態における、トンネリング基盤のメモリスタクロスバーアレイ素子の特性を説明するための図である。

【図４ｄ】本発明の一実施形態における、トンネリング基盤のメモリスタクロスバーアレイ素子の特性を説明するための図である。

【発明を実施するための形態】

【００１８】

本発明は、トンネリングを支配的な伝導メカニズムとして活用することで、極めて安定的なチャレンジ（言い換えれば、入力）－レスポンス（言い換えれば、出力）ペアを抽出することができる、高信頼性ハードウェア基盤の保安技術である物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ：ＰＵＦ）技術を提案する。一般的にハードウェアで制作されるＰＵＦは、温度などの外部環境によって入力／出力特性が入れ替わる動作をする。特に、メモリ半導体アレイを活用する場合、メモリ素子の温度特性によって入力／出力特性が入れ替わるようになるが、これは、外部環境とは関係なく常に一定のチャレンジ－レスポンスを出さなければならないＰＵＦ動作にとって致命的である。温度による動作特性が鈍感なトンネリング現象を活用する場合、これを防ぐことができる。トンネリングは、トンネリング距離に依存して電流－電圧特性が決まるようになり、温度が関与する度合いが極めて低いため、メモリ素子がこれを基盤に駆動する場合、これによって構成されたＰＵＦのチャレンジ－レスポンス特性は外部環境の影響を極小に受けるようになり、安定的な保安入力／出力特性を得ることが可能となる。以下、本発明の実施例について、添付の図面を参照しながら詳しく説明する。

【００１９】

図１は、本発明の一実施形態における、高信頼性物理的複製防止のためのトンネリング基盤のメモリ構造を示した図である。

【００２０】

図１（ａ）は、本発明の一実施形態における、高信頼性物理的複製防止のためのトンネリング基盤のメモリ構造を示した図であり、図１（ｂ）は、本発明の一実施形態における、高信頼性物理的複製防止のためのトンネリング基盤のメモリアレイ基盤のＰＵＦを示した図である。

【００２１】

メモリ素子の電圧－電流特性が、素子間散布および工程散布によってすべて異なる値を有し、隣接するメモリ素子の電流大小関係は予測ができないという点が、メモリアレイ基盤のＰＵＦの核心動作原理である。しかしながら、メモリ素子の電流－電圧関係が温度に大きく影響を受ければ電流大小関係が逆転することがあり、これにより保安認証過程でエラーが発生するようになる。通常このようなエラーをＢＥＲ（Ｂｉｔ－Ｅｒｒｏｒ　Ｒａｔｅ）と言うが、高信頼性のＰＵＦ動作のためには理想的にこのＢＥＲが０でなければならない。

【００２２】

本発明では、０に近いＢＥＲ動作を行うＰＵＦの実現のために、温度に独立的な電流－電圧特性を有するトンネリング基盤のメモリ素子、アレイで実現されるＰＵＦ技術を提案する。

【００２３】

図１（ａ）を参照すると、本発明の実施形態に係るトンネリング基盤のメモリ素子は、下部電極（Ｂｏｔｔｏｍ　ｅｌｅｃｔｒｏｄｅ）１１０上に伝導層（例えば、Al_2O_3）１２０および酸化物層（例えば、ＴｉＯｘ）１３０を積層し、上部電極（Ｔｏｐ　ｅｌｅｃｔｒｏｄｅ）１４０として構成されるメモリスタクロスバーアレイで実現し、伝導層１２０の厚さを調節することで、トンネリングが支配的な伝導メカニズムで動作するステックを実現した。本発明の実施形態では、Al_2O_3およびＴｉＯｘがそれぞれ伝導層および酸化物層であるとして説明しているが、これに限定されてはならず、この他のトンネリングメカニズムを活用してＰＵＦ動作を可能する多様な物質が使用されてよい。

【００２４】

本発明の実施形態に係るトンネリング基盤のメモリ素子は、ハードウェアの予測することができない物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ　Ｕｎｃｌｏｎａｂｌｅ　Ｆｕｎｃｔｉｏｎ：ＰＵＦ）をメモリ半導体アレイで構成するとき、前記伝導層と前記酸化物層とのトンネリングメカニズムによる外部環境変数である温度に独立的な電流－電圧特性を有するようにする。

