(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-503328
(P2018-503328A)
(43)公表日　平成30年2月1日(2018.2.1)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/10	(2006.01)	H04L	9/00	621Z	5J104
G06F 21/73	(2013.01)	G06F	21/73		

審査請求 未請求　予備審査請求 未請求　（全 27 頁）

(21)出願番号	特願2017-550470 (P2017-550470)
(86)(22)出願日	平成27年12月15日 (2015.12.15)
(85)翻訳文提出日	平成29年8月14日 (2017.8.14)
(86)国際出願番号	PCT/US2015/065909
(87)国際公開番号	WO2016/100402
(87)国際公開日	平成28年6月23日 (2016.6.23)
(31)優先権主張番号	62/091,985
(32)優先日	平成26年12月15日 (2014.12.15)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	62/199,685
(32)優先日	平成27年7月31日 (2015.7.31)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	62/204,835
(32)優先日	平成27年8月13日 (2015.8.13)
(33)優先権主張国	米国 (US)

(71)出願人　503128320
エスティーシー.　ユーエヌエム
ＳＴＣ．ＵＮＭ
アメリカ合衆国　ニューメキシコ州　８７１０２，　アルバカーキ，　スイート　１１００，　１０１　ブロードウェイ　ブールバード　ノースイースト，　ロボ　レインフォレスト　ビルディング
Ｌｏｂｏ　Ｒａｉｎｆｏｒｅｓｔ　Ｂｕｉｌｄｉｎｇ，　１０１　Ｂｒｏａｄｗａｙ　Ｂｌｖｄ．　ＮＥ，　Ｓｕｉｔｅ　１１００，　Ａｌｂｕｑｕｅｒｑｕｅ，　ＮＭ　８７１０２　ＵＳＡ
(74)代理人　100140109
弁理士　小野　新次郎

最終頁に続く

(54)【発明の名称】信頼性を高めた物理的クローン不能関数ビットストリーム生成方法

(57)【要約】
ハードウェア埋め込み遅延物理的クローン不能関数（「ＨＥＬＰ　ＰＵＦ」）は、パス安定性を監視し、コア・ロジック・マクロからパス遅延を測定することによって、エントロピを利用する。ＨＥＬＰ　ＰＵＦのための信頼性およびセキュリティ向上技法は、環境変動を受けるビットストリングの再生中にビット反転エラーを低減し、暗号強度を高め、対応してモデル構築攻撃の実行を困難にする。電圧ベースの登録プロセスは、正常に合成された（グリッチがある）機能ユニット上で不安定なパスを選別し、オンチップ電圧レギュレータを使用して制御される複数の供給電圧において登録を実行することによって、ビット反転エラーを低減する。
【選択図】図１

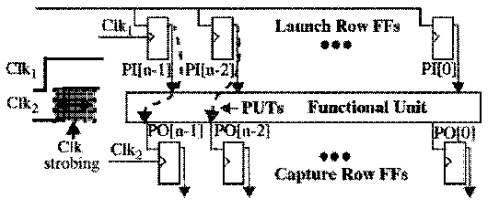

FIG. 1

【特許請求の範囲】
【請求項１】
物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法であって、
複数のインタバルの各ローンチ－キャプチャ・インタバルのパス遅延値を測定するステップと、
２つのランダムに選択したパス遅延値間の差分値を計算するステップと、
前記差分値が正であるとき前記差分値を「０」ビットとして定め、前記差分値が負であるとき、「１」ビットとして定めるステップと、
前記定めるステップに基づいて、１群のビットストリングを生成するステップであって、各ビットストリングが２つ以上の供給電圧レギュレータにおいて生成される、ステップと、
前記２つ以上の供給電圧レギュレータにおいて生成された各ビットストリングの１つ以上のビット位置において不一致を確認することによって、前記１群のビットストリングを排除するステップと、
を含む、方法。
【請求項２】
請求項１記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法において、前記定めるステップが、更に、
温度－電圧条件に基づいて閾値を導くステップと、
前記差分値が前記閾値よりも大きいとき、前記差分値を「無効」として定めるステップと、
を含む、方法。
【請求項３】
請求項１記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法であって、更に、
ジャンプ・マージン・パラメータを定めるステップと、
前記パス遅延値または前記差分値のいずれかが前記ジャンプ・マージン・パラメータよりも小さいとき、前記パス遅延値および前記差分値を無視するステップと、
を含む、方法。
【請求項４】
請求項１記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法において、各供給電圧レギュレータが、０．９５Ｖ、１．００Ｖ、１．０５Ｖの電圧で動作する、方法。
【請求項５】
請求項１記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法であって、更に、温度および電圧の変動を補償するために、１組の差分値から平均および範囲を計算するステップを含む、方法。
【請求項６】
請求項１記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法であって、更に、前記パス長バイアスを除去するために、モジュラスを前記差分値に適用するステップを含む、方法。
【請求項７】
請求項１記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法であって、更に、ビット反転を混入させる確率が最も高い差分値を特定するステップを含む、方法。
【請求項８】
請求項７記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法において、ビット反転を混入させる最も高い確率が、「０」ビットと「１」ビットとの間の境界において発生する、方法。

【請求項９】
集積回路によるビットストリング生成のための登録方法であって、
（ａ）物理的クローン不能関数について複数のローンチ－キャプチャ・インタバル・パス・タイミング値を測定するステップと、
（ｂ）前記物理的クローン不能関数の２つのパス・タイミング値をランダムに選択するステップと、
（ｃ）前記２つのパス・タイミング値間の差分値を計算するステップと、
（ｄ）前記差分値が正であるとき「０」ビットを指定し、前記差分値が負であるとき「１」ビットを指定するステップと、
（ｅ）２つ以上のビットストリングを得るために、２つ以上の供給電圧レギュレータにおいてステップ（ａ）～（ｄ）を実行するステップと、
（ｆ）前記２つ以上のビットストリングにおいて不一致を確認するステップと、
（ｇ）ビット反転の数を減らすために、前記不一致のビットストリングを除去するステップと、
を含む、方法。
【請求項１０】
請求項９記載の集積回路によるビットストリング生成のための登録方法において、前記指定するステップが、更に、
温度－電圧条件に基づいて閾値を導くステップと、
前記差分値が前記閾値よりも大きいとき、前記差分値を「無効」として定めるステップと、
を含む、方法。
【請求項１１】
請求項９記載の集積回路によるビットストリング生成のための登録方法であって、更に、
ジャンプ・マージン・パラメータを定めるステップと、
前記パス・タイミング値または前記差分値のいずれかが前記ジャンプ・マージン・パラメータよりも小さいとき、あらゆるパス・タイミング値および差分値を無視するステップと、
を含む、方法。
【請求項１２】
請求項９記載の集積回路によるビットストリング生成のための登録方法において、各供給電圧レギュレータが、０．９５Ｖ、１．００Ｖ、１．０５Ｖの電圧で動作する、方法。
【請求項１３】
請求項９記載の集積回路によるビットストリング生成のための登録方法であって、更に、チップ間ハミング距離を計算するステップを含む、方法。
【請求項１４】
請求項１３記載の集積回路によるビットストリング生成のための登録方法において、前記計算するステップが、更に、２つの集積回路によって生成されたビットストリングにおいて異なるビットの数を数えるステップを含む、方法。
【請求項１５】
請求項９記載の集積回路によるビットストリング生成のための登録方法であって、更に、チップ内ハミング距離を計算するステップを含む、方法。
【請求項１６】
請求項１５記載の集積回路によるビットストリング生成のための登録方法において、前記計算するステップが、更に、２つのＴＶコーナーにおいて生成された前記ビットストリングにおいて異なるビットの数を数えるステップを含み、各ＴＶコーナーが異なる集積回路からである、方法。
【請求項１７】
請求項９記載の集積回路によるビットストリング生成のための登録方法であって、更に

、温度および電圧の変動を補償するために、１組の差分値から平均および範囲を計算するステップを含む、方法。
【請求項１８】
請求項９記載の集積回路によるビットストリング生成のための登録方法であって、更に、前記パス長バイアスを除去するために前記差分値にモジュラスを適用するステップを含む、方法。
【請求項１９】
請求項９記載の集積回路によるビットストリング生成のための登録方法であって、更に、ビット反転を混入させる確率が最も高い差分値を特定するステップを含む、方法。
【請求項２０】
請求項１９記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法において、ビット反転を混入させる最も高い確率が、「０」ビットと「１」ビットとの間の境界において発生する、方法。
【請求項２１】
請求項１記載の物理的クローン不可関数ビットストリング生成中にビット反転の数を低減する信頼性向上方法において、前記方法が、機能ユニットのグリッチのない実装を使用する、方法。
【請求項２２】
請求項９記載の集積回路によるビットストリング生成のための登録方法において、前記方法が、機能ユニットのグリッチのない実装を使用する、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、２０１４年１２月１５日に出願された米国仮特許出願第６２／０９１，９８５号、２０１５年７月３１日に出願された米国仮特許出願第６２／１９９，６８５号、および２０１５年８月１３日に出願された米国仮特許出願第６２／２０４，８３５号の権利を主張する。これらの特許出願の各々をここで引用したことにより、その内容全体が本願にも含まれるものとする。
【０００２】
政府支援
本発明は、アメリカ国立科学財団（ＮＳＦ：National Science Foundation）によって授与された助成金ＣＮＳ－１０１８７４８を受けて、政府支援によって行われた。政府は、本発明において一定の権利を保有する。
【０００３】
発明の分野
本発明は、一般には、ハードウェア・コンポーネントにおいて使用される電気回路の保護に関し、更に特定すれば、物理的クローン不能関数（「ＰＵＦ」）のための電圧ベースの登録(voltage-based enrollment)に関する。
【従来技術】
【０００４】
チップまたはマイクロチップとしても知られている集積回路（「ＩＣ」）は、コンピュータ、電話機、ディジタル・アプリケーションのような電子機器において使用される微小化電子回路である。ＩＣは、通例、シリコンおよびゲルマニウムのような半導体デバイス、ならびにキャパシタ、抵抗器、およびダイオードのような受動コンポーネントで形成される。通常、ＩＣは、半導体材料の薄い基板上に製造される。近年では、トランジスタ当たりのＩＣ製造コストが減少している。しかしながら、価格低下は製造の実現可能性(availability)を高めるが、クローンまたはコピーのような脅威、ならびに横領および不正使用からＩＣを保護しなければならない。脅威は、暗号化されたデータへの不正アクセス、知的所有権（「ＩＰ」）の不正使用を含むＩＣ設計の複製、およびＩＣのハードウェア盗用または違法な製造を許してしまうおそれがある。セキュリティ・キーのクローン、横領

