(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-31297
(P2020-31297A)
(43)公開日　令和2年2月27日(2020.2.27)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/10	(2006.01)	H04L	9/00	621Z	5F083
G11C	13/00	(2006.01)	G11C	13/00	200	5J104
G06F	7/58	(2006.01)	G06F	7/58	680	
G06F	21/73	(2013.01)	G06F	21/73		
H01L	27/11507	(2017.01)	H01L	27/11507		

審査請求 未請求　請求項の数 15　ＯＬ　（全 25 頁）　最終頁に続く

(21)出願番号　特願2018-154477 (P2018-154477)
(22)出願日　平成30年8月21日 (2018.8.21)

(71)出願人　504132272
国立大学法人京都大学
京都府京都市左京区吉田本町３６番地１
(74)代理人　100111567
弁理士　坂本　寛
(72)発明者　佐藤　高史
京都府京都市左京区吉田本町３６番地１
国立大学法人京都大学内
(72)発明者　田中　悠貴
京都府京都市左京区吉田本町３６番地１
国立大学法人京都大学内
(72)発明者　辺　松
京都府京都市左京区吉田本町３６番地１
国立大学法人京都大学内

最終頁に続く

(54)【発明の名称】ＰＵＦ回路群，ＰＵＦ回路群の製造方法，ＰＵＦ回路の使用方法，及びネットワークシステム

(57)【要約】
【課題】サーバへのＣＲＰデータの保存を不要化する．
【解決手段】開示される回路群は，物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を複数含むＰＵＦ回路群であって，前記ＰＵＦ回路群に含まれる複数の前記ＰＵＦ回路それぞれは，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ．
【選択図】図４

図4A

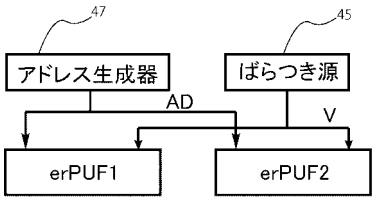


図4B

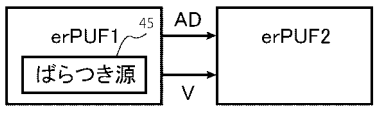
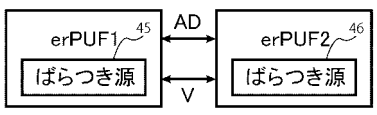


図4C



【特許請求の範囲】
【請求項１】
物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を複数含むＰＵＦ回路群であって，
前記ＰＵＦ回路群に含まれる複数の前記ＰＵＦ回路それぞれは，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ
ＰＵＦ回路群．
【請求項２】
複数の前記ＰＵＦ回路それぞれは，共通の物理的なばらつきに基づく，互いに等価な物理的特性を保持しており，
複数の前記ＰＵＦ回路それぞれのＣＲＰは，前記物理的特性に基づいて定まっている
請求項１に記載のＰＵＦ回路群．
【請求項３】
複数の前記ＰＵＦ回路それぞれは，前記物理的特性を保持する不揮発性メモリを有する
請求項２に記載のＰＵＦ回路群．
【請求項４】
前記不揮発性メモリは，メモリスタ，フラッシュメモリ及び強誘電体メモリからなる群から選択される一つのメモリであるである
請求項３に記載のＰＵＦ回路群．
【請求項５】
複数の前記ＰＵＦ回路それぞれは，共通のチップから複数の前記ＰＵＦ回路が切断により分離されたときの切断痕を有する
請求項１～４のいずれかに記載のＰＵＦ回路群．
【請求項６】
物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を複数含むＰＵＦ回路群の製造方法であって，
共通の物理的なばらつきに基づく物理的特性を，複数のデバイスそれぞれに保持させることで，複数の前記デバイスを，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ複数のＰＵＦ回路にする設定工程を含む
ＰＵＦ回路群の製造方法．
【請求項７】
前記設定工程の前に，複数の前記デバイスを一体的に備えるチップを製造する工程を更に含み，
前記物理的特性は，前記チップが有する物理的なばらつきに基づく物理的特性である
請求項６に記載の製造方法．
【請求項８】
前記設定工程の後に，前記チップ中の複数の前記ＰＵＦ回路を分離する工程を更に含む
請求項７に記載の製造方法．
【請求項９】
前記物理的特性は，複数の前記デバイスにおける少なくとも２つのデバイスそれぞれが有する物理的なばらつき相互の関係に基づく物理的特性である
請求項６から請求項８のいずれか１項に記載の製造方法．
【請求項１０】
前記物理的特性は，複数の前記デバイスにおける特定のデバイスの物理的なばらつきに基づく物理的特性である
請求項６から請求項８のいずれか１項に記載の製造方法．
【請求項１１】
前記物理的特性は，複数の前記デバイス以外のばらつき源の物理的なばらつきに基づく物理的特性である
請求項６から請求項８のいずれか１項に記載の製造方法．

【請求項１２】
複数の前記デバイスそれぞれは，前記物理的特性を保持する不揮発性メモリを有する
請求項６から請求項１１のいずれか１項に記載の製造方法．
【請求項１３】
前記不揮発性メモリは，メモリスタ，フラッシュメモリ及び強誘電体メモリからなる群から選択される一つのメモリである
請求項１２に記載の製造方法．
【請求項１４】
通信ネットワークにより接続された複数の拠点それぞれが，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を使用する
ことを含む方法．
【請求項１５】
通信ネットワークにより接続された複数の拠点それぞれが，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を有する
ネットワークシステム．
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は，ＰＵＦ回路群，ＰＵＦ回路群の製造方法，ＰＵＦ回路の使用方法，及びネットワークシステムに関する．
【背景技術】
【０００２】
ＰＵＦ(Physical Unclonable Function)は，あるチャレンジ(入力値，c)を与えると，対応するレスポンス(出力値，ｒ)を返す関数$r=f_{\alpha}(c)$として機能する．ただし，チャレンジとレスポンスの対応（ＣＲＰ: challenge response pair）はＰＵＦ回路が有する物理的なばらつきαに依存して決まるため，従来のＰＵＦ回路においては，同じチャレンジに対するレスポンスはＰＵＦ回路ごとに異なり，人工的な複製が困難となる．そのためＰＵＦ回路は，個体認証や暗号プロトコルにおける使用が期待され，更には小規模な回路で実現可能である特徴からIoTデバイスのセキュリティ等，様々なセキュリティシステムでの応用が期待されている．なお，以下では，ＰＵＦ回路を単に，「ＰＵＦ」ということがある．
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】B. Gassend, D. Clarke, M. van Dijky, and S. Devadas, “Silicon physical random functions,” in Proc. Computer and Communication Security Conf., 2002, pp. 148-160.
【非特許文献２】G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in Proc. DAC, 2007, pp. 9-14.
【発明の概要】
【０００４】
従来のＰＵＦを用いる認証方式では，サーバにあるＣＲＰとユーザが持つＰＵＦのレスポンスを比較することで認証を行う．この認証方式ではユーザがＰＵＦを所有する一方で，サーバはユーザが所有するＰＵＦのＣＲＰデータを保存する必要がある．しかし，サーバにおけるＣＲＰデータの保存には，ＰＵＦからＣＲＰデータを読み出す際，および読み出し後にこれを保管する際にかかるコスト（時間や保管のための記憶領域）を必要とする課題がある．しかも，サーバに保存すべきＣＲＰデータ量が非常に大きくなる場合もある．したがって，サーバへのＣＲＰデータの保存を不要化することが望まれる．

【０００５】
さらに，ＰＵＦ回路の応用によっては，サーバを介さずに，ユーザ間で認証を行いたい場合がある．これは，例えば，ユーザ間の通信は容易であるがサーバとの通信が困難である場合，サーバとユーザ間の通信経路の安全性が保証できない場合，サーバに悪意がないことを保証できない場合等である．これらの場合，サーバとの通信を行わずに認証を行うことができるのが望ましい．かかる観点からも，サーバへのＣＲＰデータの保存を不要化することが望まれる．
【０００６】
本開示の一側面は，物理的複製困難関数（ＰＵＦ）回路を複数含むＰＵＦ回路群であって，前記ＰＵＦ回路群に含まれる複数の前記ＰＵＦ回路それぞれは，互いに等価なチャレンジレスポンスペア（ＣＲＰ）を持つＰＵＦ回路群である．
【０００７】
本開示の他の側面は，物理的複製困難関数回路を複数含むＰＵＦ回路群の製造方法であって，共通の物理的なばらつきに基づく物理的特性を，複数のデバイスそれぞれに保持させることで，複数の前記デバイスを，互いに等価なＣＲＰを持つ複数のＰＵＦ回路にする設定工程を含むＰＵＦ回路群の製造方法である．
【０００８】
本開示の更に他の側面は，通信ネットワークにより接続された複数の拠点それぞれが，互いに等価なＣＲＰを持つ物理的複製困難関数回路を使用することを含む方法である．
【０００９】
本開示の更に他の側面は，通信ネットワークにより接続された複数の拠点それぞれが，互いに等価なＣＲＰを持つ物理的複製困難関数回路を有するネットワークシステムである．
【００１０】
更なる詳細は，後述の実施形態として説明される．
【図面の簡単な説明】
【００１１】
【図１】図１は，ＰＵＦの機能を提供するICチップの構成例及びＰＵＦを用いた認証システム例を示す図である．
【図２】図２は，等価なレスポンスを返すＰＵＦの例を示す図である．
【図３】図３は，等価なＣＲＰをもつＰＵＦを示す図である．
【図４】図４は，ｅｒＰＵＦ対の作成方法の概念図である．
【図５】図５は，製造フローの例を示す図である．
【図６】図６は，クロスカップリング型の基本回路構造を示す図であり，図６ＡはNMOS型を示し，図６ＢはPMOS型を示す．
【図７】図７は，ストレス時の状態を示す図であり，図７ＡはNMOS型を示し，図７ＢはPMOS型を示す．
【図８】図８は，ｅｒＰＵＦ対中の1ビットを生成する書き込み波形であり，図８ＡはNMOS型を示し，図８ＢはPMOS型を示す．
【図９】図９は，読み出し時の回路構造を示す図であり，図９ＡはNMOS型を示し，図９ＢはPMOS型を示す．
【図１０】図１０は，クロスカップリング型ｅｒＰＵＦ回路の全体構成図である．
【図１１】図１１は，クロスカップリング型ｅｒＰＵＦ対のアレイ回路図である．
【図１２】図１２は，クロスカップリング型ｅｒＰＵＦ対アレイ回路におけるセルの回路構造図であり，図１２ＡはNMOS型を示し，図１２ＢはPMOS型を示す．
【図１３】図１３は，書き込み制御回路図である．
【図１４】図１４は，信号制御回路図である．
【図１５】図１５は，ｅｒＰＵＦ回路の値設定におけるタイミングチャートである．
【図１６】図１６は，読み出し制御回路図である．
【図１７】図１７は，インバータリング型ｅｒＰＵＦセルの基本回路構造図である．