【００２５】

本発明の実施形態に係るトンネリング基盤のメモリ素子は、メモリスタ素子に限定されてはならず、トンネリングを主要メカニズムとする他の半導体素子およびアレイにも適用可能である。

【００２６】

図１（ｂ）を参照しながら、高信頼性物理的複製防止のためのトンネリング基盤のメモリ素子１５１を利用したメモリアレイ基盤のＰＵＦ１５０について説明する。

【００２７】

図１（ｂ）を参照すると、メモリ半導体アレイ基盤のＰＵＦは、チャレンジ１５２印加、レスポンス１５３抽出、登録されたレスポンス１５５との確認による認証１５４によって保安機能を実現する。ＰＵＦにチャレンジを印加してレスポンスを抽出する方法は多様であってよく、主に、ランダムな位置に電圧を印加した後、流れる電流を比較する形態である。メモリ半導体素子の駆動原理によって電圧－電流特性が決定され、製造上の工程偏差および素子間偏差などにより、同じ電圧を印加したとしても異なる量の電流が流れるようにしかならず、これを固有のレスポンスに活用して保安機能を実現する。

【００２８】

レスポンスは、外部環境によって変化しないことで信頼性のある保安認証を実現できるようになるが、メモリ半導体素子の一般的な伝導メカニズムであるディフュージョン、ドリフト、プール・フレンケル（ｐｏｏｌ－ｆｒｅｎｋｅ）伝導、ショッキー（ｓｃｈｏｔｋｋｙ）伝導などは、温度が増加するほど電流が変化するため（主に増加する方向）固有の出力を維持するのが難しく、ＢＥＲの主な要因となる。

【００２９】

本発明は、他の伝導メカニズムに比べて温度に対する敏感性が極めて低いトンネリングを活用したメモリ素子を活用することにより、ＰＵＦを構成する場合、温度が変化してもＰＵＦの出力特性に変化がほぼなく、信頼性の高いチャレンジ－レスポンスペアを構成することが可能な技術を提案する。

【００３０】

図２は、本発明の一実施形態における、高信頼性物理的複製防止方法を説明するためのフローチャートである。

【００３１】

提案するトンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子に対する高信頼性物理的複製防止方法は、トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子を利用して物理的複製防止関数を構成するためにチャレンジを印加する段階２１０、前記印加されたチャレンジを利用して電圧－電流特性によるレスポンスを抽出する段階２２０、および予め登録されたレスポンスと前記抽出されたレスポンスとの確認によって認証を行う段階２３０を含む。

【００３２】

図１を参照しながら説明したように、前記トンネリング基盤のメモリスタクロスバーアレイの構造を有するメモリ素子は、メモリスタクロスバーアレイの構造を備え、ハードウェアの予測することができない物理的複製困難関数（Ｐｈｙｓｉｃａｌｌｙ Ｕｎｃｌｏｎａｂｌｅ Ｆｕｎｃｔｉｏｎ：ＰＵＦ）をメモリ半導体アレイで構成するとき、トンネリングメカニズムによる外部環境変数である温度に独立的な電流－電圧特性を有することにより、物理的複製困難関数のための保安認証過程でエラーが発生しないようにするＢＥＲ（Ｂｉｔ－Ｅｒｒｏｒ Ｒａｔｅ）を減少させることができる。

【００３３】

段階２１０で、前記トンネリング基盤のメモリスタクロスバーアレイの構造を備えるメモリ素子を利用して物理的複製防止関数を構成するためにチャレンジを印加する。

【００３４】

本発明の実施形態によると、チャレンジ－レスポンスペアを形成するために、前記メモリスタクロスバーアレイの各ワードライン（ｗｏｒｄｌｉｎｅ）にチャレンジのデジタル信号に該当する電圧を印加してメモリスタ素子の伝導度とベクトル、および行列乗算によ