、および不正使用は、特に、認証プロトコルにおいてセキュリティ・キーを使用するコンピュータ・アプリケーションにおいて問題となる。

【０００５】

クローンおよび不正使用からＩＣを保護するために、多くのコンピュータ・ベースのハードウェア・セキュリティ方式が存在する。これらのセキュリティ方式は、各ＩＣから導き出される一意のクローン不能識別子(unique unclonable identifier)のような、セキュリティ・キーまたは署名へのアクセス可能性に左右される。セキュリティ・キーは、データ通信チャネルの暗号化を実行するメカニズムのような上位レベルのハードウェア・セキュリティにおいて実装されるコンピュータ・ベースのハードウェア・セキュリティ・メカニズムの基礎を定め、またはフィールド・プログラマブル・ゲート・アレイ（「ＦＰＧＡ」）を含むコンピュータ・ベースのロジック・デバイスにおいてＩＰ盗用保護(theft protection)に備える。

【０００６】

従来のセキュリティ・キーは、例えば、ＩＣ上のフラッシュ・メモリまたはリード・オンリ・メモリ（「ＲＯＭ」）に格納されているディジタル・データを使用して定められる。セキュリティの観点からは、セキュリティ・キーへのアクセスは、ＩＣ上に形成されたハードアウェア回路に制限されることが望ましい。生憎、これら従来の技術を使用して格納されたセキュリティ・キーは、侵略的な物理攻撃を受け、敵が秘密鍵を学習することを可能にするおそれがある。秘密鍵が敵によって学習されると、クローンＩＣが作成されるおそれがあり、更にセキュリティ・プロトコルが危険にさらされるおそれがある。

【０００７】

ランダム・ビットストリングが、ハードウェア・セキュリティにおける暗号化、識別、認証、および機能有効化の基礎を形成することができる。現在の技術では、暗号化のための鍵にする素材(keying material)が、ＦＰＧＡおよび特定用途集積回路（「ＡＳＩＣ」）上の不揮発性メモリ内にディジタル・ビットストリングとして格納されることがある。しかしながら、このように格納された秘密は、秘密を盗むために探索攻撃を使用する可能性がある、決意を持った敵に対しては安全ではない場合もある。

【０００８】

ディジタル・ビットストリングを不揮発性メモリに格納することの代案として、物理的クローン不能関数（「ＰＵＦ」）を使用することができる。ＰＵＦとは、製造のばらつきによって導入されるエントロピを利用してビットストリングを生成するＩＣハードウェア・プリミティブのことであり、対応するばらつきを測定しディジタル化するためのオンチップ・インフラストラクチャを内蔵することができる。ＰＵＦは、パス遅延(path delay)、漏れ電流、またはＳＲＡＭ起動パターンにおいて生ずる自然なばらつきを測定およびディジタル化して、ランダム・ビットストリングを生成することができる。

【０００９】

ＰＵＦの実装を使用してＩＣを保護するための種々の技法が提案されている。チャレンジ・ベース(challenge-based)ＩＣ認証が、その一例である。チャレンジ・ベースのＩＣ認証では、秘密鍵がＩＣに埋め込まれ、ＩＣがチャレンジに対して一意の応答を生成することを可能とし、この一意の回答はこのチャレンジにのみ有効である。このため、鍵は秘密のままであり、認証を実行するメカニズムはなりすましに強い(resistant)。遠隔有効化方式(remote activation scheme)は別の例である。遠隔有効化方式は、ＩＣ設計者が各ＩＣを起動時にロックし、次いで離れた場所からそれをイネーブルして、知的所有権保護およびハードウェア・メータリングに備える。状態が設計の有限状態機械（「ＦＳＭ」）に追加され、秘密鍵の関数である制御信号が追加される。したがって、ハードウェアは、特定の有効化コードを受け取るまで、鍵がかかる(lock up)。ＰＵＦ実装の他の例には、不一致遅延線(mismatched delay-lines)、スタティック・ランダム・アクセス・メモリ（「ＳＲＡＭ」）の電力投入パターン、金属酸化物半導体（「ＭＯＳ」）デバイスの不整合、および入力依存漏れパターン(input dependent leakage patterns)が含まれる。しかしながら、これらの技法の各々は、ＩＣに対するセキュリティ・キーの横領、クローン、ま

たは不正使用に関する脆弱性を有する。
【００１０】
認証は、試験側(prover)、例えば、ハードウェア・トークンまたはスマート・カードと、検証側(verifier)、セキュア・サーバまたは銀行との間のプロセスであり、一方または双方の補強証拠を使用して識別情報(identity)を確認する。電子機器、ソフトウェア、センサが埋め込まれた物理オブジェクト(physical object)のネットワーク、およびもののインターネット（「ＩｏＴ」）と呼ばれる、データの収集および交換を可能にするネットワーク接続により、ハードウェア・トークンがリソースに制約されるアプリケーションの数が増えつつあり、したがって、コスト、エネルギ、および面積のオーバーヘッドが低い新規の認証技法が求められている。
【００１１】
広い面積を占める(area-heavy)暗号プリミティブおよび不揮発性メモリ（「ＮＶＭ」）を使用する従来の認証方法は、発展しつつある埋め込みアプリケーション型には魅力的でない。しかしながら、ＰＵＦは、ハードウェア・セキュリティおよび信頼プリミティブであり、低コストに関する問題に取り組むことができる。何故なら、これらはＮＶＭの必要性を排除するからである（提案された殆どの認証プロトコルにおいて）。
【００１２】
ＰＵＦは、「強いＰＵＦ」または「弱いＰＵＦ」に分類することができる。「強いＰＵＦ」は、暗号プリミティブおよび処理の数および種類を減らすことによって、面積およびエネルギのオーバーヘッドを削減することができるが、面積のオーバーヘッドは、「弱いＰＵＦ」におけるエントロピ・ソースの物理サイズを制限する。
【００１３】
提案された殆どの「弱いＰＵＦ」アーキテクチャは、エントロピ・ソースとして役割を果たすために同じ設計の検査構造の専用アレイの挿入を必要とし、面積のオーバーヘッドはエントロピ・ソースの物理サイズを制限する。「弱いＰＵＦ」を認証に使用することができるが、これらは、その限られた量のエントロピを、秘密を機械学習するように設計された敵対するインターフェース攻撃に対して保護するために、難読化機能、例えば、暗号ハッシュ、暗号化およびＸＯＲ関数の挿入を必要とする。
【００１４】
一方、殆どの「強いＰＵＦ」は、既存のオンチップ・リソースにおいて利用可能なエントロピを利用することによって、特殊検査構造内におけるエントロピ量の制限を迂回する。「強いＰＵＦ」は、認証処理のために非常に多数のチャレンジ－応答－対（「ＣＲＰ」）を生成することができる。
【発明の概要】
【発明が解決しようとする課題】
【００１５】
以上で述べたように、ＰＵＦは、各ＩＣに一意である、ＩＣの物理および電気的プロパティにおけるばらつきからエントロピ（ランダム性）を、ディジタル秘密（ビットストリング）を生成する手段として、抽出する。ビットストリングは、認証アプリケーションのためにハードウェア・トークンを一意に識別する役割を果たすことができる。ビットストリングは、実行中に生成され、これによってこれらのディジタル・コピーをＮＶＭに格納する必要性を排除し、（理想的には）ある範囲の環境変動の下で再生可能である。秘密ビットストリングの正確な生成時間を制御する能力、および侵略的探索攻撃に対するＰＵＦエントロピ・ソースの感度（それを無効にするように作用する）は、リソース制約ハードウェア・トークンにおける認証に対してこれらを魅力的にする追加の属性である。しかしながら、ＩＣの信頼性およびセキュリティを高める要望がある。特に、クローン、偽装、横領、および不正使用を含む脅威に対するセキュリティ・キーの脆弱性を軽減する要望がある。本発明はこの要望を満足する。
【課題を解決するための手段】
【００１６】

ＩＣの信頼性およびセキュリティを高める要望、特に、クローン、偽装、横領、および不正使用を含む脅威に対するセキュリティ・キーの脆弱性を軽減するという要望に応じて、ハードウェア埋め込み遅延物理的クローン不能関数（「ＨＥＬＰ　ＰＵＦ」：Hardware-Embedded Delay Physical Unclonable Function）は、２０１４年８月２８日に出願された国際出願ＰＣＴ／ＵＳ２０１４／０５３２７６に更に詳しく記載されているように、チップのコア・ロジック・マクロにおいて発生するパス遅延ばらつきを利用して、ランダム・ビットストリングを作成する。この国際出願をここで引用したことにより、その内容全体が本願にも含まれるものとする。

【００１７】

ＨＥＬＰ　ＰＵＦは、既存の機能ユニット内における遅延ばらつきからのそのビットストリングの生成に基づく「強いＰＵＦ」であり、機能ユニットの相互接続が複雑であるために、エントロピ・ソースのサイズが著しく増大する。ＰＵＦによって生成されたビットストリングは、多数の用途に使用することができ、例えば、通信の暗号化、偽造防止技法の実現、現場における悪意のシステム変更の検出、サプライ・チェーン認証(supply chain authentication)の実行、ＩＣ上における販売業者特定機能(feature)の有効化が含まれる。

【００１８】

認証処理のためにハードウェア・トークンを用意するプロセスは、初期化または登録(enrollment)として知られている。初期化の間、セキュア・サーバはＰＵＦに与えられるチャレンジから小さな部分集合を、対応する１組の応答を生成するためにランダムに選択する。次に、この１組のＣＲＰはサーバによってセキュア・データベースに記録され、後にフィールド・トークン(fielded token)を認証するために使用される。トークン毎に格納されるＣＲＰの数を小さくすることができる。何故なら、大きなＣＰＲ空間が、選択された部分集合の秘匿性と共に、敵がトークンを偽装するためにクローンを作る(build)ことを非常に困難にするからである。