【図１８】図１８は，インバータリング型ｅｒＰＵＦセルの基本回路構造図である．
【図１９】図１９は，メモリスタを用いたｅｒＰＵＦグループ構成のためのセルの基本回路構造である．
【図２０】図２０は，ｅｒＰＵＦグループ構成のためのセルの基本回路構造である．
【図２１】図２１は，SRAMメモリセルの特性ばらつきの自己修復の説明図であり，図２１Ａは，SRAMメモリセルの原理的な回路図であり，図２１Ｂは，インバータの入出力特性を示し，図２１ＣはSRAMメモリセルの安定性を評価するバタフライカーブを示す．
【図２２】図２２は，NBTIを用いるｅｒＰＵＦセルの基本構造図である．
【図２３】図２３は，セキュア通信におけるｅｒＰＵＦの使用例を示す図である．
【発明を実施するための形態】
【００１２】
＜１．従来のＰＵＦ＞
【００１３】
理解の容易のため，実施形態の説明に先立ち，まず，従来のＰＵＦについて説明する．
【００１４】
＜１．１　ＰＵＦを有するＩＣチップ＞
【００１５】
ＰＵＦは，典型的には電子回路として実現され，それ自体で単機能のＩＣチップとして製造される場合，およびマイコンなどのＰＵＦ以外の回路とともにＩＣチップ内に組み込まれる場合等がある．
【００１６】
図１Ａは，ＰＵＦを単機能のＩＣチップ１として実現する場合の例を示している．ＩＣチップ１は，複数ビット（ここではnビット）からなるチャレンジＣを，入力回路２を通して受け取り，複数ビット（ここではmビット）からなるレスポンスＲを，出力回路４を介して出力する．入力回路２と出力回路４において直列－並列変換や並列－直列変換等を行うことにより，ＩＣチップ１に同時に入力されるチャレンジＣのビット数とＰＵＦ回路３に入力されるチャレンジのビット数はそれぞれ異なっていてもよい．また，ＩＣチップ１から同時に出力されるレスポンスＲのビット数とＰＵＦ回路３から出力されるレスポンスＲのビット数はそれぞれ異なっていても良い．
【００１７】
図１Ｂは，マイコン回路５とともにＰＵＦ回路３を有するチップ６として実現する場合の例を示している．この例では，外部からの要求に応じて，または外部から与えられたチャレンジＣ’に応じて，マイコン回路５がＰＵＦ回路３と通信を行い，チャレンジＣ’に対するレスポンスＲ’を得る．
【００１８】
図１Ａの単機能のＩＣチップ１は，例えばソケット等を介してプリント基板上に接続され，認証システムの一部をなす場合もある．単機能のＩＣチップ１は，ＵＳＢメモリやＳＤカードのような挿抜可能な形に実装されて可搬性を与えられるとともに，システムに組み込まれる．
【００１９】
図１Ｃは，認証制御回路を用いてＰＵＦの単機能ＩＣチップ１と通信を行う場合を示している．携帯電話等の主要回路２２に設けられた認証制御回路２１から単機能のＩＣチップ１に対しチャレンジＣを入力し，レスポンスＲを得ることで認証を行う．
【００２０】
＜１．２　ＰＵＦの応用例＞
【００２１】
ＰＵＦを用いてチップの認証を行う場合には，例えば以下の手順を取る．まず，チップ製造者が，製造したチップに搭載されているＰＵＦについて，認証を行う回数と等しいかそれよりも十分大きい回数分のＣＲＰを調べ記録し，製造者のサーバにＣＲＰデータのデータベースを作成しておく．チップ購入者がチップの認証を行う際には，製造者のサーバ

に認証の要求を行う．製造者のサーバは作成したデータベースからあるチャレンジｃを選び，ネットワークを介して，ＰＵＦに送信する．ＰＵＦは受け取ったチャレンジｃからレスポンスｒを得て，製造者のサーバにレスポンスｒを返す．最後に製造者のサーバは受け取ったレスポンスｒとデータベース内のｒ’を照合し，一致すれば正規品と判定する．

【００２２】

ｎ者（ｎ＞２）のユーザ認証を行う場合も同様にして，ユーザそれぞれが持つＰＵＦとサーバが持つユーザごとのＣＲＰデータベースとを用いる．各ユーザがサーバとの間でチャレンジとレスポンスを交換する通信を繰返してサーバが各ユーザを認証すれば，サーバを介してユーザ同士を認証することができる．

【００２３】

ＣＲＰを秘密鍵として用い，一般的な暗号アルゴリズムと組み合わせる等の方法も提案されている．従来手法では，サーバがＣＲＰデータを保持し，ユーザが物理的なＰＵＦを保持することを前提として手続きが定義されている．

【００２４】

上記のように，従来のＰＵＦの応用では，サーバへのＣＲＰデータの保存が必須であり，サーバへのＣＲＰデータの保存を不要化することが望まれる．

【００２５】

＜２．実施形態に係るＰＵＦ回路群，ＰＵＦ回路群の製造方法，ＰＵＦ回路の使用方法，及びネットワークシステムの概要＞

【００２６】

（１）実施形態に係る回路群（回路グループ）は，物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を複数含むＰＵＦ回路群である．ＰＵＦ回路群は，２又はそれ以上のＰＵＦ回路の集合である．実施形態において，前記ＰＵＦ回路群に含まれる複数の前記ＰＵＦ回路それぞれは，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ．異なる回路群（回路グループ）間では，従来のＰＵＦと同様に，ＣＲＰが異なる．すなわち，前記ＰＵＦ回路それぞれは，前記ＰＵＦ回路群において固有のＣＲＰを持ち，ＰＵＦ回路群内においては，各ＣＲＰが等価である．等価なＣＲＰを持つＰＵＦ回路群を使用することで，サーバへのＣＲＰデータの保存が不要となる．

【００２７】

ここで，「複数のＰＵＦ回路が等価なＣＲＰを持つ」とは，複数のＰＵＦ回路それぞれに同一のチャレンジが与えられたときに，複数のＰＵＦ回路のレスポンスが極めて強く相関することを意味する．相関は，正でも負でもよい．すなわち，「複数のＰＵＦ回路が等価なＣＲＰを持つ」とは，同一のチャレンジに対して，複数のＰＵＦ回路が常に完全に同一であるレスポンスを返すこと，または複数のＰＵＦ回路のレスポンスが互いに論理反転関係にあるなど，自明な変換によりそれぞれのレスポンスが実質的に同一であるととみなすことができる，ことを意味する．

【００２８】

図２は，実質的に同一のレスポンスを返すとみなせるＰＵＦ，および同一のレスポンスとはみなせないＰＵＦのＣＲＰの例を示している．図２では，チャレンジの一部c0,c1,...,c14,...に対するＰＵＦ１，ＰＵＦ２，ＰＵＦ３，ＰＵＦ４，ＰＵＦ５のレスポンスが示されている．ＰＵＦ１とＰＵＦ２のレスポンスは全て等しく，図示していないチャレンジに対しても同様にレスポンスが全て等しければ，ＰＵＦ１とＰＵＦ２のＣＲＰは明らかに完全同一であり，ＰＵＦ１とＰＵＦ２は等価なＣＲＰを持つといえる．次に，ＰＵＦ１とＰＵＦ３の応答を比較すると，これらは互いに論理反転関係にある．この場合においても，図示していないチャレンジを含めて全てのレスポンスが互いに論理反転関係にあるならば，一方のレスポンスを反転することで他方のレスポンスに一致させることが出来る．したがって，ＰＵＦ１とＰＵＦ３のＣＲＰは実質的に同一であり，ＰＵＦ１とＰＵＦ３は等価なＣＲＰを持つといえる．

【００２９】

ＰＵＦ１とＰＵＦ４のレスポンスを比較すると，図２中の１５ビットのレスポンスのうち一致するものは７ビットであり，一致の場所もランダムである．したがって，レスポンスには相関が見られず，明らかにＰＵＦ１とＰＵＦ４のレスポンスは等価であるとは言えない．

【００３０】

一方，ＰＵＦ１とＰＵＦ５は大部分のレスポンスが等しいが，チャレンジc9に対するレスポンスだけが異なっている．ＰＵＦがばらつきを利用してその出力を決めていることから，従来のＰＵＦにおいても，一般には，低い確率でのレスポンスの揺らぎは許容される．したがって，図示していないＣＲＰを含め，例えば二つのＰＵＦのレスポンスに対する一致性が予め決めたしきい値を上回る場合には，ＰＵＦ１とＰＵＦ５のように完全一致が得られない場合にも等価なレスポンスを返すＰＵＦとみなすことが出来る．

【００３１】

以下では，等価なＣＲＰを持つＰＵＦ回路をequivalent response PUF（ｅｒＰＵＦ）と呼び，図３Ａのように等価なＣＲＰを持つ複数のｅｒＰＵＦからなる群（グループ）をｅｒＰＵＦグループと呼ぶことがある．特に，図３Ｂのようにｅｒ ＰＵＦグループが２つのｅｒＰＵＦから構成されるとき，そのｅｒＰＵＦグループをｅｒＰＵＦ対とも呼ぶ．例えば，図２では，（ＰＵＦ１，ＰＵＦ２，ＰＵＦ３，ＰＵＦ５）が一つのｅｒＰＵＦグループを構成している．

【００３２】

（２）複数の前記ＰＵＦ回路それぞれは，共通の物理的なばらつきに基づく，互いに等価な物理的特性を保持しており，複数の前記ＰＵＦ回路それぞれのＣＲＰは，前記物理的特性に基づいて定まっているのが好ましい．物理的なばらつきは，例えば，回路の製造ばらつきである．共通の物理的なばらつきは，単一の物理的なばらつきによって構成されていてもよいし，複数の物理的なばらつきによって構成されていてもよい．物理的特性は，例えば，抵抗値である．等価な物理的特性とは，等価なＣＲＰが得られる程度に，物理的特性が共通していればよく，例えば，完全に同一の物理特性（例えば，等しい抵抗値），反転した物理特性（例えば，反転関係にある抵抗値，より具体的には高抵抗と低抵抗），実質的に同一の物理特性（例えば，ほぼ等しい抵抗値）を含む．