って各ビットライン（ｂｉｔｌｉｎｅ）に電流が流れるようにし、全体ビットラインから選択された半分のビットラインに流れる電流を加え、選択されなかった半分のビットラインに流れる電流を加えてそれぞれ互いに異なるレジスタに記録する。

【００３５】

段階２２０で、前記前記印加されたチャレンジを利用して電圧－電流特性によるレスポンスを抽出する。

【００３６】

本発明の実施形態によると、前記選択されなかったワードラインとビットラインは、フローティング（ｆｌｏａｔｉｎｇ）またはグラウンド（ｇｒｏｕｎｄ）に連結され、選択されなかった半分のビットラインに流れる電流を加える場合、選択された残りのビットラインがビットラインまたはグラウンドに連結される。互いに異なるレジスタに記録された電流は電圧に換算され、比較器によって大小比較を判断した後、０または１の１－ｂｉｔレスポンスを生成する。

【００３７】

段階２３０で、前記予め登録されたレスポンスと前記抽出されたレスポンスとの確認によって認証を実行する。

【００３８】

本発明の実施形態によると、メモリ半導体素子の駆動原理によって電圧－電流特性が決定され、製造上の工程偏差および素子間偏差により、同じ電圧が印加されたとしても異なる量の電流が流れる特徴を固有のレスポンスに活用することにより、保安機能を実現することができる。

【００３９】

図３は、本発明の一実施形態における、トンネリング基盤のメモリスタクロスバーアレイ素子の温度特性を説明するための図である。

【００４０】

本発明の実施形態に係るメモリスタクロスバーアレイの素子は、ＡＬＤ（Ａｔｏｍｉｃ Ｌａｙｅｒ Ｄｅｐｏｓｉｔｉｏｎ）により、Al_2O_3蒸着時にはサイクル回数、ＴｉＯｘの蒸着時にはスパッタリングO_2流量によって合計４つの条件を確認した。分割されたステックのうち、最も金属の伝導的な特性を有するスイッチングレイヤと酸素貯蔵所で構成されたＩＬ１（Ｉｎｓｕｌａｔｏｒ Ｌａｙｅｒ １）素子（図３ａ）、最も絶縁体の非伝導的な特性を有するスイッチングレイヤと酸素貯蔵所で構成されたＩＬ４素子（図３ｄ）、そしてその間のトンネリングメカニズムが支配的なＩＬ２素子（図３ｂ）とＩＬ３素子（図３ｃ）の温度変化による電流変化の傾向を読み取る方式によって分析して本発明の効果を検証した。図３ａを参照すると、ＩＬ１素子は１０ｃｙｃｌｅｓ ０．６ｓｃｃｍ、図３ｂを参照すると、ＩＬ２素子は１０ｃｙｃｌｅｓ ０．８ｓｃｃｍ、図３ｃを参照すると、ＩＬ３素子は１４ｃｙｃｌｅｓ ０．８ｓｃｃｍ、図３ａを参照すると、ＩＬ４素子は１７ｃｙｃｌｅｓ １．２ｓｃｃｍが測定された。

【００４１】

温度が増加するとき、図３ａのような伝導的な特性の素子は、ビットライン（ｂｉｔｌｉｎｅ）に流れる電流が減少し、図３ｄのような非伝導的な特性の素子は、ビットラインに流れる電流が増加する。温度によって電流が変化する特性は、出力特性のエラーに繋がる恐れがあり、安定的な保安動作の特性を妨害する。この反面、トンネリングメカニズムが支配的な２つの素子は、図３ｂと図３ｃで確認できるように、ＦＦ（Ｆｌｏａｔｉｎｇ－Ｆｌｏａｔｉｎｇ）読み取り方式の場合、ＧＧ（Ｇｒｏｕｎｄ－Ｇｒｏｕｎｄ）読み取り方式よりもクロスバーアレイで発生する漏洩電流（ｓｎｅａｋ ｃｕｒｒｅｎｔ）の量が多いため多少の変化傾向が現れることもあるが、温度変化に対しては電流の変化がほぼない。これにより、トンネリング基盤のメモリスタ素子は、温度変化に関係なくほぼ一定の電流を流すため安定的なチャレンジ－レスポンス動作が可能であり、これは物理的複製防止機能の低いＢＥＲに繋がる。