【００１９】

本発明は、ＨＥＬＰ　ＰＵＦのための信頼性およびセキュリティ向上技法を対象とする。本発明によれば、環境変動を受ける(across)ビットストリングの再生の間、ビット反転エラーが減少する。加えて、暗号強度が向上し、対応してモデル構築攻撃の実行が困難となる。

【００２０】

本発明の一実施形態によれば、信頼性およびセキュリティ向上技法は、電圧ベースの登録プロセスを対象とする。電圧ベースの登録プロセスは、正常に合成された（欠陥のある(glitchy)）機能ユニット上で不安定なパスをふるい分け(screen)、オンチップ電圧レギュレータを使用して制御される複数の供給電圧において登録を実行することによって、ビット反転エラーを減少させる。

【００２１】

本発明の他の実施形態によれば、マージン技法(margin technique)が信頼性を著しく向上させる。波動差分動的ロジック（「ＷＤＤＬ」：wave-differential dynamic logic）と呼ばれるロジック・スタイルを実装することによって、機能ユニットにおけるグリッチを排除し、信頼性およびセキュリティの、正常に合成された機能ユニットとの比較を容易にする。グリッチを排除するためのＷＤＤＬを使用して本発明について論ずるが、グリッチの排除する技法であればいずれでも可能であると考えられる(contemplate)。

【００２２】

本発明の他の実施形態は、ＷＤＤＬベースの標準セル・ライブラリの拡張バージョンを対象とする。ＷＤＤＬロジック・スタイルの使用により、グリッチのない機能ユニットの面積オーバーヘッドが減少する。機能多様性(functional diversity)と呼ばれる技法を使用することによって、ＨＥＬＰ　ＰＵＦのセキュリティを向上させ、異なる実施態様の機能ユニットを構築するために、ライブラリの異なる部分集合が使用される。

【００２３】

本発明の他の実施形態によれば、特殊なＣＡＤベースの回路分析ツールを使用して、エントロピを定量化する。これらのツールは、機能ユニットにおけるパスによって表されるエントロピの総量を定量化する手段として、グリッチのないバージョンの機能ユニットに適用される。

【００２４】

１つ以上の例の詳細について、添付図面および以下の説明において明記する。その他の特徴、目的、および利点は、説明および図面から、そして特許請求の範囲から明らかとなろう。

【００２５】

本発明の好ましい実施形態について、限定するためではなく本発明を例示するために用意された添付図面と関連付けて説明する。図面では、同様の参照番号は同様のエレメントを示す。

【図面の簡単な説明】

【００２６】

【図１】図１は、本発明の実施形態にしたがってパス遅延を測定するためのクロック・ストローブ技法(clock strobing technique)のブロック図である。

【図２】図２は、本発明の実施形態による安定したパス（ｘ軸）に関連付けられた遅延（ｙ軸）のグラフである。

【図３Ａ】図３Ａは、本発明の実施形態による登録におけるＬＣＩパス・タイミング値（「ＰＮ」）の分布グラフである。

【図３Ｂ】図３Ｂは、本発明の実施形態による、図３Ａに示したようなＰＮから選択した対の遅延差の分布グラフである。

【図４】図４は、本発明の実施形態による電圧ベースの登録（「ＶＢＥ」）技法を示すＰＮ差のセグメントを示すグラフである。

【図５】図５は、本発明の実施形態による、ジャンプ・マージンと平均ビットストリング・サイズとの間のトレードオフを示すグラフである。

【図６】図６は、本発明の実施形態による個々のチップ間ハミング距離（「ＨＤ」）のヒストグラムである。

【図７】図７は、本発明の実施形態によるＰＮ、ＰＮＤｉｆｆ、ＭｏｄＰＮＤｉｆｆを示すグラフである。

【図８】図８は、本発明の実施形態による、全体的なばらつきがある、および全体的なばらつきない温度－電圧（「ＴＶ」）補償ＰＮＤｉｆｆを示すグラフである。

【図９】図９は、本発明の実施形態によるマージン技法を示すグラフである。

【図１０Ａ】図１０Ａは、本発明の実施形態によるマージン技法を使用しない場合の標準設計に対するハミング距離（「ＨＤ」）の結果を示すグラフである。

【図１０Ｂ】図１０Ｂは、本発明の実施形態によるマージン技法を使用した場合の標準設計に対するハミング距離（「ＨＤ」）の結果を示すグラフである。

【図１１Ａ】図１１Ａは、本発明の実施形態によるマージン技法を使用しない場合のＷＤＤＬ設計に対するハミング距離（「ＨＤ」）の結果を示すグラフである。

【図１１Ｂ】図１１Ｂは、本発明の実施形態によるマージン技法を使用した場合のＷＤＤＬ設計に対するハミング距離（「ＨＤ」）の結果を示すグラフである。

【図１２】図１２は、本発明の実施形態によるカルノー図である。

【図１３】図１３は、本発明の実施形態による機能ユニットを示す。

【図１４】図１４は、本発明の実施形態による変換プロセスのフロー・チャートを示す。

【図１５】図１５は、本発明の実施形態によるエントロピ分析のフロー・チャートを示す。

【図１６】図１６は、本発明の実施形態による認証プロトコルのブロック図である。

【発明を実施するための形態】

【００２７】

本明細書において説明したように、ＨＥＬＰ ＰＵＦはハードウェア・ベースの認証に

適した「強いＰＵＦ」である。セキュリティ・プロパティは、特に、クレジット・カード、埋め込みセンサ、および医療用インプラントのような、リソースに制約がある現場ハードウェア・トークン(resource-constrained in-field hardware token)の側において、プロトコルの複雑さを低減する。トークンに要求される暗号関数の数を最少限に抑え、面積およびエネルギ双方のオーバーヘッドを低減する単純なＰＵＦベースの認証方式を提案する。

【００２８】

ＨＥＬＰ ＰＵＦのエントロピ（ランダム性）のソースは、機能ユニットを定めるパスの遅延に起こる製造ばらつきである。パス遅延は、図１に示すようなクロック・ストローブ技法を使用して測定される。機能ユニットとは、加算器、乗算器、または暗号プリミティブとすることができる。「ローンチ行ＦＦ」(Launch Row FF)および「キャプチャ行ＦＦ」(Capture Row FF)も、機能ユニットのコンポーネントである。ＨＥＬＰ ＰＵＦを機能ユニットに統合するときに必要とされる唯一の修正は、Clk_2で示す第２クロックの使用を必要とすることであり、第２クロックはキャプチャ行ＦＦを駆動する。

【００２９】

図１における検査対象パスに対してＰＵＴで示す１組のパスの遅延は、図１に示すClk_1およびClk_2を使用して、クロック・ストローブと呼ぶ、一連のローンチ－キャプチャ・クロッキング・イベント(launch-capture clocking event)を適用することによって測定される。Clk_1およびClk_2間の位相シフトは、ローンチ－キャプチャ検査のシーケンスにわたって徐々に大きくなる。これら２つのクロック間の位相シフトのディジタル選択値を、ローンチ－キャプチャ・インタバル（「ＬＣＩ」）と呼ぶ。

【００３０】

ローンチＦＦから開始するパスに沿った伝搬エッジ(propagating edge)をキャプチャＦＦにおいてキャプチャすることを可能にする最も小さいＬＣＩが、そのパスに対するディジタル化タイミング値として使用される。ローンチＦＦから主入力（「ＰＩ」）に適用される１組の二進入力ベクトルに対してクロック・ストローブ動作を繰り返すことによって、多数のパスに対するディジタル・タイミング値を得ることができる。

【００３１】

位相シフト・クロックを作成する能力は、オンチップ・ディジタル・クロック・マネージャ（「ＤＣＭ」）の極普通の機能である。ＤＣＭを含まない低価格コンポーネントでは、マルチタップ遅延チェーンを使用して、小さい面積オーバーヘッドで、この位相シフト能力を実現することができる。本願に限ったことであるが、ＬＣＩパス・タイミング値を「ＰＵＦＮｕｍ」または「ＰＮ」と呼ぶ。２つのランダムに選択したＰＮの符号付きの差を「ＰＮＤｉｆｆ」と呼ぶ。

【００３２】

本発明の一実施形態によれば、２５°Ｃ、１．００Ｖにおける登録中に、１０，０００本の安定したパスを測定する。登録中に検査されたパスは、ファイルに格納され、９箇所の温度－電圧（「ＴＶ」）コーナーにおける再生(regeneration)の間に再現(replay)される。ＴＶコーナーとは、V_{DD}供給電圧（－５％、正常、＋５％）および温度（０°Ｃ、２５°Ｃ、８５°Ｃ）の全ての組み合わせである。ＦＰＡ掃引範囲は、２００から１０２０までででサイズ２の刻みであるので、各パスは、最大（１０２０－２００）／２＝４１０回、クロック・ストローブを使用して再検査される。

【００３３】

図２は、ＴＶコーナーの各々におけるチップC_1に対する最初の１００本の安定したパスの遅延のグラフを示す。「Ａ」で示す波形は、供給電圧V_{DD}＝０．９５Ｖ（または－５％）における遅延を表す。「Ｂ」で示す波形は、供給電圧V_{DD}＝１．００Ｖ（正常）における遅延を表し、「Ｃ」で示す波形は、供給電圧V_{DD}＝１．０５Ｖ（または＋５％）における遅延を表す。各「Ａ」、「Ｂ」、「Ｃ」の３本の重複する波形は、３通りの温度の各々における遅延を表す。V_{DD}の変動は温度の変動よりも遙かに重要であることは明らかである。ＴＶ変動の正味の効果は、図２の底辺に沿った波形によって示されており

、この波形は、登録中に測定された遅延と、９箇所のＴＶコーナーの各々において測定された遅延との間の点毎の差として計算されたものである。ＴＶ変動がない場合、２５°Ｃ、１．００Ｖにおける登録波形を同じＴＶコーナーにおける再生波形から減算する場合について示すように、差波形は０になるはずである。差波形におけるパスの殆どについて描かれた０からの遅延における平均一定オフセットが、ロバストな検査可能なパスと関連付けられる。ロバストな検査可能なパスとは、定義によれば、いずれのＴＶコーナーにおいても安定であり続けるパスである。これは、感作されたパス(sensitized path)に沿ったゲートの全ての側入力(all side inputs)が安定であり続ける、即ち、これらは不調を生じないからである。