【００３３】

（３）複数の前記ＰＵＦ回路それぞれは，前記物理的特性を保持する不揮発性メモリを有するのが好ましい．

【００３４】

（４）前記不揮発性メモリは，メモリスタ，フラッシュメモリ及び強誘電体メモリからなる群から選択される一つのメモリであるであるのが好ましい．メモリスタは，物理特性として抵抗値を保持することができる．なお，フラッシュメモリ及び強誘電体メモリなどメモリスタ以外の他の不揮発性メモリを採用することもできる．

【００３５】

（５）複数の前記ＰＵＦ回路それぞれは，共通のチップから複数の前記ＰＵＦ回路が切断により分離されたときの切断痕を有するのが好ましい．切断痕は，分離されたチップに残る切断面そのもののほか，切断箇所において途切れた残留配線も含む．

【００３６】

（６）実施形態に係る回路群（回路グループ）の製造方法は，物理的複製困難関数回路を複数含むＰＵＦ回路群の製造方法である．製造方法は，共通の物理的なばらつきに基づく物理的特性を，複数のデバイスそれぞれに保持させることで，複数の前記デバイスを，互いに等価なＣＲＰを持つ複数のＰＵＦ回路にする設定工程を含む．

【００３７】

（７）製造方法は，前記設定工程の前に，複数の前記デバイスを一体的に備えるチップを製造する工程を更に含むことができる．前記物理的特性としては，前記チップが有する物理的なばらつきに基づく物理的特性を利用できる．

【００３８】

（８）製造方法は，前記設定工程の後に，前記チップ中の複数の前記ＰＵＦ回路を分離する工程を更に含むことができる．この工程により，分離された複数のＰＵＦ回路を得ることができる．

【００３９】

（９）前記物理的特性は，複数の前記デバイスにおける少なくとも２つのデバイスそれぞれが有する物理的なばらつき相互の関係に基づく物理的特性であってもよい（図４Ｃ参照，図については後述する）．すなわち，共通の物理的なばらつきとして，複数の物理的なばらつきを用い，それら複数の物理的なばらつき相互の関係で物理的特性を決めることができる．なお，物理的特性の決定に用いられる複数の物理的なばらつきは，全デバイスの物理的なばらつきであってもよいし，全デバイスのうちの２以上のデバイスの物理的なばらつきであってもよい．

【００４０】

（１０）前記物理的特性は，複数の前記デバイスにおける特定のデバイスの物理的なばらつきに基づく物理的特性であってもよい（図４Ｂ参照，図については後述する）．

【００４１】

（１１）前記物理的特性は，複数の前記デバイス以外のばらつき源の物理的なばらつきに基づく物理的特性であってもよい（図４Ａ参照，図については後述する）．なお，ばらつき源は，チップ内に存在するが前記デバイス以外の箇所に存在するばらつき源であってもよいし，チップ外に存在し，デバイスに接続されたばらつき源であってもよい．

【００４２】

（１２）複数の前記デバイスそれぞれは，前記物理的特性を保持する不揮発性メモリを有することができる．

【００４３】

（１３）前記不揮発性メモリは，メモリスタ，フラッシュメモリ及び強誘電体メモリからなる群から選択される一つのメモリであるのが好ましい．

【００４４】

（１４）実施形態に係る方法は，通信ネットワークにより接続された複数の拠点それぞれが，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を使用することを含む．

【００４５】

（１５）実施形態に係るネットワークシステムは，通信ネットワークにより接続された複数の拠点それぞれが，互いに等価なチャレンジレスポンスペア（Challenge Response Pair:ＣＲＰ）を持つ物理的複製困難関数（Physically Unclonable Function:ＰＵＦ）回路を有する．

【００４６】

＜３．実施形態に係るＰＵＦ回路群（ｅｒＰＵＦグループ），ｅｒＰＵＦグループの製造方法，ｅｒＰＵＦグループの使用方法，及びネットワークシステムの例＞

【００４７】

＜３．１　ｅｒＰＵＦの製造方法，値設定＞

【００４８】

ＰＵＦでは，ＣＲＰがチップ固有となるように，何らかの物理的なばらつき源を用いてレスポンスが決定される．原理的には，同一グループに属するｅｒＰＵＦが，一つのばらつきを共通に用いることでレスポンスを同一とし，異なるグループに属するＰＵＦ間では，それぞれ別のばらつきを用いるように回路を作成することで，そのレスポンスを異なるものにできる．これを考慮すれば，ｅｒＰＵＦグループは，様々な方法で作成できる．

【００４９】

図４Ａ，図４Ｂ，図４Ｃに，ｅｒＰＵＦ対を例として，ｅｒＰＵＦグループを製造するための基本的な方法を示している．実施形態においては，複数のｅｒＰＵＦ１，ｅｒＰＵＦ２が同じレスポンスを返せるように，ばらつき源４５から得られる値Ｖを参照して，ｅ

ｒＰＵＦ１，ｅｒＰＵＦ２が同じレスポンスを返せるような構成をとっている．このため，例えば，同じばらつき源４５から得られるランダムな値Ｖが共通に書き込んである不揮発性メモリ回路は，ｅｒＰＵＦとして機能する．ランダムな値Ｖは，不揮発性メモリ回路のセルに保持される．この場合には，アドレス生成器４７によって生成されたアドレスＡＤがチャレンジ，アドレスにより指定されるメモリセルが保持する値が，そのレスポンスとなる．

【００５０】

なお，図４により作成されるｅｒＰＵＦと，既存の不揮発性メモリ回路は，明らかに異なっている．ｅｒＰＵＦ１には，ばらつき源４５に由来するランダムな値があらかじめ書き込んであり，かつ，等価なＣＲＰを持つ別のｅｒＰＵＦ２が存在するためである．

【００５１】

図４Ａは，ｅｒＰＵＦの作成方法の例である．図４Ａの方法では，アドレス生成器４７から与えられるアドレス（チャレンジに相当）ＡＤを，ｅｒＰＵＦ１とｅｒＰＵＦ２が共通に用いて，一つのばらつき源４５から得られる出力値Ｖをそれぞれ共通のアドレスに記憶する．ばらつき源４５としては，例えばトランジスタの熱雑音等から乱数を発生する物理乱数を用いることが出来る．または，計算機等を用いて得られる擬似乱数を用いることも可能である．

【００５２】

図４Ｂは，ｅｒＰＵＦの別の作成方法の例である．図４Ｂの方法では，ｅｒＰＵＦ対の一方（図４Ｂではｅｒ ＰＵＦ１）に含まれるばらつき源４５から得られる値を，他方（図４Ｂではｅｒ ＰＵＦ２）にコピーすることにより，ｅｒＰＵＦ対を作成する．もちろん，この役割を適宜交換すること，すなわち，アドレス空間の前半部分の値をｅｒＰＵＦ１のばらつき源４５を使って定めてｅｒＰＵＦ２へコピーし，アドレス空間の後半の値をｅｒＰＵＦ２のばらつき源を使って定めてｅｒＰＵＦ１へコピーするなど，双方向にデータをやり取りするような構成も可能である．

【００５３】

図４Ｃは，ｅｒＰＵＦ対それぞれに含まれるばらつき源４５，４６の相互の関係から，ｅｒＰＵＦ対の値を決める方法の例である．図４Ｃの方法による構成を「相互型ｅｒＰＵＦ」と呼ぶことにする．相互型ｅｒＰＵＦについては，後ほど，具体的な回路構成例を用いて詳細に説明する．

【００５４】

図４Ａ，図４Ｂ，図４Ｃに示す方法は，３以上のｅｒＰＵＦへ拡張することも容易である．なお，アドレス生成器４７は，全てのアドレスを順次生成できれば良いことから，簡単なカウンタ等で構成できる．また，図４Ｂ，図４Ｃでは，ｅｒＰＵＦ１が図示しないアドレス生成器を持ち，アドレス信号ＡＤをｅｒＰＵＦ２に渡す前提で描かれているが，アドレスは，図４Ａに示すように，ｅｒＰＵＦ１の外部から与えてもよい．また，ｅｒＰＵＦ１，ｅｒＰＵＦ２の両方がアドレス生成器を持つように構成することも可能である．この場合，信号ＡＤは両者を同期させるためのリセット信号やクロック信号として用いることとなる．

【００５５】

図４Ａ，図４Ｂ，図４Ｃに示した作成方法によれば，ｅｒＰＵＦを極めて容易に作成できる．一方で，値設定の際のセキュリティが必ずしも完全でない場合がある．ｅｒＰＵＦ１とｅｒＰＵＦ２に書き込まれる値は，製造時にＡＤやＶ等の信号を直接観測できる者，典型的にはｅｒＰＵＦ対の作成を担当する人間等が観測し，記録出来る可能性がある．製造者が完全には信頼できないような場合には，ＡＤやＶを観測した情報が用いられてｅｒＰＵＦの実体を持たない第三者による「なりすまし」が可能となり得るため，ＡＤやＶ等の信号は，製造者からも直接の観測が困難な形，例えば，チップ内に配線した状態で値を設定することが望ましい．