【００４２】

図４は、本発明の一実施形態における、トンネリング基盤のメモリスタクロスバーアレイ素子特性を説明するための図である。

【００４３】

本発明の実施形態に係るトンネリング基盤のメモリスタクロスバーアレイを活用して図４ａのようなシステムを構成した後にチャレンジ－レスポンスを確認した。図４に示した方式は一例に過ぎず、本発明がこの方式に限定されてはならない。

【００４４】

本発明の実施形態に係るチャレンジ－レスポンスペアを形成するために、各ワードライン（ｗｏｒｄｌｉｎｅ）にチャレンジのデジタル信号に該当する電圧を印加することでメモリスタ素子の伝導度とベクトル、行列乗算によって各ビットライン（ｂｉｔｌｉｎｅ）に電流が流れるようになり、全体ビットラインから選択された半分のビットラインに流れる電流を加え、選択されなかった半分のビットラインに流れる電流を加えてそれぞれ互いに異なるレジスタに記録する。

【００４５】

このとき、選択されなかったワードラインとビットラインは、フローティング（ｆｌｏａｔｉｎｇ）またはグラウンド（ｇｒｏｕｎｄ）に連結され、選択されなかった半分のビットラインに流れる電流を加える場合、選択された残りのビットラインがビットラインまたはグラウンドに連結される。２つのレジスタに記録された電流は電圧に換算され、比較器によって大小比較を判断した後、０または１の１－ｂｉｔレスポンスを生成する。チャレンジ－レスポンスが形成されるまで各ステップで印加されるスイッチ信号に対するタイミングダイヤグラムは、図４ｂのとおりとなる。

【００４６】

本発明の実施形態によって設計されたメモリスタクロスバーアレイ基盤の物理的複製防止機能に上述したような温度－電流特性を適用してビットエラー率を確認するためにハミング距離（Ｈａｍｍｉｎｇ　ｄｉｓｔａｎｃｅ）を比較した結果、図４ｃおよび図４ｄのように、トンネリング基盤の２つのステックであるＩＬ２とＩＬ３は相対的に低いＢＥＲを示すことが確認できたし、特に、最もビットエラー率が低い素子の場合は、すべての温度に対して１％未満のＢＥＲを達成することが確認できた。一般的なメモリスタ素子の特性を備える絶縁膜基盤の素子ＩＬ４は、温度の上昇によって５％を超えるＢＥＲを示し、安定的なＰＵＦの動作が困難であることが分かった。

【００４７】

上述した装置は、ハードウェア構成要素、ソフトウェア構成要素、および／またはハードウェア構成要素とソフトウェア構成要素との組み合わせによって実現されてよい。例えば、実施形態で説明された装置および構成要素は、例えば、プロセッサ、コントローラ、ＡＬＵ（ａｒｉｔｈｍｅｔｉｃ　ｌｏｇｉｃ　ｕｎｉｔ）、デジタル信号プロセッサ、マイクロコンピュータ、ＦＰＧＡ（ｆｉｅｌｄ　ｐｒｏｇｒａｍｍａｂｌｅ　ｇａｔｅ　ａｒｒａｙ）、ＰＬＵ（ｐｒｏｇｒａｍｍａｂｌｅ　ｌｏｇｉｃ　ｕｎｉｔ）、マイクロプロセッサ、または命令を実行して応答することができる様々な装置のように、１つ以上の汎用コンピュータまたは特殊目的コンピュータを利用して実現されてよい。処理装置は、オペレーティングシステム（ＯＳ）およびＯＳ上で実行される１つ以上のソフトウェアアプリケーションを実行してよい。また、処理装置は、ソフトウェアの実行に応答し、データにアクセスし、データを記録、操作、処理、および生成してもよい。理解の便宜のために、１つの処理装置が使用されるとして説明される場合もあるが、当業者であれば、処理装置が複数個の処理要素および／または複数種類の処理要素を含んでもよいことが理解できるであろう。例えば、処理装置は、複数個のプロセッサまたは１つのプロセッサおよび１つのコントローラを含んでよい。また、並列プロセッサのような、他の処理構成も可能である。