【００３４】

対照的に、遅延が動的に変化するパスは、ロバストでない検査可能なパスと関連付けられ、感作されたパスに沿ったゲートの側入力が瞬間的に変化する。ある側入力上の変化が、感作パス入力上の変化の前に僅かに変化した場合、感作パスに沿って伝搬するエッジが、側入力グリッチによって瞬間的に遅延を受ける可能性がある。一方、このために、このパスの遅延に追加の変化またはジャンプが混入する（ＴＶコーナー条件によって混入される変化を超えて）。これらの事例は、１つまたは少数のＴＶコーナーにおいてのみ生ずる遅延の大きな変化によって最も顕著になる（様々な事例が図２において円で囲って示されている）。

【００３５】

ビットストリングの生成において、パス遅延を同じチップ上における他のパス遅延と常に比較すると仮定すると、双方の遅延におけるいずれｎのタイプの統計的な変化も、同じビット値を生成することを可能にする。しかしながら、ジャンプのために１本のパスに大きな遅延変化が生じた場合、ビット反転が起こる可能性がある（大抵の場合、起こる）。どのパスがジャンプを生じそうか見極めることによって、ビットストリングの信頼性高い再生に関する不確実性を低下させるまたは排除することができる。

【００３６】

本発明によれば、登録中にこれらのパスをより多く発見するために、ビットストリングがエラーなく再生される確率を高める手段として、電圧ベースの登録方式を設計する。

【００３７】

一実施形態によれば、電圧ベースの登録を使用する認証を受ける不偏的無モジュラス差（「ＵＮＭＤ」：Universal No-Modulus Difference）方法の下でビットを生成する。このビットはＵＮＭＤの下で生成されるが、任意のビット生成方法、例えば、デュアルＰＮカウント（ＤＰＮＣ）も可能であると考えられる。

【００３８】

１対のパス遅延間における符号付きの差を、ディジタルＰＮ表現を使用して計算することによって、ＵＮＭＤ方法の下でビットを生成する。前述のように、ＬＣＩパス・タイミング値を「ＰＵＦＮｕｍ」または「ＰＮ」と呼び、２つのランダムに選択されたＰＮの符号付きの差を「ＰＮＤｉｆｆ」と呼ぶ。差が負のときは「０」ビットが生成され、一方差が正のときは「１」ビットが生成される。ビットストリングの再生でエラーをなくす可能性を高めるために、温度－電圧（「ＴＶ」）条件の変化によって混入されるノイズやドリフトを克服するように、差が十分に大きいＰＮ対を選択するために閾値を使用する。

【００３９】

一例として、正常状態の下におけるチップC_1についての遅延分布を、$PNDiff_a$および$PNDiff_b$で示す２つの対の例と共に、図３Ａに示す。$PNDiff_a$の大きさのために、図３Ｂに示すＰＮ差分布の中央に「無効領域」が生じ、したがって、この対におけるＰＮには登録中に無効と印される。

【００４０】

対照的に、$PNDiff_b$の大きさの方が大きく、図３Ｂの「０」領域内に現れる。公開データ・ビットストリング(public data bitstring)は、ビットストリング生成に関与するＰＮ（「１」と印される）、および関与しないＰＮ（「０」と印される）を記録する

。この判断基準は、不安定なパスについて以前に与えられたものを増大させる。したがって、検査された各パスは、１）パスが１つの遷移を生じる（安定である）場合、および２）対のＰＮ差が閾値よりも大きい場合、「１」で印された対応する公開データ・ビットを有する。

【００４１】

エラーのない再生を確保するためには、一定の方法を使用して全てのＴＶ条件下において全てのチップにおいて全てのビット反転エラーを排除するために比較的大きな閾値が必要であるが、一方、ビットストリングに利用可能なビット数が減少する。

【００４２】

例えば、図３Ｂは、閾値が平均してほぼ＋／－４０であることを示す。これは、４０×３６ｐｓ＝１．４ｎｓに換算される。これによって、ＨＥＬＰ ＰＵＦがダイ内部のばらつきを利用することが可能になるが、排除されるパス対の数はかなり大きくなる。これらの対の多くはＴＶコーナー全体にわたって安定であり続け、即ち、ビット反転エラーを混入せず、したがって、閾値を設定することに伴って、比較的大きな「歩留まり損失」(yield loss)がビットに生じる。

【００４３】

電圧ベースの登録（「ＶＢＥ」）は、閾値を小さくすることを許容することによって、この歩留まり損失の問題に取り組むように設計されている。有利なこととして、ＶＢＥは、同じ１組のＰＮを使用して、ビットストリングのサイズを平均で６７％増大させる。ＶＢＥによれば、登録は複数の供給電圧において実行される。本発明の一実施形態によれば、３つの供給電圧が使用されるが、いずれの数でも可能であると考えられる。

【００４４】

温度とは異なり、供給電圧は、素早く、例えば、ＤＶが小さい場合にはミリ秒範囲で変化する可能性がある。しかしながら、小さい変化はＭＵＴ遅延に大きな変化をもたらす。一般に、ＶＢＥは、パス遅延の供給電圧に対する高い感度を、他のＴＶコーナーにおいてどのパス遅延がジャンプするかより良く予測する手段として利用する。

【００４５】

図４に示すように、パス対の部分集合がｘ軸に沿って、ｙ軸上の対応するＰＮ差と比較して、プロットされている。ＰＮ差は、ＰＮの対を減算することによって計算される。図４は、１本の登録曲線および２本のＶＢＥ曲線を示す。６本の再生曲線の内２本だけを示す（他の４本の曲線は登録曲線と一貫性があり、グラフにおける乱雑を減らすために省略した）。対の番号５４４、５４６、および５４７は、ビット反転が起こった場合を示す。ビット反転は、１組の曲線を横切る点が０ラインの両側に現れるときにはいつでも起こる。ＰＮ差に関連付けられた異なる符号は、生成されたビットを「０」から「１」に、またはその逆に変化させる。これらの対は再生中にビット反転を混入させるおそれがあるので、ＶＢＥは、これらの問題がある対を特定しこれらをビット生成プロセスから除外する手段として、２つの追加の電圧コーナーを使用する。

【００４６】

ＶＢＥの第１異形(variant)によれば、ビットストリングは、３つの電圧、０．９５Ｖ、１．００Ｖ、１．０５Ｖの各々において３回計算され、各ビット位置において３つのビットの不一致を捜す。尚、ＶＢＥビットストリングは、再生プロセスを使用して生成され、再生プロセスは検査すべきパスを決定するために登録からの公開データを使用することは注意してしかるべきである。所与のビット位置におけるビットが他の２つと異なる場合、登録ビットストリングおよび公開データは、このビットおよびパスを排除するために更新される。図４において５４４および５４６で示されるビットおよび対が除去される。何故なら、２５°Ｃ、０．９５ＶのＶＢＥビットストリングにおいて生成されたビットは登録ビットとは異なるからである。生憎、この方法を使用しても、対５４７におけるビット反転は検出されない。しかしながら、この場合、２５°Ｃ、１．０５ＶのＶＢＥ曲線からのデータ点に関連付けられたもっと小さいＰＮ差を、予測器として使用することができる。

【００４７】
ＶＢＥの第２異形によれば、以上で論じた第１異形では見逃されたビット反転に対処するために、ジャンプ・マージン・パラメータを使用する。具体的には、第２異形は、ビット反転はないが、ＶＢＥデータ点の内１つまたは双方がジャンプ・マージン未満である場合、対を除去する。例えば、ジャンプ・マージンを３０に設定すると、対５４７によって混入されたビット反転エラーが検出および除去される。
【００４８】
図５における曲線は、種々のジャンプ・マージン値を使用したＶＢＥの有効性を示し、ジャンプ・マージンはｘ軸に沿ってプロットされている。左側のｙ軸は、全てのチップおよびＴＶコーナーにわたって発生したビット反転の総数を示す(count)。ＶＢＥがディスエーブルされると、ビット反転の数は１７０になる。ＶＢＥをイネーブルするが、０のジャンプ・マージンを使用すると、この数が６４に減少する。したがって、ＶＢＥの異形１では、ほぼ６２％ビット反転の数が減少する。異形２の影響(impact)を、この曲線の残りの成分によって示す。例えば、１５のジャンプ・マージンを使用すると、ビット反転の数は３８に減少する。また、ｘ軸に沿ったジャンプ・マージンの各々について、平均ビットストリング・サイズも右ｙ軸に沿ってプロットされている。ビットストリングの平均サイズは７８０として与えられる。ジャンプ・マージンが２０に増大するまでに、非常に小さい変化がサイズに生じ、ジャンプ・マージンが４０以上になると、大きな減少が始まる。これは、明らかに、ビット反転の数を減少させつつ、更に歩留まり損失によるビットの不利な条件(yield loss bit penalty)を低減するときにもＶＢＥの効果(benefit)があることを示す。
【００４９】
ジャンプ・マージンが２０未満ではビット反転の数はゼロでないので、ＶＢＥをある種の生成方法と組み合わせて、エラーのない再生を達成しなければならない。しかしながら、ビット反転の数が少ない程、閾値を小さくすることが可能になる。例えば、１５のジャンプ・マージンを用いつつ、全てのＴＶコーナーにおいて全てのチップに対してエラーのない再生を保持すると、閾値がＰＮ＝２３（ほぼ８２０ｐｓ）に減少する。
【００５０】
１０，０００本のパスを生成するには、約３０，０００本のパスを検査する必要があった。検査したパス毎に１ビットの公開データ・ストレージを必要とするので、公開データ・サイズは約３．７５ＫＢとなる。本願で提案する技法は、再検査されるパスを排除するので、有効なパスの本数を１０，０００から５，０００に減らす。ビットストリング生成アルゴリズムは、チップ毎に５，０００のシーケンスにおいて連続するＰＮからパスの対を作成する。したがって、５，０００個のＰＮを使用して最大２，５００ビットを生成する。前述のように閾値を８２０ｐｓに設定すると、有効なＰＮ対（またはビット）の数は約１，３００に減少する。ＴＭＲは、ビットストリングのコピーを３つ組み立てるが、これを達成するためには平均で５つのコピーが必要となる。したがって、最終的な平均ビットストリング・サイズは１，３００／５　２５９ビットとなる。
【００５１】
最も小さいビットストリング・サイズである２２７ビットを使用すると、チップ内ハミング距離（ＨＤ）はゼロとなる。即ち、９箇所のＴＶコーナーのいずれにおいても３０チップのいずれにもビット反転はない。チップ内ＨＤは４９．７％であり、理想値である５０％に近い。図６は、個々のＨＤのヒストグラムを示す。チップが３０個あると、ＨＤは、３０×２９／２＝４３５対のチップ・ビット・ストリングと計算される。
【００５２】
本発明によれば、信頼性向上およびエントロピ増大はグリッチのない機能ユニットによって得られる(provide)。本発明の実施形態によれば、代入ボックス（「ＳＢＯＸ」）コンポーネントが機能ユニットとして使用される。暗号法では、ＳＢＯＸは、代入を実行する対称鍵アルゴリズムの基本コンポーネントである。一般に、ＳＢＯＸはある数ｍの入力ビットを取り込み、これらをある数ｎの出力ビットに変換する。ここで、ｎは必ずしもｍ