【００５６】

＜３．２　相互型ｅｒＰＵＦの作成方法＞

【００５７】
図５は，「相互型ｅｒＰＵＦ対」の製造フローを示す．ここでは，ｅｒＰＵＦ対の例を用いて説明するが，この製造フローはｅｒＰＵＦグループにおいても同様である．また，この製造フローは，相互型ｅｒＰＵＦ以外のｅｒＰＵＦの製造にも適用できる．
【００５８】
ここでは，単一チップ上にｅｒＰＵＦ対を形成し，その後，それぞれのｅｒＰＵＦを切り離す場合について説明する．このような製造方法をとれば，先に述べた観測によるセキュリティ上の懸念を低減できる．ただし，単一チップ上にｅｒＰＵＦ対を形成することは必須ではない．予め分離して作成されたｅｒＰＵＦチップに同じ値を書き込む場合についても，チップ間での信号をやり取りするための接続を行う必要があることを除けば，以下に示すものと同様のフローに従いｅｒＰＵＦ対の作成が可能である．
【００５９】
まず，複数のｅｒＰＵＦが搭載されたチップ（半導体チップ）を設計しその製造を行う（図５のステップＳ１）．このチップにはグループをなす複数のｅｒＰＵＦと，ｅｒＰＵＦへの，ばらつき書き込みおよび読み出しを行うための周辺回路とが同時に搭載されるため，各ｅｒＰＵＦは互いにチップ上の配線により接続されている．なお，ばらつき書き込みを，「値書き込み」または「値設定」ということがある．また，後述のステップＳ２における値設定がされる前のｅｒＰＵＦを，単にデバイスという．
【００６０】
次に，各デバイスをｅｒＰＵＦとして機能させるため，各デバイスに値設定を行う（図５のステップＳ２）．先に述べたように，共通のエントロピー源を使用して，各ｅｒＰＵＦが等価なＣＲＰを持つようにｅｒＰＵＦへの値書き込みを行う．これにより，各デバイスそれぞれが，等価なＣＲＰを持つｅｒＰＵＦとなり，ｅｒＰＵＦグループが生成される．
【００６１】
その後，チップを切断して，各ｅｒＰＵＦを別々のチップに分離する（図５のステップＳ３）．必要に応じて，上記で設定したＣＲＰの書き換えを防ぐための書き込み回路を無効化する．書き込み回路を分離し破棄するなど，チップの切断により書き込み回路の無効化を同時に行うことができる場合には，この処理は省略できる．
【００６２】
＜３．３　ｅｒＰＵＦの回路実現例＞
【００６３】
＜３．３．１　クロスカップリング型ｅｒＰＵＦの基本回路＞
【００６４】
ここでは，不揮発性メモリであるメモリスタMR_L，MR_Rを用いて，ｅｒＰＵＦを構成する．メモリスタMR_L，MR_Rは，通過した電荷を抵抗値として記憶可能な素子であり，抵抗値をプログラム（設定）する際には，高い電圧を与え多くの電流を流す．抵抗値を読み出す際には，プログラム（設定）された抵抗値を変更しない低い電圧を用いる．以下，メモリスタに抵抗値をプログラムする高い電圧を与えることを，ストレスを与える，と呼ぶ．
【００６５】
図６Ａ，図６Ｂに示すクロスカップリング型回路を用いることで，ｅｒＰＵＦ対を実現できる．これらの回路では，左右ペアをなす回路双方に同時にストレスを与えると，一方のメモリスタMR_L，MR_Rにのみ強いストレスがかかることを利用する．強くストレスのかかったメモリスタは他方のメモリスタと比較して高抵抗となるが，左右のどちらが高抵抗，低抵抗となるかは，主としてメモリスタMR_L，MR_Rの初期ばらつきにより決まる．例えば高抵抗のメモリスタを含む場合を１，高抵抗のメモリスタを含まない低抵抗の場合を０として扱えば，これは対をなす二つのＰＵＦと考えることが出来る．ここで二つのＰＵＦの値は強い負の相関を持つことから，これをｅｒＰＵＦとして使うことができる．

【００６６】
クロスカップリング型回路は，NMOSトランジスタ，PMOSトランジスタのいずれを用いても実現可能である．NMOSを用いたクロスカップリング型回路を図６Ａに示し，PMOSを用いたクロスカップリング型回路を図６Ｂに示す．図６Ａ，図６Ｂの回路はいずれも，一つのチップ６０内に作成される．また，図６Ａ，図６Ｂは，いずれもＣＲＰの１ビット分の回路であり，実際のチップ６０内には，多ビット分の回路が存在する．
【００６７】
以下では，NMOSを用いる場合について主に説明する．NMOSを用いたクロスカップリング回路では，メモリスタMR_L，MR_RとNMOSトランジスタM_L，M_Rとを組（MR_LとM_L，およびMR_RとM_R）としてそれぞれ擬似インバータの形に接続する．擬似インバータの１対について，互いの出力であるV_R，V_Lを互いの入力（MOSトランジスタM_L，M_Rのゲート）端子に接続する．
【００６８】
図６Ａに示す回路の動作を説明する．いま，左右のメモリスタMR_L，MR_Rの初期抵抗値をそれぞれR_LとR_Rとする．$R_L > R_R$である場合の書き込み時における波形を図８Ａに示す．まず，$V_{dd} = V_{ss} = 0$Vから出発し，タイミング８１において，V_{dd}を低電圧から高電圧に上げる．$R_L > R_R$であるため$V_L < V_R$となり，図７ＡのようにM_Lはオン状態，M_Rはオフ状態となり，V_Lの電圧は変化しないが，V_Rの電圧はV_{dd}まで上昇する（図８Ａのタイミング８２）．V_Rの上昇によりMR_Rには電圧がかからないが，MR_Lにはストレスがかかり抵抗値R_Lが上昇する（図８Ａのタイミング８３）．
【００６９】
図６Ｂに示すPMOSトランジスタを用いたｅｒＰＵＦ対についても，メモリスタの抵抗値書き込み動作は同様である．$V_{dd} = V_{ss}$の初期状態から，V_{ss}の電位を下げる．$R_L > R_R$である場合の書き込み時における波形を図８Ｂに示す．タイミング８１において，V_{ss}を高電圧から低電圧に落とすと，$R_L > R_R$であるため$V_L > V_R$となり，図７ＢのようにM_Lはオン状態，M_Rはオフ状態となる．このとき，V_Lの電圧は変化しないが，V_Rの電圧はV_{ss}となる（図８Ｂのタイミング８２）．これによりMR_Rにはストレス電圧がかからないが，MR_Lにはストレスがかかり抵抗値R_Lが上昇する（図８のタイミング８３）．
【００７０】
回路が対称であるから，$R_L < R_R$の場合にはMR_Rにのみストレスがかかり抵抗値R_Rのみが上昇する．以上のストレス印加により二つのメモリスタのいずれかが高抵抗となる．この動作により，２つのメモリスタMR_R，MR_Lから，応答が互いに論理反転関係にあるメモリセルを作成できる．この処理は，図５のステップＳ２の「ＰＵＦの値設定」（のうちの１ビット分）に相当する．
【００７１】
この書き込み動作を行った後，図６中の点線で示している位置６１でチップ６０を切断し，対を切り離す．この処理は，図５におけるステップＳ３の「チップの切断」に相当する．位置６１は，切り離されたチップにおける切断面となる．また，切り離されたチップには，切断により途切れた配線（残留配線）が残る．残留配線は，例えば，M_LとV_Rとを接続していた配線の一部である．切断面及び残留配線は，切断痕の一例である．
【００７２】
切断後の基本回路構造を読み出し経路とともに図９Ａ，９Ｂに示す．それぞれのｅｒＰＵＦのレスポンスを生成する際には，書き込まれている値が破壊されないよう，V_{dd}を読み出し用の電圧とする．MOSトランジスタM_L，M_Rのゲート端子にバイアス電圧V_{input}を入力してV_{read}と参照電圧V_{ref}をコンパレータ９１で比較して０または１のレスポンスとして出力する．
【００７３】
＜３．３．２　クロスカップリング型ｅｒＰＵＦ対＞

【００７４】
図１０は，上の基本回路を用いたｅｒＰＵＦ回路（デバイス）１０６，１０７を備えるチップ（製造チップ）１１０の例を示す．ｅｒＰＵＦ１０６，１０７は，それぞれアレイ回路１０１，１０２を備えている．アレイ回路１０１，１０２は，図６Ａ，６Ｂに示す基本回路構造（切断後）をセルとして複数備える回路である．
【００７５】
製造時の値設定には，書き込み制御回路１０３と信号制御回路１０４を使用し，両アレイ回路の同位置のメモリスタ（セル）にストレスを印加し抵抗値を書き込む．製造後にはカットライン１０５でチップ１１０を切断し，第１ｅｒＰＵＦチップ１０６と，第２ｅｒＰＵＦチップ１０７と，書き込み制御回路１０３と，に分ける．書き込み制御回路１０３は不要であるため，カットライン１０５が書き込み制御回路１０３上を横切るようにすれば，切断は１回でもよい．
【００７６】
チップの切断後，ｅｒＰＵＦとして用いる場合には，Ｉ／Ｏ回路１０９から与えられる読み出しアドレス（チャレンジ）に基づき，読み出し制御回路１０８と信号制御回路１０４を用いてレスポンスを出力する．出力されたレスポンスは，読み出し制御回路１０８からＩ／Ｏ回路１０９に与えられる．なお，本例では行選択にnビット，列選択にｍビットを用いるため，チャレンジとなるアドレスはn+mビットである．そのため，アレイ回路は$N=2^n$行，$M=2^m$列で構成され，ＣＲＰはN×M個である．以下ではそれぞれの回路構造を詳しく説明する．
【００７７】
＜３．３．３　クロスカップリング型ｅｒＰＵＦ対におけるアレイ回路＞
【００７８】
図１１は，ｅｒＰＵＦ１０６，１０７が備えるアレイ回路１０１，１０２を示す．アレイ回路１０１，１０２ではV_{ri}とV_{si}を同じ行毎に，V_{xj}とV_{yj}を同じ列毎に共有する．なお，iは，1からNであり，jは，1からMである．また，書き込み制御回路１０３によって，ｅｒＰＵＦ１０１のV_xとｅｒＰＵＦ１０７のＶｙとを繋ぐ配線，ｅｒＰＵＦ１０６のV_yとｅｒＰＵＦ１０７のV_xとを繋ぐ配線がそれぞれ交差するように接続して，選択されたセルのメモリスタへ抵抗値の書き込みを可能としている．
【００７９】
図１２Ａは，NMOSトランジスタを用いる場合のi行j列目の「セル」１１１の回路構造を示す．ここで，ｅｒＰＵＦ１０６とｅｒＰＵＦ１０７の二つの回路は，回路図上は同一である．図１２Ａのセル１１１は，図６Ａの切断線６１で分割した回路にNMOSトランジスタによるスイッチM_x，M_yを備えている．ストレス印加時には，V_{ri}を高電圧V_{dd}とする．ｅｒＰＵＦ１０６とｅｒＰＵＦ１０７のアレイ回路１０１，１０２は全く同じ回路構造であるため，アレイ回路１０１，１０２中の選択セル１１１が，図６Ａと同じ回路を形成できるよう，たすきがけに接続する．すなわち，ｅｒＰＵＦ１０６のセル１１１の端子V_{xj}とｅｒＰＵＦ１０７のセル１１１の端子V_{yj}を接続し，ｅｒＰＵＦ１０６のセル１１１の端子V_{yj}とｅｒＰＵＦ１０７のセル１１１の端子V_{xj}を接続し，スイッチM_x，M_yを閉じれば，図６Ａと同様の回路が実現される．
【００８０】
図１２Ｂは，PMOSトランジスタを用いる場合のセル回路を示す．NMOSトランジスタを用いる場合と同様の回路構造であるが，スイッチM_x，M_yをPMOSトランジスタとし，ストレス印加時にはV_{ri}を負電圧とする点等が異なる．
【００８１】
＜３．３．４　クロスカップリング型ｅｒＰＵＦ対における書き込み制御回路と書き込み動作＞
【００８２】
ｅｒＰＵＦ製造時の値設定に用いる書き込み制御回路１０３と信号制御回路１０４について，アレイ回路１０１，１０２のセル１１１にNMOSトランジスタを用いる場合を例に説