【００４８】

ソフトウェアは、コンピュータプログラム、コード、命令、またはこれらのうちの１つ以上の組み合わせを含んでもよく、思うままに動作するように処理装置を構成したり、独立的または集合的に処理装置に命令したりしてよい。ソフトウェアおよび／またはデータ

は、処理装置に基づいて解釈されたり、処理装置に命令またはデータを提供したりするために、いかなる種類の機械、コンポーネント、物理装置、仮想装置（Ｖｉｒｔｕａｌ ｅｑｕｉｐｍｅｔ）、コンピュータ記録媒体または装置に具現化されてよい。ソフトウェアは、ネットワークによって接続されたコンピュータシステム上に分散され、分散された状態で記録されても実行されてもよい。ソフトウェアおよびデータは、１つ以上のコンピュータ読み取り可能な記録媒体に記録されてよい。

【００４９】

実施形態に係る方法は、多様なコンピュータ手段によって実行可能なプログラム命令の形態で実現されてコンピュータ読み取り可能な媒体に記録されてよい。前記コンピュータ読み取り可能な媒体は、プログラム命令、データファイル、データ構造などを単独でまたは組み合わせて含んでよい。前記媒体に記録されるプログラム命令は、実施形態のために特別に設計されて構成されるものであってもよいし、コンピュータソフトウェアの当業者に公知されて使用可能なものであってもよい。コンピュータ読み取り可能な記録媒体の例としては、ハードディスク、フロッピー（登録商標）ディスク、および磁気テープのような磁気媒体、ＣＤ－ＲＯＭおよびＤＶＤのような光媒体、フロプティカルディスク（ｆｌｏｐｔｉｃａｌ ｄｉｓｋ）のような光磁気媒体、およびＲＯＭ、ＲＡＭ、フラッシュメモリなどのようなプログラム命令を記録して実行するように特別に構成されたハードウェア装置が含まれる。プログラム命令の例としては、コンパイラによって生成されるもののような機械語コードだけではなく、インタプリタなどを使用してコンピュータによって実行される高級言語コードを含む。

【００５０】

以上のように、実施形態を、限定された実施形態および図面に基づいて説明したが、当業者であれば、上述した記載から多様な修正および変形が可能であろう。例えば、説明された技術が、説明された方法とは異なる順序で実行されたり、かつ／あるいは、説明されたシステム、構造、装置、回路などの構成要素が、説明された方法とは異なる形態で結合されたりまたは組み合わされたり、他の構成要素または均等物によって対置されたり置換されたとしても、適切な結果を達成することができる。