に等しくはない。

【００５３】

ＳＢＯＸコンポーネントは、「標準設計」または「ＷＤＤＬ設計」と呼ばれる２つの方法で実装される。「標準設計」は、いずれのタイプの特殊なロジック・スタイルも、制約もなく、即ち、通常に合成される。「ＷＤＤＬ設計」は、波動差動的ロジック(wave-differential dynamic logic)を使用し、グリッチがない。本発明については、グリッチを排除するためのＷＤＤＬを使用して論ずるが、グリッチを排除する技法はいずれも可能であると考えられる。２つのロジック・スタイルのランダム性、一意性、および信頼性に対するトレードオフを決定するために、チップ間ハミング距離（「ＨＤ」）を評価する。

【００５４】

温度および電圧の変動は、遅延に望ましくない変化を生じさせるが、その殆どはＴＶ補償プロセスを適用することによって除去することができる。ＴＶ補償は、チップ毎に、そしてＴＶコーナー毎に別々に、１組のＰＮＤｉｆｆから平均（オフセット）および範囲（乗数）を計算することによって実行される。登録中に計算されるオフセットおよび乗数が、各ＴＶコーナーにおいて計算されるオフセットおよび乗数と共に使用され、式１を使用してＴＶコーナーにおいて生成されるＰＮＤｉｆｆを補償する。

【００５５】

【数１】

$$zval_i = \frac{(PNDiff_{TVx} - \mu_{TVx})}{rng_{TVx}}$$

$$PNDiffs_{TVComp} = zval_i rng_{TVEnroll} + \mu_{TVEnroll}$$

【００５６】

ここで、$zval_i$は、平均を減算し、特定のチップに対してＴＶコーナー、TV_Xにおいて生成された１組のＰＮＤｉｆｆを使用して計算された範囲で除算した後の、標準化されたＰＮＤｉｆｆを表す。次いで、登録中に同じチップについて先に計算された平均および範囲を使用して、即ち、ＴＶＥｎｒｏｌｌにおいて個々の$zval_i$を変換する。登録中に生成されたＰＮＤｉｆｆは「基準」として使用される。この線形変換は、異なるＴＶコーナーにおいてパス遅延に発生するずれ(shifting)および増減(scaling)を排除するのに非常に有効である。

【００５７】

モジュラス方式に基づく第２のビット生成方式は、グリッチのない機能ユニットにおいてエントロピを利用するときには更に効果的である。モジュラス方式は、モデル構築に対抗してアルゴリズムをハードニングする(hardening)手段、およびＰＵＦ応答において多様性を増加させる手段の双方として、２つパス遅延における符号付きの差（ＰＮＤｉｆｆ）を使用する。ＭｏｄＰＮＤｉｆｆは、２つの任意に選択されたＰＮ間における符号付きの差を計算し、次いでモジュラスを適用することによって定められる。モジュラスが必要なのは、ＦＵにおけるパスの長さが変動するからである。例えば、短いパスは１つのＬＵＴで構成されるが、最も長いパスは１３個のＬＵＴで構成され、ＰＮＤｉｆｆにおいてキャプチャされる。モジュラスは、「パス長」バイアスを除去しつつ、ダイ内部のもっと小さい遅延のばらつきを完全に保存する。

【００５８】

例として、図７の一番上に、「立ち上がりエッジＰＮ」および「立ち下がりエッジＰＮ」で示す２組の波形を示す。これらの波形における点は、ＳＢＯＸ機能ユニットにおいてチップC_1における１組のパスから測定された遅延値（ＰＮ）を表す。同様の形状を有する波形の各グループは、ＴＶ補償方法を適用した後において１０箇所のＴＶコーナーの各々において測定されたＰＮを表す（以上で説明したＰＮＤｉｆｆに適用されたＴＶ補償と同一のプロセス）。１０個の点に広がる垂直線は未補償のＴＶノイズを表す。図７の真ん中に示す波形は、図７の一番上に示した、立ち上がりおよび立ち下がりエッジＰＮのラン

ダム化された対から計算されたＰＮＤｉｆｆを表す。チップ$Ｃ_{1}$のデータのみを示すが、パス長バイアスのために、差波形の形状は他のチップでも同様である。図７の一番下に示すＭｏｄＰＮＤｉｆｆは、６４のモジュラスを、図７の真ん中に示した立ち上がりおよび立ち下がりエッジＰＮのランダム化された対から計算されたＰＮＤｉｆｆに適用した結果である。モジュラスは、全ての差を０から６３の範囲内に効果的に「包み込み」、バイアスを減少および／または排除する。ビット生成アルゴリズムは、０から３１までの範囲内にあるＭｏｄＰＮＤｉｆｆを「０」として指定し、３２から６３の範囲内にあるＭｏｄＰＮＤｉｆｆを「１」として指定する。

【００５９】

図７の真ん中において見られるように、点１０および１４における円はビット反転を示す。ビット反転が起こるのは、各グループにおける１０個の点の全てではないがいくつかが、０または６３によって与えられる境界の内１つを交差するときである。図７の一番下において、点４の円によって追加のビット反転が示されており、これらの点は「０」および「１」の間の境界を交差する。近い１０個の点をグループ化することにより、これらのビット反転の殆ど／全てを回避する予測スクリーニング・プロセスを適用することが可能になる。これについては以下で更に詳しく論ずる。更に、前述のようにバイアスを除去するためにモジュラス・パラメータを使用することができるが、以下で更に詳しく論ずるように、これはＨＥＬＰ　ＰＵＦの入力－出力空間を広げるのにも有用である。

【００６０】

「ＷＤＤＬ設計」によれば、波形差動ダイナミック・ロジック（「ＷＤＤＬ」：wave-differential dynamic logic）を、全体的なばらつきおよびダイ内部遅延ばらつきによって混入されるエントロピを測定する手段として、そしてＨＥＬＰ　ＰＵＦの信頼性を高める手段として使用して、グリッチのないＳＢＯＸコンポーネントを実現する。ＷＤＤＬは、刺激制約(stimulus constraints)を強制し、正ゲート(positive gate)のみを使用するように実施に制約を設けることによって、機能およびロジックのハザードを排除する。ＷＤＤＬは、ＡＥＳのような設計ユニットをサイド・チャネル攻撃に対抗してハードニングするメカニズムとして提案され、したがってパワー曲線(power curve)における情報も排除しようとする。ＷＤＤＬの利点は、実施が簡単であり、グリッチのないロジックの実施を評価するのに相応しいテスト・ベッドを提供することである。

【００６１】

機能ユニットのＷＤＤＬバージョンを作成するプロセス・フローの詳細を以下に示す。簡略化のために、ネットリストのＷＤＤＬバージョンは、元のネットワークと、１組の二重ゲートで組み立てられた相補ネットワークを含むことが知られればよいとする。ＳＢＯＸの８つの主入力が複製され、相補ネットワークを駆動するために補完される。ＷＤＤＬの動作は２つのフェーズ、即ち、プリチャージ・フェーズおよび評価フェーズで構成される。プリチャージ・フェーズは、全ての主入力（相補入力を含む）を「０」で駆動することを含む。これは、回路全体における全てのゲートの入力および出力上に０を強制する。評価フェーズは、真値および相補値を８つの真および相補主入力にそれぞれ印加し、１組の立ち上がり遷移を回路全体に伝搬させる。ＳＢＯＸ実装のために、平均して真出力の半分および相補出力の半分が評価中に遷移する。したがって、２５６通りの可能な入力遷移の各々について、即ち、００００００００からｘｘｘｘｘｘｘｘまで、合計で２０４８個のＰＮを生成するために８つのＰＮが得られる。プリチャージ・フェーズの間に、他の２０４８個、即ち、ｘｘｘｘｘｘｘｘから００００００００までが得られるので、合計で４０９６個のＰＮが生成され、これらから２０４８個で１組のＰＮＤｉｆｆを一意に組み立てることができる。

【００６２】

温度０°Ｃ、２５°Ｃ、および８５°Ｃ、ならびに供給電圧０．９５Ｖ、１．００Ｖ、および１．０５Ｖにおいて、３０個のチップ上で実験を行った。ＴＶコーナーにおいてこれら３０個のチップから測定された２０４８個のＰＮＤｉｆｆの２５点サンプルを図８に示す。ＰＮＤｉｆｆの計算は、ＰＮの一意のランダムな対、即ち、立ち上がりパスから１

つおよび立ち下がりパスから１つを選択することによって行われる（図７の一番上のグラフを参照のこと）。波形のグループは、前述のように、チップ毎に登録値を「基準」として使用してＴＶ補償されている（式１参照）。波形グループ間の垂直方向のオフセットは、全体的な（チップ規模）ばらつきによって、即ち、チップの全体的な性能特性のばらつきによって発生する。ダイ内部のばらつきと同様、全体的なばらつきをエントロピのソースとして利用することができるが、それに依存することには欠点がある。