明する．図１３は，書き込み制御回路１０３の例を示している．後に別チップとして切り分けられるデバイス，第１ｅｒＰＵＦ１０６と第２ｅｒＰＵＦ１０７とを同一チップ（製造チップ）上に作成している．両者１０６，１０７の他に書き込み制御回路１０３がある．

【００８３】

書き込み制御回路１０３によって生成されたV_xとV_yは，第１ｅｒＰＵＦ１０６と第２ｅｒＰＵＦ１０７のアレイ回路１０１，１０２に入力される．第１ｅｒＰＵＦ１０６のセル１１１と第２ｅｒＰＵＦ１０７のセル１１１とでクロスカップリング回路を構成するため，V_xとV_yを交差して接続する．すなわち，第１ｅｒＰＵＦ１０６のV_{xj}の端子１３４と第２ｅｒＰＵＦ１０７のV_{yj}の端子１３５を接続し，第１ｅｒＰＵＦ１０６のV_{yj}の端子１３６と第２ｅｒＰＵＦ１０７のV_{xj}の端子１３７を接続する．

【００８４】

この回路１０３では，カウンタ１３１により生成された行アドレスを用いて，１行毎にセル１１１への値設定を行う．ストレス電圧の印加時間は，タイミング制御回路１３２から出力されるVtにより制御する．V_{xj},V_{yj}には，別の行の書き込みによる電荷が残ることで本来設定されるべき値を変えてしまう可能性があることから，タイミング制御回路１３２から出力されるV_{RESET}信号により，スイッチトランジスタM_{Aj}，M_{Bj}を介して，V_{xj}，V_{yj}をリセット可能とする．

【００８５】

図１４は，信号制御回路１０４を示す．書き込み時には，信号制御回路１０４のセレクタ１４３に書き込み選択信号が与えられ，書き込み制御回路１０３から出力された書き込み行アドレスが，ワンホットエンコーダ１４１に与えられる．信号制御回路１０４は，書き込み制御回路１０３から出力された書き込み行アドレスから，アレイ回路１０１，１０２に与えられる書き込み行アドレスを，ワンホットエンコーダ１４１を用いて生成し，アレイ回路１０１，１０２のV_sとV_rに入力する．ここでは，ストレス印加を行選択後に行うため，V_rの印加を遅延回路１４２により遅延させている．遅延回路は，書き込み時には書き込み用の高い電源電圧（例えば2.5V）を，読み出し時には通常の電源電圧（例えば1.2V）を出力する．

【００８６】

図１５は，i行目の値設定（書き込み）を例に各信号の動作タイミングを示す．まず，タイミング制御回路１３２から出力されたV_{RESET}により，V_xとV_yをV_{ss}とする（図１５のタイミング１５１）．次にタイミング制御回路１３２から出力されたクロック信号CLKにより（図１５のタイミング１５２），カウンタをi-1からiにインクリメントする（図１５のタイミング１５３）．さらに，タイミング制御回路１３２は，Vtを立ち上げて行アドレスを選択する（図１５のタイミング１５４）．これによりV_{si}が立ち上がり，i行目の全セルがクロスカップリング回路となる（図１５のタイミング１５５）．次いでV_{ri}がセルのメモリスタに印加されることでi行目の全てのメモリスタにストレス電圧が印加され，メモリスタに抵抗値が書き込まれる（図１５のタイミング１５６）．

【００８７】

以上の回路構造と入力信号はアレイ回路のセルにNMOSトランジスタを用いた場合の回路と信号であるが，PMOSトランジスタを用いる場合も，信号の極性を反転させる等により同様の回路で構成できる．

【００８８】

＜３．３．５　クロスカップリング型ｅｒＰＵＦ対における読み出し制御回路と読み出し動作＞

【００８９】

図１６は，読み出し制御回路１０８の構成例を示す．V_xには，読み出し用の電圧V_{input}（例えば0.4V）を入力し，アレイ回路１０１，１０２において読み出し行アドレスによって指定された行のセルからV_yにあらわれる電圧を，コンパレータ１６３において，参照電圧V_{ref}と比較する．読み出すべき列を，読み出し列アドレスに基づき，列

選択回路１６４により選び，特定の一つのセルから得られたレスポンスを出力する．複数レスポンスを同時に用いるような応用では，列選択回路を設けず，１列分のレスポンスを一度に出力するような構成も可能である．

【００９０】

読み出し行アドレス（nビット）及び読み出し列アドレス（mビット）は，Ｉ／Ｏ回路１０９（図１０参照）から，信号制御回路１０４及び読み出し制御回路１０８へ与えられる．Ｉ／Ｏ回路１０９は，チャレンジを読み出しアドレス（n+mビット）として受け取り，読み出しアドレスの上位nビットを，読み出し行アドレスとして信号制御回路１０４へ与え，下位mビットを，読み出し列アドレスとして読み出し制御回路１０８へ与える．

【００９１】

図１４に戻り，レスポンスの読み出し時には，信号制御回路１０４のセレクタ１４３に読み出し選択信号が与えられ，Ｉ／Ｏ回路１０９から出力された読み出し行アドレスが，ワンホットエンコーダ１４１に与えられる．ワンホットエンコーダ１４１は，与えられた読み出し行アドレスから，アレイ回路１０１，１０２に与えられる読み出し行アドレスを生成し，アレイ回路１０１，１０２のV_sとV_rに入力する．

【００９２】

＜３．３．６　インバータリング型＞

【００９３】

図１７は，メモリスタを用いる別のｅｒＰＵＦの構成例を示す．メモリスタは，両端にストレス電圧を与えることで抵抗値を書き込める．そこで，0/1を対として出力する任意の0/1出力回路１７０を複数のメモリスタＭＭＲ１，ＭＭＲ２の両端に接続して電位差を与えれば，様々な回路によりｅｒＰＵＦを作成できる．

【００９４】

例えば，図１７において，両出力端nodeL，nodeRの値が，(nodeL=0，nodeR=1)または(nodeL=1,nodeR=0)となるような0/1出力回路１７０を用い，メモリスタＭＭＲ１，ＭＭＲ２にプログラム可能な電位差を与えれば，メモリスタＭＭＲ１，ＭＭＲ２に同じ抵抗値（いずれも高抵抗，またはいずれも低抵抗）を与えることができる．

【００９５】

ここでは，メモリスタＭＭＲ１，ＭＭＲ２を同方向にしているため，メモリスタＭＭＲ１，ＭＭＲ２の書き込み結果が揃うが，メモリスタＭＭＲ１，ＭＭＲ２の向きを互いに逆とすれば書き込み結果は互いに反転状態となる．

【００９６】

メモリスタＭＭＲ１，ＭＭＲ２への値書き込み後は0/1出力回路１７０は不要となるため，図１７では，チップをカットライン１７１，１７２にて切断し，２つのメモリスタＭＭＲ１，ＭＭＲ２からなるｅｒＰＵＦ対を作成している．この回路は図４Ａの例となっており，0/1出力回路１７０が，図４Ａのばらつき源４５に相当する．すなわち，図１７の回路における値書き込みは，一つのばらつき源を用いてｅｒＰＵＦ対の書き込みを行うことと等価である．図４Ｂに示すように，一方のｅｒＰＵＦ中のばらつき源をもとに0/1出力を得る構成や，図４Ｃに示すようにエントロピー源をｅｒＰＵＦ対で分散して持つ構成も可能である．

【００９７】

図１８Ａ，図１８Ｂ，図１８Ｃは，ｅｒＰＵＦセル対の具体的な回路構成例を示す．これらの回路ではいずれも，0/1出力回路１７０を，それぞれの出力端子を相手の入力端子に接続するインバータ１８１，１８２の対により実現している．これは，SRAM PUFと原理的には同じ回路であるが，これを用いて２つ（以上）からなるｅｒＰＵＦを作成する点が異なっている．

【００９８】

図１８Ａでは，CUTLINE1,CUTLINE2でチップを切断することで図１７と同様にＭＭＲ１，ＭＭＲ２によるｅｒＰＵＦ対を得ると同時に，0/1出力回路１７０を破棄できる．この回路を用いて，図４Ｂの形を構成できることは自明である．