【００５１】

したがって、異なる実施形態であっても、特許請求の範囲と均等なものであれば、添付される特許請求の範囲に属する。

【符号の説明】

【００５２】

１１０：下部電極

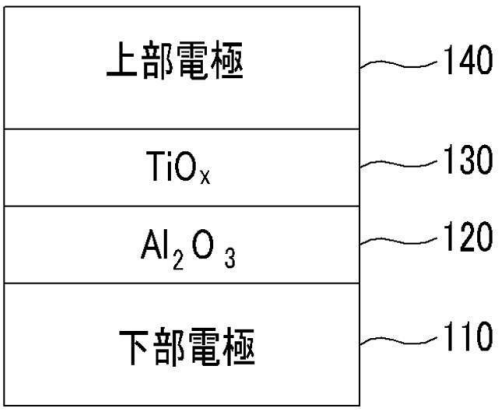
１２０：Al_2O_3

１３０：Tio_x

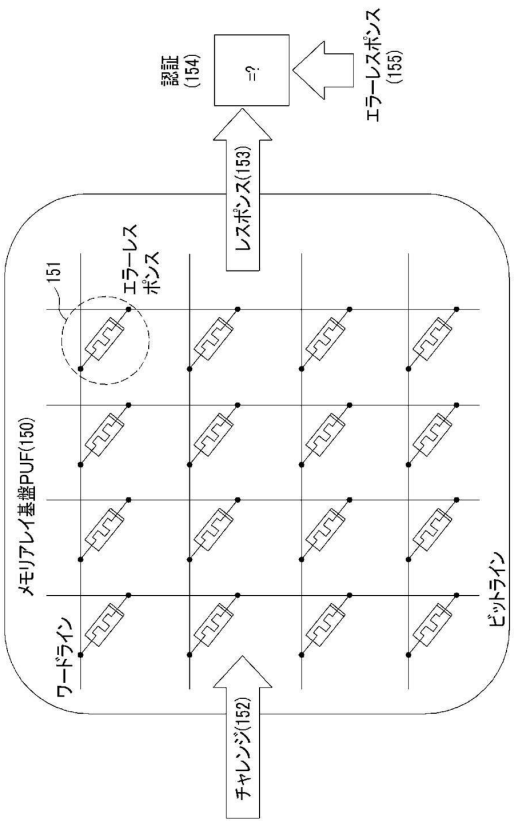
１４０：上部電極

【図面】

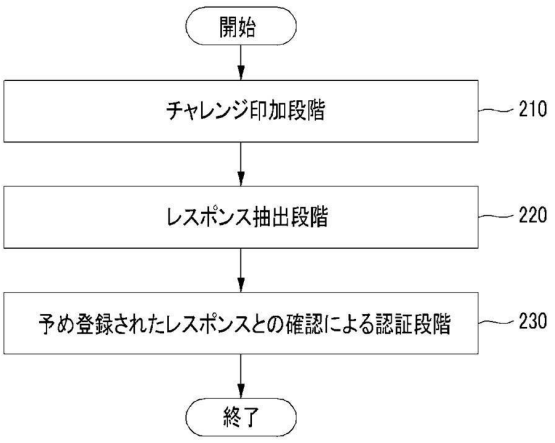
【図１】



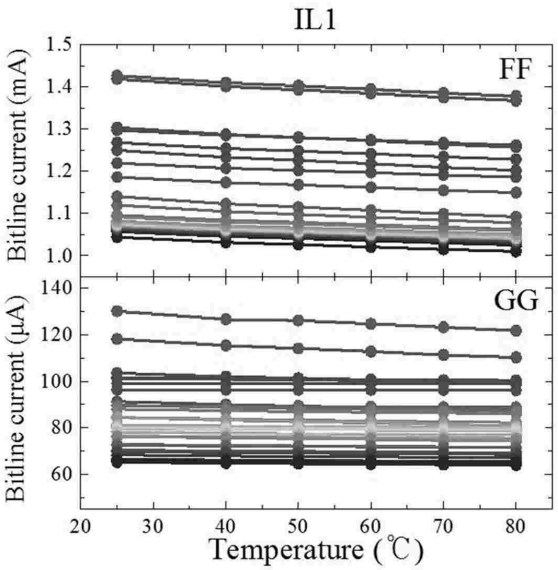
【図１ｂ】



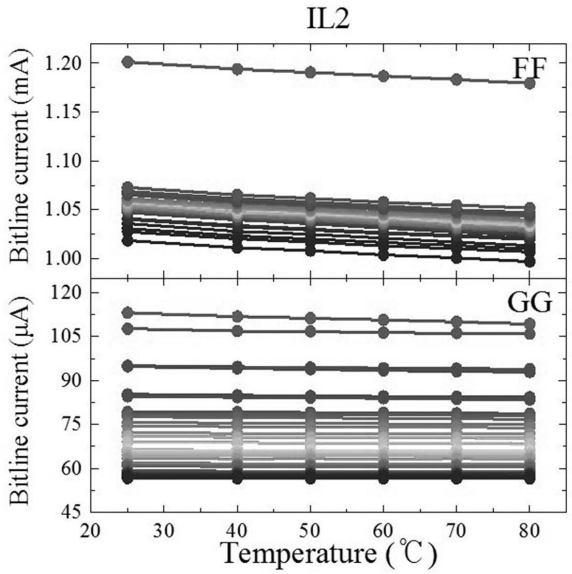
【図２】



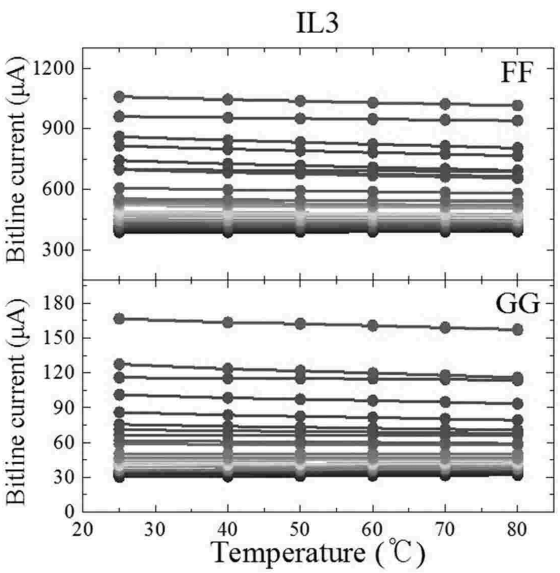
【図３ａ】



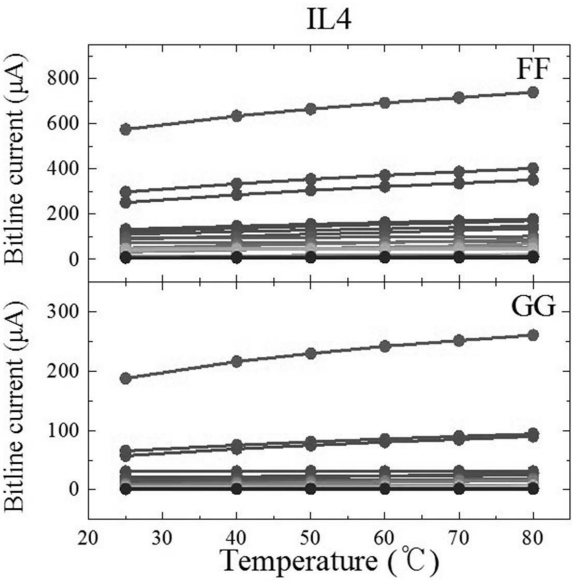
【図３ｂ】



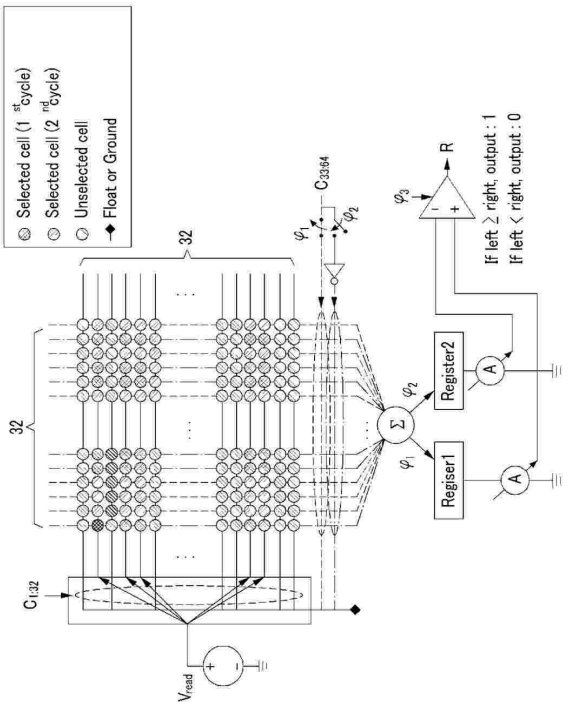
【図３ｃ】



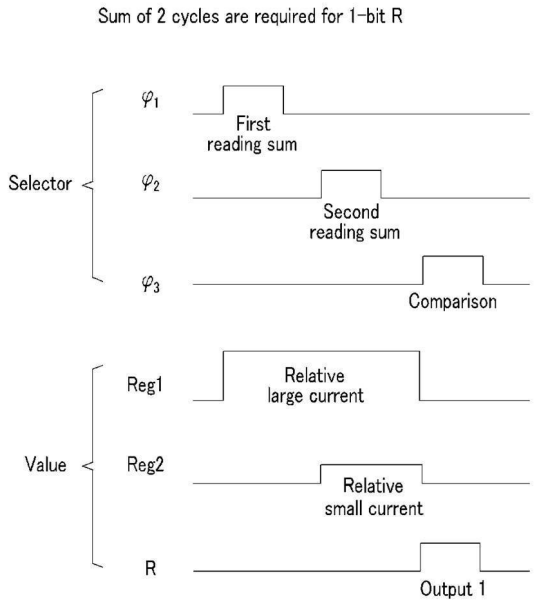