【００６３】

この問題を例示するために、図８の底辺に沿って示す波形は、この場合も３０個のチップからであるが、チップC_1からの登録データが全てのチップに対する基準として使用される特殊なプロセスを使用してＴＶ補償された場合である。これは、全体的なばらつきを効果的に排除し、測定ノイズ、未補償ＴＶノイズ、およびダイ内部のばらつき（ＷＤＶ）のみを残す（図８を参照のこと。）。大きな母数のチップでは、複数組のチップが同じレベルの全体的なばらつきを有する可能性が非常に高く、したがってこのグラフはこの場合を示し、ダイ内部のばらつきのみをエントロピのソースとして利用することができる。

【００６４】

ノイズ・ソースの大きさは、図８の上側に沿って示す波形の帯域の幅に反映される。測定ノイズ（１６個のサンプルで平均した場合）は、平均してほぼ１ＰＮ（ほぼ１８ｐｓ）であるので、ばらつきの大半が未補償ＴＶノイズによって混入されたことになる。波形内に残る、１０個のＴＶ補償ＰＮＤｉｆｆの２σ値の平均として計算されたばらつきの平均値は、平均して、登録値の上または下に約＋／－２．５ＬＣＩまたは４５ｐｓであり、最悪の場合の値は＋／－８ＬＣＩまたは１４５ｐｓ未満である。この数は、失われたエントロピの量を表すので重要である。即ち、このＬＣＩ値未満のダイ内部のばらつきは、利用することが更に困難になる。ダイ内部のばらつきは、チップ毎の波形グループの形状における変化に反映される。ダイ内部のばらつきによって混入されたばらつきの大きさは、平均して、ＴＶノイズによって混入される平均ばらつき（５ＬＣＩ）よりも約４倍大きく（２０ＬＣＩ）、即ち、それぞれ３６０ｐｓに対して９０ｐｓとなる。

【００６５】

本発明によれば、マージン技法を使用することによって信頼性を向上させる。マージン技法は、登録中に、ビット反転を混入させる確率が最も高いＰＮＤｉｆｆを特定する。図７の一番下に沿って示すＰＮモジュラスのグラフが、例示として役割を果たすために、図９にコピーされている。図９は、ビット反転が発生する３つの場合を示す。これらのデータ点の全ては、「０」および「１」の間の境界を表す線、即ち、０、３１、および６３に近接する。マージン技法は、登録ＰＮＤｉｆｆがこれらの境界周囲の小領域（マージン）内に入る場合、それを「無効」と分類する。このマージンは、理想的には、最良の結果に対する最悪の場合のＴＶノイズ・レベルに設定される（図９では８のマージンが使用されている）が、要求される許容度のレベルにしたがって調整することができる。登録の間に、各ＭｏｄＰＮＤｉｆｆデータ点の有効ステータスを記録するヘルパー・データ・ビットストリング(helper data bitstring)が組み立てられる。再生の間、応答における「弱い」ビットを選別し破棄するために、ヘルパー・データが使用される。

【００６６】

また、ＰＮモジュラスおよびマージンの特定の組み合わせが、応答ビットストリングにおいて、破棄されたビットを使用可能にする。図９に示す例は、１つの有効な組み合わせを示し、ＰＮモジュラスが６４であり、マージンは８に設定されている。この例では、ヘルパー・データの補数(complement)を使用して第２応答ビットストリングを生成することが可能である。第２応答ビットストリングは、同じ１組のＰＮＤｉｆｆを使用するが、モジュラス処理を適用する前に、最初にＰＮＭｏｄの１／４に等しいオフセット（この例では１６）を加算する。これは、効果的に分布をシフトさせ、以前の「弱い」ビットの全てを「強い」ビットに（そしてその逆に）変換する。この技法は、全てのデータ点を応答ビットストリングにおいて使用することを可能にし、ヘルパー・データのサイズ対応答ビットストリング・サイズを１対１にすることによって、ヘルパー・データのオーバーヘッド

の不利(penalty)を低減する。この技法は、マージンによって明確に定められた(delineated)領域の総和が「０」および「１」に対して定められた「有効な」領域の総和に等しい場合に使用することができる。

【００６７】

２つのロジック・スタイルのランダム性、一意性、および信頼性に対するトレードオフを決定するために、チップ間ハンマリング距離（「ＨＤ」）を評価する。図１０は、標準設計ＳＢＯＸから収集したデータを使用した統計結果を示す。分析は、ｘ軸に沿ってプロットされた１組のＰＮモジュラス（ＰＮＭｏｄ）値に対して行う。登録中に２つのチップによって生成された２０４８ビットのビットストリングにおいて異なるビットの数を数え、次いでビット数で除算することによって、チップ間ＨＤを計算する。プロットされた値は、ビットストリングの全ての可能な対（３０×２９／２＝４３５対）にわたる平均チップ間ＨＤである。同様にしてチップ内ＨＤを計算するが、チップ毎にＴＶコーナーにおいて生成されたビットストリングを使用して対を定めることを除く（１０×９／２＝４５対）。この場合も、プロットされた値は、３０個の個々のチップ値にわたって計算された平均である。最悪の場合のチップ内ＨＤは、単に、個々のチップの内の１つによって生成された最大値である。図１０Ａにおける最悪の場合および平均の場合のチップ内ＨＤの曲線は、ノイズ・レベルを反映し、一方チップ間およびチップ内ＨＤ曲線間の差は、使用可能なエントロピの範囲を反映する。結果は、全体的なばらつきと共に、および全体的なばらつきなしで示されている。

【００６８】

チップ内ＨＤ（理想的には０％である）の比較的大きな値は、グリッチ(glitching)の存在に直接起因する。尚、グリッチはチップ内およびチップ間ＨＤ双方を増大させる可能性があることに注意すべきである。全てのＴＶコーナーにわたって一貫してグリッチによって遅延が影響を受けるパスでは、パス遅延は通例１０から１００ＬＣＩだけ変化し、したがってダイ内部のばらつきの大きなソースを表すので、この効果は有益である。グリッチが一部のＴＶコーナーにおいて存在し他では消失するパスでは、この効果は有害であり、ビット反転に至る。最悪の場合のチップ内ＨＤおよびチップ間ＨＤ曲線は、双方のタイプが発生することを示す。チップ間ＨＤは増加するが、この効果は最悪の場合のビット反転の増加によって、部分的に相殺される。一方、平均の場合のチップ内ＨＤは僅かに増加するだけである。

【００６９】

図１０Ｂは、マージン技法を適用した後の結果を示す。マージン技法は、図１０Ｂに示すように、チップ内およびチップ間ＨＤの結果双方を著しく改善する。応答における「弱い」ビットを識別するために、８のマージンを閾値として使用したが、いずれのマージン数も可能であると考えられる。チップ間ＨＤが改善するのは、異なるチップにおける「強い」ビットの生成に対応するＰＮＤｉｆｆがここでは変動する可能性があるからである。これが正しいのは、ダイ内部のばらつきは、一部のチップについてのＰＮＤｉｆｆがマージン内に入る原因となるが、他のチップについては、同じＰＮＤｉｆｆがマージンの外側に出るからである。他の重要な特性は、全体的なばらつきが存在するか否かに対する結果の感度が低いことであり、これは非常に望ましい特徴である。また、図１０Ｂには、前述した特別な「相補ヘルパー・データ」方式が使用されないとき、この場合におけるオーバーヘッドを示すために、３０個のチップの内の１つによって生成された最も小さいビットストリングのサイズも、ヘルパー・データに伴うオーバーヘッドを示すために、プロットされている。６４以上であるＰＮＭｏｄを選択することによって、ヘルパー・データ・ビットストリングは、最悪の場合における応答ビットストリングのサイズの２倍以下となる。

【００７０】

ＷＤＤＬバージョンを使用した結果を図１１に示す。ＷＤＤＬバージョンに存在する長い方のパスは、図１１Ａの左側に示すように、チップ間ＨＤのほぼ理想的な改良に寄与する(responsible)。つまり、長い方のパスはチップ間ＨＤを改良するが、全体的なばらつ

きが保存される場合、即ち、全体的なばらつきがないチップ間ＨＤ曲線が非常に異なる結果を示す場合だけである。一方、図１１Ｂに示すマージン技法を使用した結果は、全体的なばらつきがある場合もない場合も、ほぼ理想的である。また、チップ内ＨＤ曲線は、図１０Ｂからの対応する結果の中に残っているビット反転の大多数は、「標準設計」において生成されたグリッチに起因することも示す。即ち、遅延の変化は、マージンとして使用される最悪の場合のＴＶノイズよりも大きいので、マージン設定(margining)はグリッチには有効ではない。これは、最悪の場合に対するほぼ０の値、およびＷＤＤＬバージョンに対する平均チップ内ＨＤによって明らかである。

【００７１】

グリッチのない機能ユニットの利点を考えると、これらを実装するときのオーバーヘッドを低減することが望ましい。具体的には、本発明は、ＷＤＤＬ型実施態様(WDDL-like implementation)において使用することができる、効率的な分岐限定アルゴリズムを使用して、２入力から６入力までのゲートのハザード・フリー関数(hazard-free function)について完全な１組の真理値表を生成する方法を含む。このアルゴリズムは、ＷＤＤＬロジックについて先に説明したように、プリチャージ・フェーズおよび評価フェーズによって、２フェーズ・ロジック・スタイルを取る。尚、このアルゴリズムは他のタイプのプリチャージおよび評価条件に合わせて改変できることは注意してしかるべきである。導かれたハザード・フリー関数から選択された部分集合（１つまたは複数）をＣＡＤ合成ツールにおいて使用して、以下で説明するように、ゲートの数を最少限に抑えること、そして機能の実装に多様性を追加することの双方を可能にする。

【００７２】

このアルゴリズムはｎ入力(n-input)関数のカルノー図（Ｋ－図）の抽象的表現をそのデータ構造として使用する。遷移キューブ(transition cube)とは、開始点Ａ、終了点Ｂを有し、ＡからＢへの遷移中に到達することができる全ての入力の組み合わせを収容するキューブを意味する。ハザードがない回路の実現では極普通であるように、ゲート入力は、主入力に対する２ベクトル検査の適用中せいぜい１回しか変化しないと仮定されるが、任意の順序で変化することができる。関数ｆを実装するゲートをハザードなく実現すると、その出力においてせいぜい１回しか遷移しない。