【００９９】
また，図１８Ａの回路を変形すると，図１８Ｂのような回路構成が可能である．CUTLINE3で切断することで，ばらつき源となるインバータ１８１，１８２をチップ毎に分散してもたせてｅｒＰＵＦ対を得ることができ，図４Ｃの形を構成できる．
【０１００】
さらに，0/1出力回路１７０は最小トランジスタサイズで設計されることが一般的であるため，十分な駆動力が得られない場合がある．例えば図１８Ｃのようにバッファ回路（ここではインバータ１８３，１８４）等を介してメモリスタをプログラムすることで，メモリスタへの値の書き込みを高速に，高電圧で行うことも可能である．
【０１０１】
このような回路形式では，３以上のｅｒＰＵＦからなるｅｒＰＵＦグループの構成は容易である．図１９のように0/1出力回路１７０の出力を任意個のメモリスタＭＭＲ１，ＭＭＲ２，ＭＭＲｎに（バッファを介して）接続することによりｅｒＰＵＦグループを容易にプログラムできる．さらに，値が書き込まれるのはメモリスタである必要はなく，図２０のように0/1出力回路１７０の出力を任意個のメモリ２０１，２０２，２０３に書き込むことでもｅｒＰＵＦグループを生成可能である．メモリ２０１，２０２，２０３は，フラッシュメモリや強誘電体メモリ等の不揮発性メモリであるのが好ましい．
【０１０２】
＜３．３．７　ＮＢＴＩ型＞
【０１０３】
本発明のさらに別の実現形態として，標準的なCMOSプロセス技術のみを用いてｅｒＰＵＦを実現する方法がある．SRAMメモリセルにストレス電圧を与えることでNBTI（負バイアス電圧温度不安定性: Negative Bias Temperature Instability）現象を生じさせ，これによりメモリセルを構成するトランジスタの特性の一つである駆動力を変え，メモリセルの安定性を向上させる特性ばらつきの自己修復が提案されている(N. E. Alias, A. Kumar, T. Saraya, S. Miyano, and T. Hiramoto, “NBTI Reliability of PFETs under Post-Fabrication Self-Improvement Scheme for SRAM,” IEICE Transactions on Electronics, vol. E96.C, no. 5, pp. 620-623, 2013.：以下，「参考文献」という)．このNBTI現象を応用することでも，ｅｒＰＵＦが実現できる．
【０１０４】
まず，準備としてNBTI現象を利用したSRAMメモリセルの自己修復について説明する．図２１ＡにSRAMメモリセルの原理的な回路図を示す．説明を単純化するため，アクセストランジスタは省略している．SRAMメモリセルを構成するインバータの入出力特性の概形は図２１Ｂのような形である．いま，入出力特性の傾きが最大となる位置を論理しきい電圧V_{lt}と呼ぶものとする．SRAMメモリセルは，インバータが二つ（INV1とINV2）組み合わされた形となっている．図２１Ｃに，図２１Aに示す回路の論理しきい電圧V_{lt1}とV_{lt2}の例を示す．図２１Ｃはバタフライカーブと呼ばれ，二つのインバータの入出力特性により囲われる領域が大きいほどメモリセルが安定であることを意味する．
【０１０５】
いま電源電圧Vddを0Vから上げていくと，INV1とINV2それぞれの論理しきい電圧V_{lt1}とV_{lt2}について，より高い論理しきい電圧を持つインバータの出力ノードが論理１，他方が論理０となる．この例では，node1が論理０，node2が論理１となる．参考文献は，電源電圧をさらに上げると，オンとなっているトランジスタMP_1に選択的にNBTI現象が生じることを利用した自己修復を提案している．NBTI現象を起こす電源電圧を繰返し与えることで，MP_1のしきい値が上がり電流が減少する．その結果，INV2の論理しきい電圧V_{lt2}が低下する．これを繰り返すと，最終的にはV_{lt2}をV_{lt1}にほぼ一致させることができる．
【０１０６】
次に，NBTIを用いてｅｒＰＵＦを構成する方法を説明する．図２２が１ビット分のレスポンスを出力する回路の一例である．

【０１０７】
チップの製造後の書き込みは次のように行う．まず，スイッチφ１をすべて閉じ，スイッチφ２はすべて開ける．これにより，インバータINV1とインバータINV4がSRAMメモリセルと同様の形で接続される．また，インバータINV2とインバータINV3がSRAMメモリセルと同様の形で接続される．先に述べたように，INV1-INV4とINV2-INV3とからなる二つのインバータペアについてNBTIストレスを与える．すると，INV1とINV4を構成するPMOSトランジスタとNMOSトランジスタの論理しきい電圧がほぼ等しい値V14をとるようになる．また，INV2とINV3を構成するPMOSトランジスタとNMOSトランジスタの論理しきい値がほぼ等しい値V23をとる．ただし，V14とV23は互いに無相関であり，インバータのペア毎にばらついている．論理しきい値の操作を行なった後，CUTLINEでチップの切り離しを行う．

【０１０８】
切り離し後にはφ１のスイッチは事実上開いており，φ２のスイッチを閉じることにより，INV1-INV2からなるSRAMメモリセルと，INV3-INV4からなるSRAMメモリセルがそれぞれのチップ上にできる．この二つのSRAMメモリセルは，SRAM PUFの基本セルと同じ形となっている．ただし，これらの二つのSRAMメモリセルは，先に行なった電源電圧操作によるNBTIストレス印加により，INV1とINV4,INV2とINV3の論理しきい値がそれぞれほぼ等しくなっている．一方で，V14とV23は，チップ製造時のばらつきによりランダムに決定されている．ゆえに，V14がV23よりも高ければ，node1Lとnode2Rが論理1，node1Rとnode2Lが論理0となる．逆にV14がV23よりも低ければ，node1Lとnode2Rが論理0，node1Rとnode2Lが論理1となる．クロスカップル型と同様にアレイ構成として適切に周辺回路を設計すれば，二つのチップの対応するセルに同じ情報を記録できていることになるため，ｅｒＰＵＦとして使用できる．

【０１０９】
＜３．４　実施形態に係るＰＵＦの使用方法例及びＰＵＦを利用したネットワークシステム例＞

【０１１０】
＜３．４．１　チップ認証＞

【０１１１】
チップ認証とは，製造されたチップが正規品であるかを判定する真贋判定のことであり，安全性が要求される応用では必須の手続きとなる．従来のＰＵＦでは，チップ認証を行うために十分な数のCRPデータを読み出してデータベースを作成，保持する必要があった．しかし，ｅｒＰＵＦを用いることにより，このようなデータベースを使用することなくチップ認証が行える．

【０１１２】
ｅｒＰＵＦ対を用いたチップ認証方式では，チップ製造者はｅｒＰＵＦ対（第１ｅｒＰＵＦ,第２ｅｒＰＵＦ）を作成し，片方（第１ｅｒＰＵＦ，またはそれを組み込んだ機器）をチップ購入者に販売し，他方（第２ｅｒＰＵＦ）を製造者が所持しサーバとなる．チップ製造者の拠点とチップ購入者の拠点とが通信ネットワークを介して接続されたネットワークシステムが構築される．チップ購入者がチップの認証を行う際にはまず，ネットワークを介して，製造者に認証の要求を行う．それに応じて製造者はチャレンジCを生成し，ネットワークを介して，チップ購入者に送信する．チップ購入者は，チャレンジCから，第１ｅｒＰＵＦ（またはそれを組み込んだ機器）のレスポンスR1を得て製造者に，ネットワークを介して送信する．製造者は第２ｅｒＰＵＦのレスポンスR2を求める．製造者は，R1とR2を比較し，これらが等価であると判断できれば正規品と判定できる．これは，ｋチップ（kは２以上の整数）からなるｅｒＰＵＦグループを用いて，製造者と(k-1)個のチップとの間で認証を行う拡張は，自明に可能である．

【０１１３】
＜３．４．２　セキュア通信＞

【０１１４】
従来は通信者間で秘密鍵の交換をする必要があった通信はすべて，ｅｒＰＵＦを応用し

た安全な通信に置き換えることが出来る．
【０１１５】
ｅｒＰＵＦ群を利用してｋ者間でセキュアな通信を行うネットワークシステムの例を図２３に示す．通信ネットワーク（通信路）にて接続された複数の拠点（端末）Ａ１～Ａｋの間でセキュア通信を行いたい場合には，事前に物理的な流通方法により同じｅｒＰＵＦグループに属するｅｒＰＵＦの物理的な実体をそれぞれが持つ．図に示すとおり，端末Ａ１～Ａｋは，同じグループのｅｒＰＵＦを用いてレスポンスを得られるようになっていれば，必ずしも同一の構成でなくても良い．
【０１１６】
例えば，端末Ａ１と端末Ａ２の二者間でセキュアな通信を行う場合には，まず端末Ａ１が乱数生成器などを用いてチャレンジＣを生成して，通信経路を介してそれを端末Ａ２に渡す．それぞれが持つｅｒＰＵＦにチャレンジＣを与えてレスポンスＲを生成すれば，Ａ１とＡ２は実質的に秘密鍵Ｒを共有していることとなるから，以降の通信ではレスポンスＲを何らかの形で用いた共通鍵暗号方式等による通信が可能となる．三者間以上であっても同様に，秘密鍵をやりとりすることなく秘密鍵を共有できることは明らかである．
【０１１７】
＜３．４．１　その他＞
【０１１８】
さらに同様に，ディジタル署名が暗号化・復号化とほぼ同様の手続きであることから，ｅｒＰＵＦを用いた安全な秘密鍵の共有を利用すれば，ｋ者間のディジタル署名も実現可能であることは明らかである．また，ｅｒＰＵＦのレスポンスを擬似乱数の初期値に用いれば，ｅｒＰＵＦを持つ者の間でだけ共通であることを保証する，擬似乱数の系列を得ることが可能になる．
【０１１９】
＜４．付記＞
【０１２０】
本発明は，上記実施形態に限定されるものではなく，様々な変形が可能である．
【符号の説明】
【０１２１】
１　：ＩＣチップ
２　：入力回路
３　：ＰＵＦ回路
４　：出力回路
５　：マイコン回路
６　：チップ
２１　：認証制御回路
２２　：主要回路
４５　：ばらつき源
４６　：ばらつき源
４７　：アドレス生成器
６０　：チップ
６１　：切断線
９１　：コンパレータ
１０１　：アレイ回路
１０２　：アレイ回路
１０３　：書き込み制御回路
１０４　：信号制御回路
１０５　：カットライン
１０６　：第１ｅｒＰＵＦ
１０７　：第２ｅｒＰＵＦ

１０８　：読み出し制御回路
１０９　：Ｉ／Ｏ回路
１１０　：チップ
１１１　：セル
１３１　：カウンタ
１３２　：タイミング制御回路
１３４　：端子
１３５　：端子
１３６　：端子
１３７　：端子
１４１　：ワンホットエンコーダ
１４２　：遅延回路
１４３　：セレクタ
１６３　：コンパレータ
１６４　：列選択回路
１７０　：0/1出力回路
１７１　：カットライン
１７２　：カットライン
１８１　：インバータ
１８２　：インバータ
１８３　：インバータ
１８４　：インバータ
２０１　：メモリ
２０２　：メモリ
２０３　：メモリ

【図１】

図1A

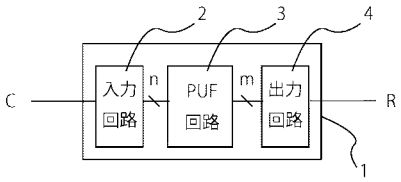


図1B

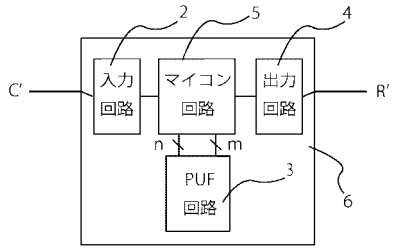
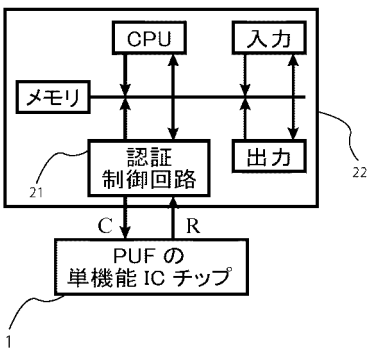