【図３ｄ】



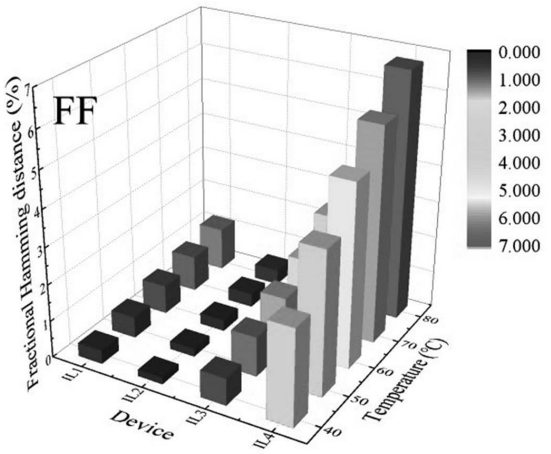
【図４ａ】



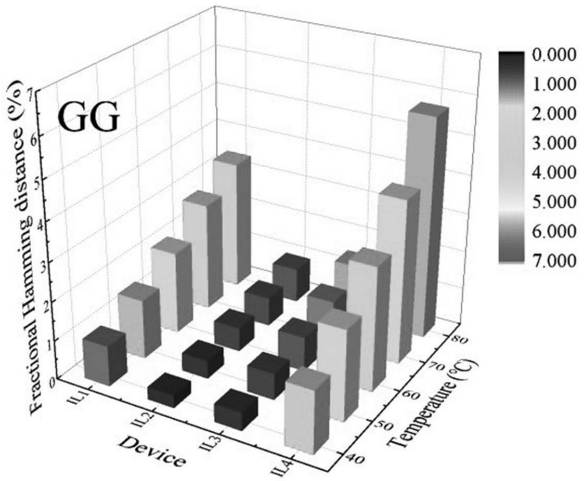
【図４ｂ】


Sum of 2 cycles are required for 1-bit R
Selector
φ1
First reading sum
φ2
Second reading sum
φ3
Comparison
Value
Reg1
Relative large current
Reg2
Relative small current
R
Output 1

【図４ｃ】


FF
Fractional Hamming distance (%)
Device
Temperature (℃)
0.000
1.000
2.000
3.000
4.000
5.000
6.000
7.000

【図４ｄ】


GG
Fractional Hamming distance (%)
Device
Temperature (℃)
0.000
1.000
2.000
3.000
4.000
5.000
6.000
7.000

フロントページの続き

(51)国際特許分類　　ＦＩ
Ｈ０１Ｌ　29/792(2006.01)

ョホルーグ、インハーロ、１００

審査官　金沢 史明

(56)参考文献　国際公開第２０２０／２１２６８９（WO，Ａ１）
米国特許第１０８０３９４２（ＵＳ，Ｂ１）
KIM, Dayoung et al.，Selected Bit-Line Current PUF: Implementation of Hardware Security Primitive Based on a Memristor Crossbar Array，IEEE Access [online]，2021年，Volume 9，pp. 120901-120910，[2024年5月22日検索], インターネット〈URL: https://ieeexplore.ieee.org/document/9524627〉，〈DOI: 10.1109/ACCESS.2021.3108534〉

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／１０，９／３２
Ｇ１１Ｃ　１３／００
Ｇ０６Ｆ　２１／７５
Ｈ１０Ｂ　４３／３０
Ｈ０１Ｌ　２３／００