【００７３】

ＷＤＤＬスタイルの関数に関連付けられた遷移は、追加の制約を有し、図１２において３入力関数ｆ＝ａ＋ｂｃについて示すように、関数のカルノー図における開始点がｆ（０００．．０）＝０でなければならない（これは、「全て０」プリチャージ条件によって強制される）。評価中に、Ｋ－図において辿る(traverse)ことができるパスの全てを、曲線によって強調する。図１２の右側は、これらのパスを「ゲート入力値－出力値」というフォーマットでリストにして示す。尚、開始点が（０００）＝０であり、終了点が（１１１）＝１であっても、このゲートが実際の動作において感作されるときに全ての入力が変化することは必要でなく、したがって、終了点は、リストに示されたパスに沿った任意の点であることができ、それでもなおハザードのない動作を維持することに注意すること。

【００７４】

本発明によれば、これらの制約を満たす全ての関数を生成するアルゴリズムは、６入力までのゲートに対するＫ－図表現を組み立てる（最新のＦＰＧＡ上のＬＵＴ入力サイズと一致する）。図１２の右側にリストに纏めた軌跡(trace)は、このアルゴリズムのテンプレートとして使用される。ｎ入力ゲートでは、軌跡の長さはｎ＋１となる。例えば、図１２の３入力ゲートでは軌跡長は４であり、軌跡の数はｎ！（階乗）によって示され、３入力ゲートでは６であるが、６入力ゲートでは７２０に増加する。この図の右側に示す出力値も、有効なＫ－図を発見するためにこのアルゴリズムによって使用される。左から右に軌跡順にリストに示された出力値は、温度計コード・フォーマットに対応する。即ち、０の後に１が続き、組み立てられたゲートのハザードがない動作を確保する。

【００７５】

６入力関数に可能なＫ－図の数は2^{64}であるので、ハザードがないという条件に対す

る一致の可能性を全て検索するのは厄介である。代わりに、全てのハザードのないＫ－図を繰り返し組み立てるために、分岐限定アルゴリズム手法(branch-and-bound algorithm approach)を開発した。このアルゴリズムは全ての可能な軌跡、およびこれらの軌跡に対する全ての可能な温度計コード指定を配列する(sequence through)。可能な温度計コード出力指定の数はｎとして与えられ、例えば、３入力ゲートでは（０００１，００１１，０１１１）として与えられる。図１２から、これらの温度計コード出力値の内２つだけ、即ち、００１１および０１１１が、関数ｆ＝ａ＋ｂｃに実際に使用されるが、３番目は他の有効なハザード・フリー３入力関数において使用される。

【００７６】

これは検索空間をｎ$^{n^b}$に、例えば、３入力関数では３^6＝７２９に広げるが、検索プロセスは、この検索空間の非常に大きな部分を排除する（限定する）ことを可能にし、６入力までの関数に対して、このアルゴリズムを扱いやすくする。ｎ本の軌跡の各々に、出力値に対して特定の温度計コードが指定され、Ｋ－図を定めるためにこれらの指定が組み合わされたときにｎ本の軌跡全てに一貫性があるとき、有効なＫ－図が求められる。一貫性とは、Ｋ－図における出力値に、全ての軌跡によって一貫して０または１が指定されるという要件のことを言う。１つの軌跡が０を指定し一方他の軌跡が１を指定するという場合に検索プロセスが遭遇したとき、このＫ－図、およびこの同じ「一貫性のない」指定を使用した全ての後続のＫ－図は無効になる(fail)。このアルゴリズムの特徴により、検索空間の大部分が排除される。例えば、可能な５$^{5!}$＝７．５ｅ＋８３個の５入力ゲートを求めて検索されるエレメントの数は１．８ｅ＋６個であり、一方生成される有効なＫ－図の数は７，５７９個である。６入力ゲートでは、有効なＫ－図の数は数百万個になる。

【００７７】

複雑過ぎるために、生成された関数の多くは合成ツールによって無視されるが、これは数百個のゲートの部分集合には該当しない。以下で説明するように、例えば、ＷＤＤＬロジックを使用して、合成に使用されるライブラリにこれらのゲートを含ませると、機能ユニットをハザードなく実装するときのゲート個数が減少し、合成のＦＰＧＡに対する直接的な利点(benefit)を表す。更に、開示するアルゴリズムによって生成されるハザード・フリー関数間における大きな多様性も、ＦＰＧＡ指向合成が、「機能多様性」(functional diversity)と呼ばれる、異なる「バージョン」の機能ユニットを作成することを可能にする。

【００７８】

分析に使用される機能ユニットを図１３に示す。図１３に示すように、この機能ユニットは、ＳＢＯＸ、およびＷＤＤＬ実装(WDDL implementation)の混合列コンポーネント（ここでは「ＭＩＸＣＯＬ」と呼ぶ）を含む。以上で説明したアルゴリズムを使用して生成されたハザード・フリー関数の内９０エレメントの部分集合を使用して、ＭＩＸＣＯＬの挙動ＨＤＬ記述からシングル・エンド型構造的ネットリスト(single-ended structural netlist)を合成する。９０エレメントの部分集合は、生成されたＥＸＴ関数の最も簡単なバージョンのみ、具体的には、各入力リテラル(input literal)の１つのインスタンスを含む関数のみを使用することによって選択された。構造的ネットリストは、ライブラリにおいて利用可能な９０個のセルの内２５個を使用して合成される。相補ネットワークを作成することによって、そして反転器を排除することによって、シングル・エンド・バージョンをＷＤＤＬバージョンに変換するために、Ｐｅｒｌスクリプトが使用される。この変換プロセスを図１４に示す。ここでは、反転出力を有するＥＸＴゲートが、同じＥＸＴゲートに、その二重（相補）ゲートを加え、反転器を排除する手段として出力が交換されたものに変換される。

【００７９】

ＷＤＤＬネットリストは、合成および実装ツール、例えば、Ｖｉｖａｄｏへの入力として使用される。ネットリストは最適化されるが、最適化の殆どは、最近のＦＰＧＡ ＬＵＴ特性に一致するように故意に組み立てられたＥＸＴライブラリを使用して、コンパイラによって既に行われている。一実施形態によれば、コンパイラ生成バージョンにおけるゲ

ートの総数は３，０９６個であり、一方Ｖｉｖａｄｏ生成バージョンは２，８９１個のＬＵＴを含んでいた。Ｖｉｖａｄｏによって生成されたＬＵＴベースのネットリストは、以下で説明する分析において使用される。

【００８０】

図１３のＭＩＸＣＯＬ機能ユニットにおいて、プリチャージ－評価制約を使用して、２ベクトル・シーケンスを３２の真入力および相補入力に印加することによって、ハザードのない遷移を生成する。例えば、６４ビットＷＤＤＬベクトル対は、（００．．．０／００．．．０，ｘｘ．．．ｘ／ｘｘ．．．ｘ）という形態で表すことができる。これは、プリチャージ中に真入力および相補入力双方に全て０が印加され、続いて評価中に集合２３２およびその補数からの任意のベクトルが印加されることを示す。

【００８１】

機能ユニットの個々のゲートおよびワイヤ内部でおよびこれらを跨いで発生する遅延のばらつきは、ＨＥＬＰ　ＰＵＦのための根本的なエントロピのソースとなる。ＨＥＬＰ　ＰＵＦは、パス遅延におけるエントロピを利用し、ゲートおよびワイヤ遅延からのばらつきを独自の方法で組み合わせる。本発明によれば、機能ユニットにおけるパスは、予測可能な様式で統計的に組み合わされておらず、むしろ複雑な相互接続ネットワークとして定められる。この複雑な相互接続ネットワークは、長さが変化し、グリッチを呈する可能性があり、数が非常に多く、感作することが困難な可能性がある。異なる長さのパスによって混入される望ましくないバイアスは、モジュラス技法を使用することによって、低減または排除することができ、一方望ましくないグリッチ(glitching)を排除するためには、ＷＤＤＬのようなグリッチのないロジック・スタイルを使用することができる。

【００８２】

機能ユニットをエントロピのソースとして使用することの主な利点の１つは、それが提供する大多数のパス、およびこれらを感作するためにベクトルを生成することの困難さに基づく。大多数のパスは、認証のような用途に、特に主な脅威メカニズムがモデル構築であるときに、利点をもたらす。

【００８３】

図１３に示すように、ＭＩＸＣＯＬのＷＤＤＬバージョンは、６４個の主入力と６４個の主出力とを有する。本来コンパイラによって生成されたネットリストのシングル・エンド・バージョン（ＷＤＤＬへの変換前）は、６５２個の反転器と、１，５４８個の論理ゲートとを有する。ＷＤＤＬへの変換によって、反転器が処理される（そして排除される）ときはいつでも、真および相補ネットワーク間に、相互接続(interconnector)が作られる。大多数の反転器は、２つのネットワークが多くの場所で相互接続されることを示す。ＭＩＸＣＯＬにおける構造的パスの総数は、１，７３２，０８５本である。ＭＩＸＣＯＬは機能ユニット全体の１／４未満を表すことを考慮すると、パスの総数は、最大バージョンの機能ユニットでは、一千万本を超えそうであることを示す。したがって、ＭＩＸＣＯＬの構造的ネットリストは、非常に多くのエントロピのソースを提供する。

【００８４】

ＷＤＤＬネットリストをプリチャージ－評価制約と組み合わせることによって、機能ユニットのグリッチのない動作を確保する。これらの制約の下で適用することができるＷＤＤＬベクトルの総数は2^{33}個であり、立ち上がり遷移および立ち下がり遷移双方から成る(account for)。相補ネットワークは、（６４の内）正確に３２個の主出力が各ベクトル・シーケンスの下で遷移し、合計2^{38}回の立ち上がりおよび立ち下がり遷移を生ずることを保証する。各遷移は、パスの検査に対応する。先に示したように、全てのパスがＷＤＤＬベクトルによって検査される場合、パスは１７０万本だけであり、次いで各パスは、全てのベクトルにわたって平均で約$2^{38}／2^{20}＝2^{18}$回検査される。

【００８５】

ＷＤＤＬベクトルによって検査されるパスの実際の本数を決定するために、シミュレーションおよび信号伝搬分析のための特殊な形態が必要となる。ネットリストの相互接続構造は、任意の特定のパスに沿ったゲート入力において再収束する複数の信号が、主出力に