図1C



【図２】

図2

challenge	response				
	PUF1	PUF2	PUF3	PUF4	PUF5
c0	0	0	1	0	0
c1	1	1	0	1	1
c2	1	1	0	0	1
c3	0	0	1	1	0
c4	1	1	0	0	1
c5	0	0	1	0	0
c6	0	0	1	0	0
c7	0	0	1	1	0
c8	1	1	0	0	1
c9	1	1	0	1	0
c10	1	1	0	0	1
c11	0	0	1	1	0
c12	1	1	0	1	1
c13	0	0	1	0	0
c14	0	0	1	1	0
⋮	⋮	⋮	⋮	⋮	⋮

【図３】

図3A

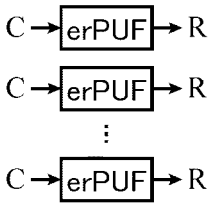
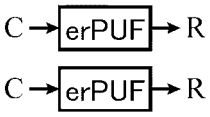


図3B



【図４】

図4A

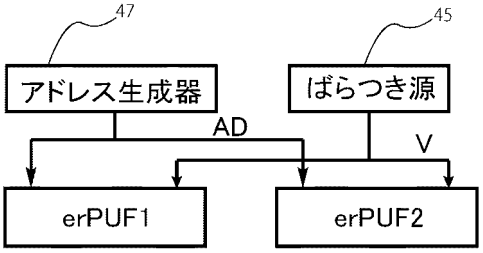


図4B

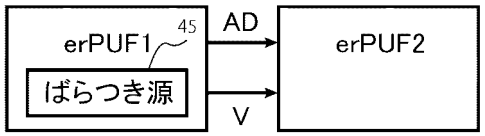
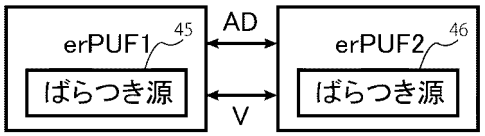
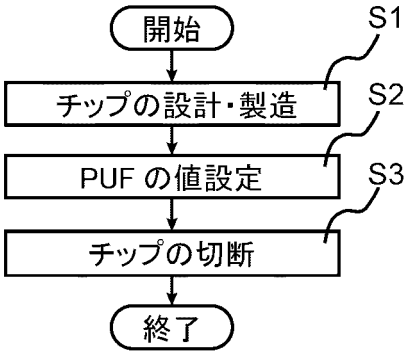


図4C



【図５】

図5



【図６】

図6A

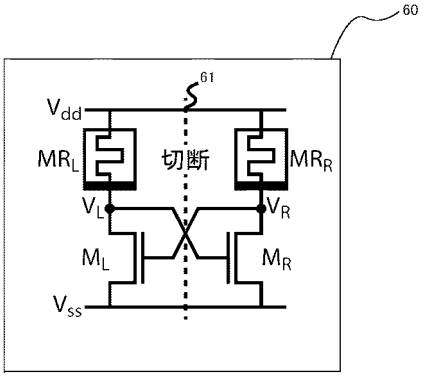
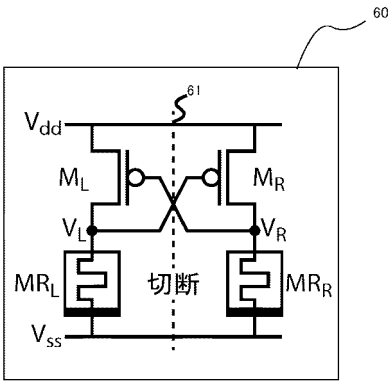


図6B



【図７】

図7A

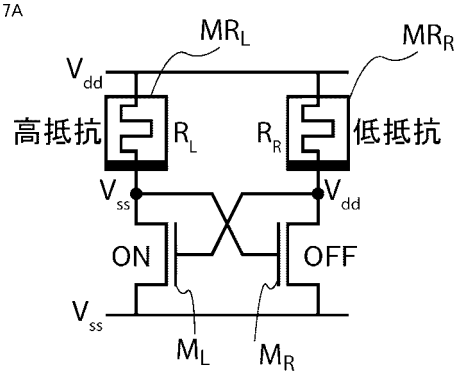
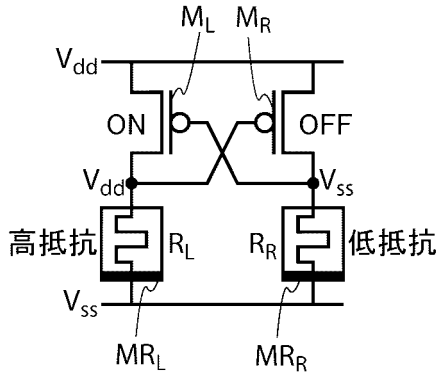


図7B



【図８】

図8A

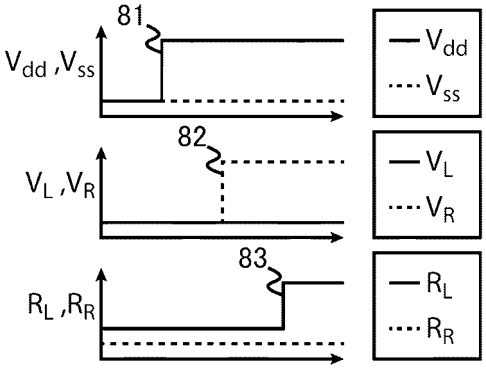
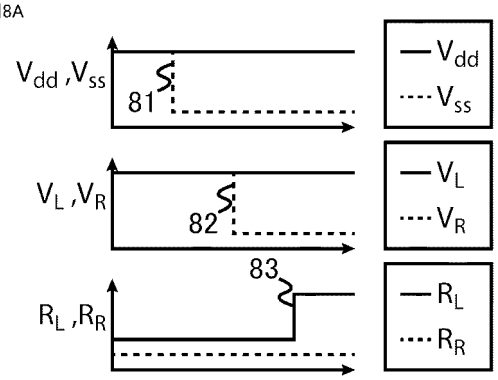


図8A



【図９】

図9A

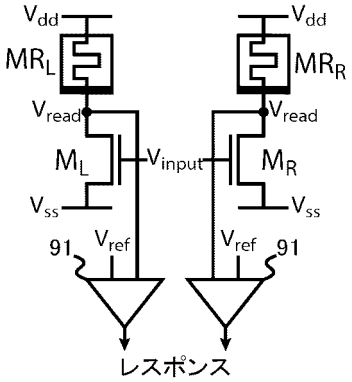
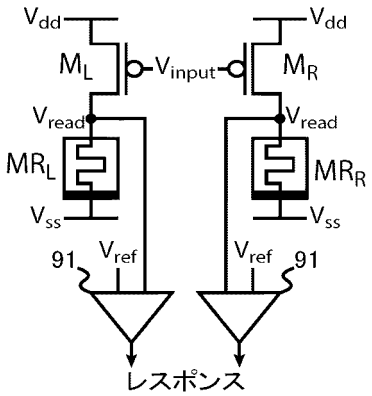
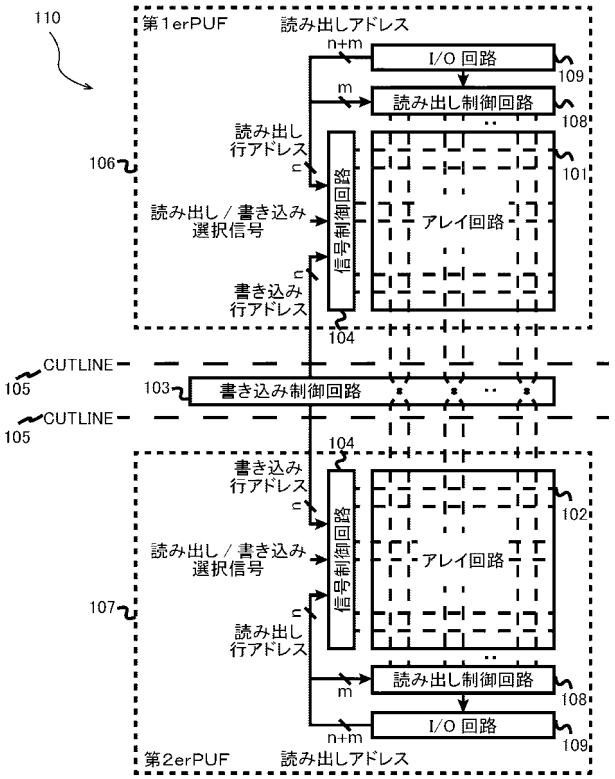


図9B



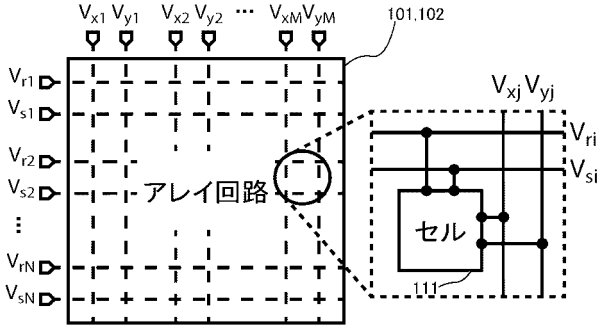
【図１０】

図10



【図１１】

図11



【図１２】

図12A

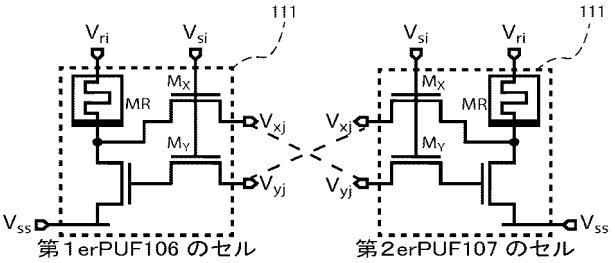
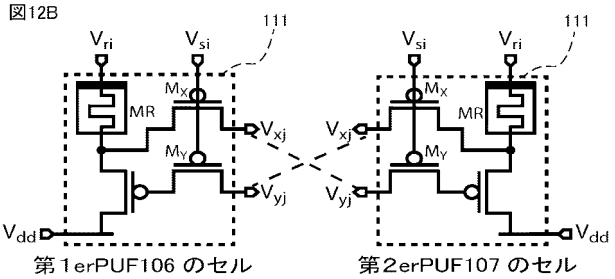
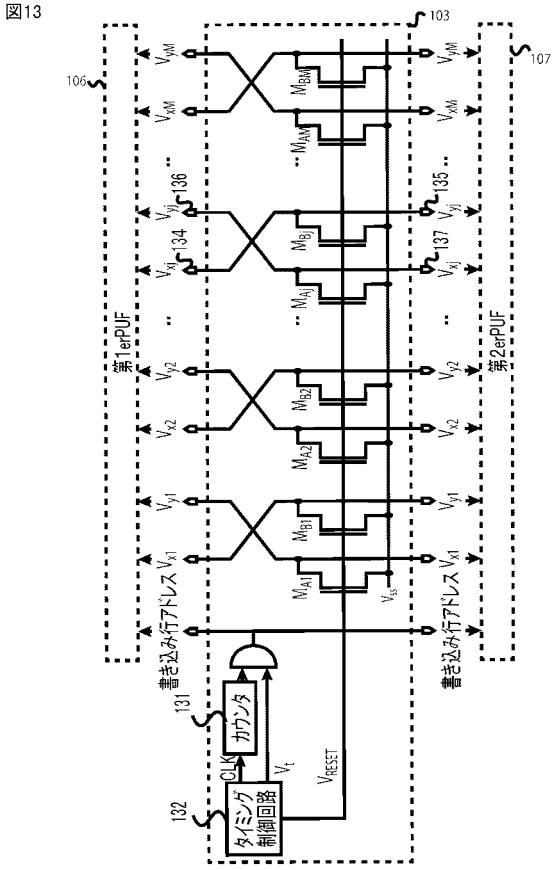


図12B



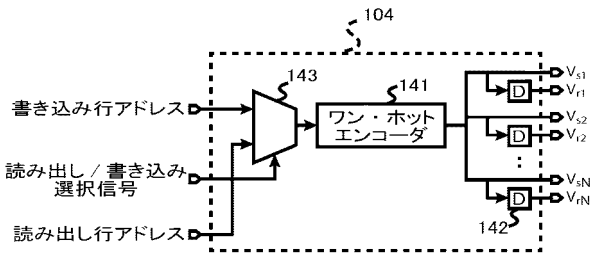
【図１３】

図13



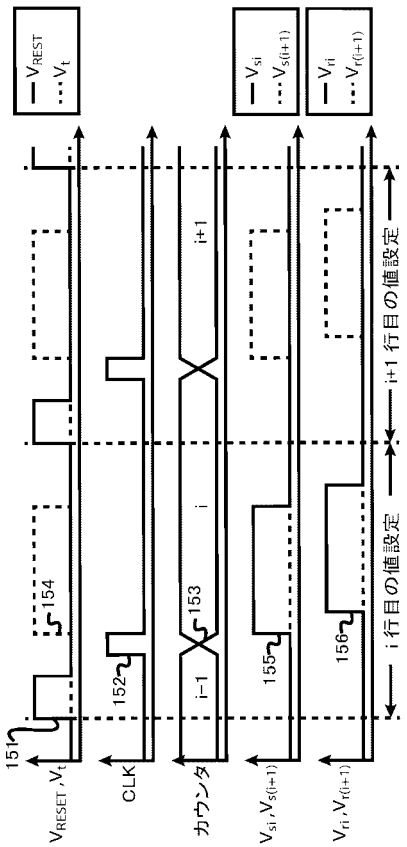
【図１４】

図14



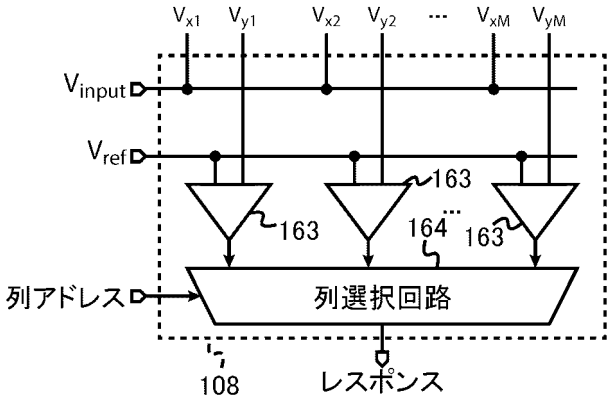
【図１５】

図15



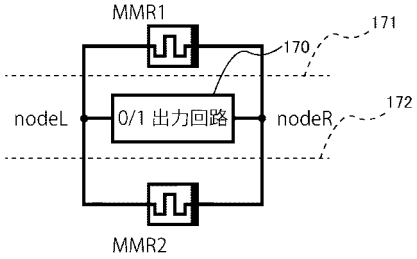
【図１６】

図16



【図１７】

図17



【図１８】

図18A

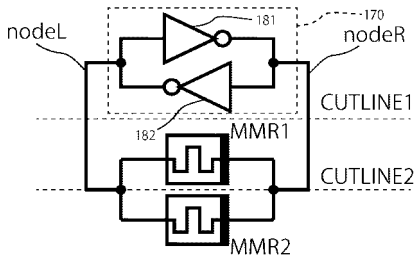


図18B

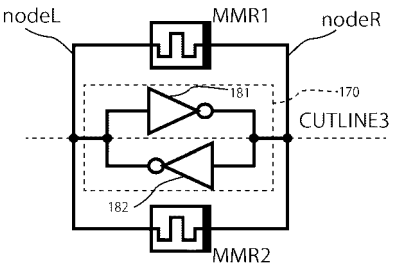
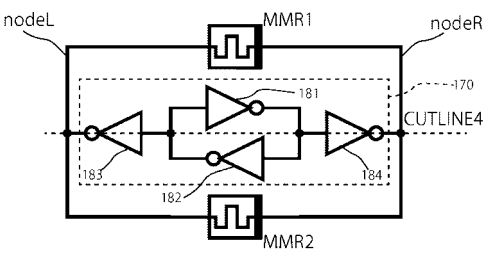
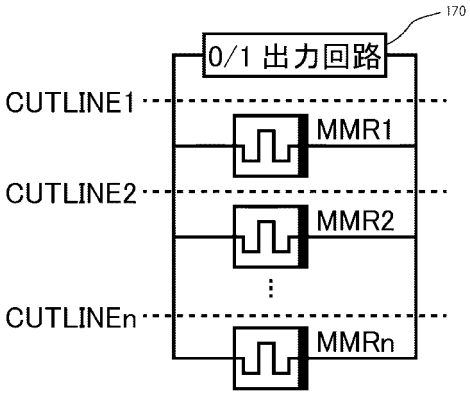


図18C



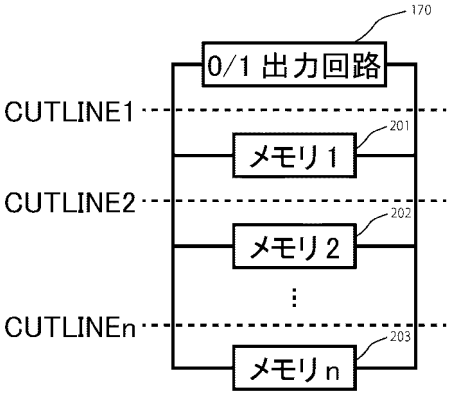
【図１９】

図19



【図２０】

図20



【図２１】

図21A

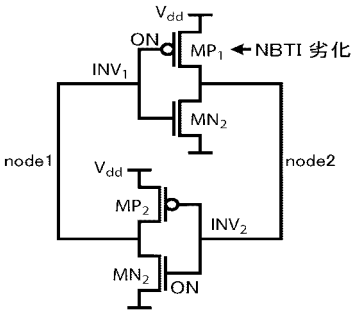


図21B

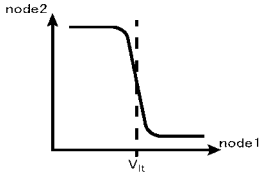
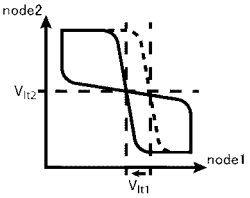
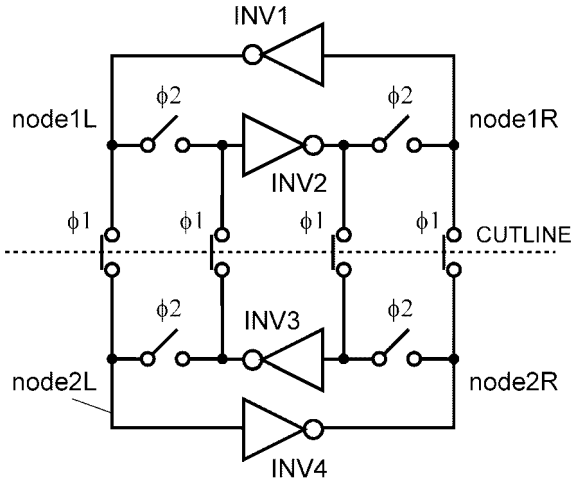


図21C



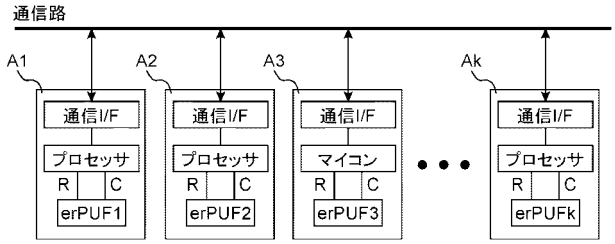
【図２２】

図22



【図２３】

図23


通信路
A1
A2
A3
Ak
通信I/F
プロセッサ
R
C
erPUF1
通信I/F
プロセッサ
R
C
erPUF2
通信I/F
マイコン
R
C
erPUF3
通信I/F
プロセッサ
R
C
erPUFk

フロントページの続き

(51)Int.Cl.			F I			テーマコード（参考）
Ｈ０１Ｌ	***27/10***	***(2006.01)***	Ｈ０１Ｌ	27/10	４３１	
Ｈ０１Ｌ	***21/8229***	***(2006.01)***	Ｈ０１Ｌ	27/102	３９１	
Ｈ０１Ｌ	***27/102***	***(2006.01)***				

(72)発明者　廣本　正之
京都府京都市左京区吉田本町３６番地１　国立大学法人京都大学内

Ｆターム(参考) 5F083 BS50 CR15 ER22 FR00 GA27 GA30 LA02 LA04 LA07 LA10
ZA13
5J104 AA07 AA16 EA08 KA02 KA06 KA14 NA38