おける信号遷移のタイミングを決定することを可能にする。例えば、ＡＮＤゲートへの入力上に最後に到達した０→１の遷移が、そのゲート上における出力の０→１遷移を制御する。同様に、ＯＲゲートでは逆の条件が成り立ち、最初の０→１遷移を駆動するパス・セグメントが、０→１の出力遷移を制御する。タイミングを支配する入力／セグメントは、パス入力、および出力遷移を制御する対応するパス・セグメントを指す。したがって、実際に検査されるパスは、タイミングを支配するパスに沿ったパス・セグメントで構成され、全ての他のパス・セグメントに関連付けられた遷移は隠される。隠されたパス・セグメントは、検査されるパスに関連付けられたエントロピには関与せず、数えられない。

【００８６】

図１５は、本発明の実施形態によるエントロピ分析のフロー・チャートを示す。この分析にしたがって、主出力の各々に対するタイミングを支配するパスを列挙する。このプログラムは、構造的ネットリストを使用し、２ベクトル・シーケンスとして生成されたシミュレーション・データが主入力に印加される。シミュレーション・データはファイル（例えば、「値－変化－減衰」ファイル）に保存され、タイムスタンプと、検査シーケンス（１つまたは複数）を受ける回路の各ノード上で発生する信号遷移との圧縮表現を与える。

【００８７】

このプログラムは、ＶＣＤファイルに取り込まれた検査ベクトル・シーケンスのタイミングを支配する、一意に感作されたパスの本数を報告する。また、これは、主出力（ＰＯ）上で起こった静的および動的ハザードの数、ならびに内部ノード上で起こったハザードも報告する（多くのハザードはＰＯ上では観察可能でない）。ＶＣＤファイルにおける信号遷移のタイミングは、最悪の場合のプロセス、温度、および供給電圧条件を表す。更に重要なのは、Ｖｉｖａｄｏはタイミング分布を全く与えず、ダイ内部のばらつきも全くモデリングしないことである。したがって、報告される結果は控えめとなる。何故なら、ダイ内部のばらつきは、他のパス・セグメントがタイミングを支配することを可能にすることもあるからである。実際のハードウェアをより良く近似するために、ＰＯ出力遷移毎に追加のパス・セグメントの報告を可能にする優勢パスを発見するために許容度パラメータが利用可能である。各チップにおいて、可能なパス・セグメントの各々の１つだけがタイミングを支配するが（２つ以上のセグメントが等しい遅延値を有するのでない場合）、ＰＯ遷移毎に生成されるパスのリスト、そして更に重要なのは、所与の許容度に対して報告される一意のパスの総数が、ハードウェアの挙動をより良く反映する。

【００８８】

以上で示したように、2^{33}個のＷＤＤＬベクトル（立ち上がりおよび立ち下がり）があり、これは、図１５に示すツール・フロー・チャート(tool flow chart)を使用して処理するには多過ぎる。代わりに、これらのＷＤＤＬベクトルの小さな部分集合を処理し、その結果を使用して、８６億個のベクトル全てについてパス収束を予測する。サイズ１，５００，１０００，２０００，４０００，８０００のベクトル部分集合によって行われる収束は、指数を使用する曲線当てはめである。予測されたＷＤＤＬベクトルの収束は、１７０万本以上の構造的パス(1.7+ million structural paths)の約２０％である。

【００８９】

実際にハザードなく検査可能なパスの本数は、任意のタイプの２ベクトル・シーケンスを使用して決定される。問題を扱いやすくするために、１７０万本以上のパスから部分集合を作成し、遭遇検査（「ＥＴ」：encounter test）への入力として使用する。ＥＴは、部分集合におけるパスのほぼ半分に対してハザードのない検査を生成することができ、機能ユニットからほぼ３０％多いエントロピを利用できることを示唆する。更に、全てのパスを検査するためのベクトルを生成することの難しさと、膨大な数の入手可能なパスとの組み合わせにより、敵が系統的に検査パターンをハードウェア・トークンに、モデル構築攻撃を実行する手段として適用することを難しく、または不可能にする。

【００９０】

１つの可能な認証プロトコルを図１６に示す。登録中に、サーバはランダム・チャレンジ、c_i、$PNMod_i$、および$margin_i$を生成し、これらはハードウェア・トー

クンによって入力として使用される。ＨＥＬＰ　ＰＵＦは、応答ｒ$_i$およびヘルパー・データｈ$_i$を生成し、これらをサーバ上にチャレンジ情報と共に格納する。全体的なばらつきが利用される場合、チップのためにμおよびｒｎｇも計算され、サーバ上に格納される（これらの値もチップの擬似ｉｄとして使用できることに注意すること）。多くの提案された認証プロトコルにおいて、チャレンジは、ＰＵＦの応答特性を系統的に学習しようとするモデル構築攻撃の困難さを高めるために、暗号ハッシュ関数を通されるのが通例である。

【００９１】

ハッシュは、ハッシュの出力が特定のＰＵＦ入力値に制御されるようにするにはｃ$_i$をどのように選択するか決定するのを困難にする。同様に、応答を難読化するために、応答のＸＯＲ難読化機能を追加することができる。これらの難読化機能は、「ｘを付けて消される」('x'ed)。何故なら、モデル構築ＨＥＬＰは、その入力および出力への直接アクセスによってでも、非常に困難であるからである。したがって、ＨＥＬＰを使用する本発明による認証プロトコルは、保護されていないインターフェースを有する。重い暗号ハッシュやＸＯＲネットワークを排除することにより、ハードウェア・トークン上における面積およびエネルギのオーバーヘッドを低減する。

【００９２】

認証は、ヘルパー・データ、ｈ$_i$、μ、ｒｎｇの送信方向を除いて、同様に実行される。尚、ＰＮＤｉｆｆが世界標準（これもエントロピを全体的なばらつきから排除する）に対してＴＶ補償されている場合、およびｒｎｇは不要であることは注意してしかるべきである。また、ヘルパー・データ処理は、リソースに制約があるトークン上でエネルギを節約するために、サーバ側で行われるとよい（トークンにそれを送信する必要がない）。最後に、トークンがビット反転エラーを起こさずにビットストリング再生を実行できる場合、「ファジー・マッチング」は不要でもよい。

【００９３】

先に示したように、マージンおよびＰＮＭｏｄパラメータは、ＨＥＬＰ　ＰＵＦのセキュリティ・プロパティを改善する。何故なら、これらはチャレンジ－応答空間を広げるからである。しかしながら、制約なしにこのパラメータを設定させることは、敵によって、モデル構築を補助するために使用される可能性がある。本発明は、ハード・コード化マージン、または小さい値の範囲、例えば、５および８の間だけを許すことによって、統計を改善しつつ、情報漏洩が限定されるチャネル(limited information leakage channel)を維持するという目標を達成することを示唆する。これはＰＮＭｏｄパラメータにも当てはまり、限られた１組の値だけを許容すべきである。例えば、２のべき乗に制限すると、ＣＲＰ空間の「限定された」拡張を行いつつ、モジュラス動作の実施が著しく簡略化する。

【００９４】

以上、本発明、およびその最良の態様であると現時点において考えられるものについて、本発明者によってその所有を確定し、当業者が本発明を実施および使用できるような方法で説明したが、本明細書において開示した例証的な実施形態には多くの均等物があること、そして例証的な実施形態によってではなく、添付した特許請求の範囲によって限定されるべき本発明の範囲および主旨から逸脱することなく、無数の変更および変形もそれらに対して行えることは、理解され認められよう。

【図１】

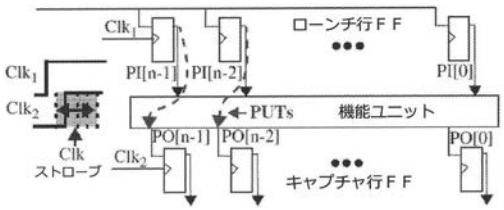

FIG. 1

【図２】

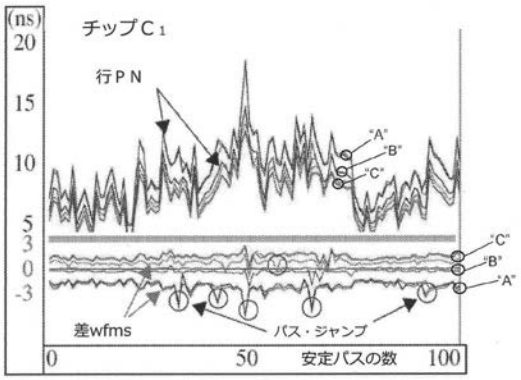

FIG. 2

【図３Ａ】

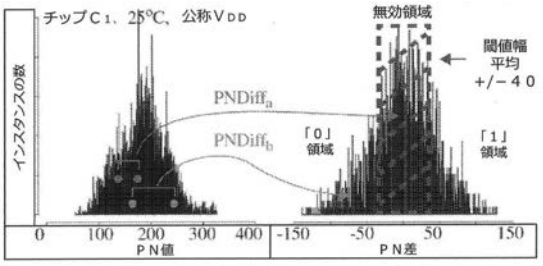

FIG. 3A FIG. 3B

【図３Ｂ】

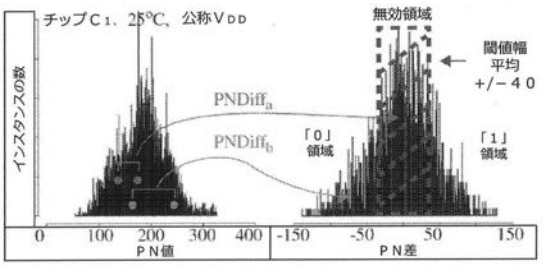

FIG. 3A FIG. 3B

【図４】

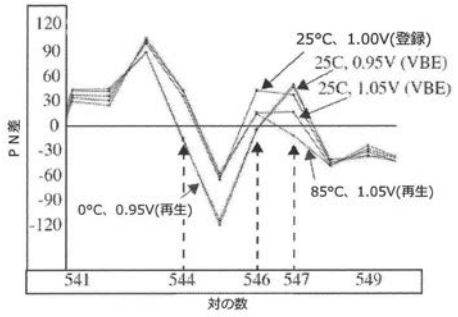

FIG. 4

【図５】

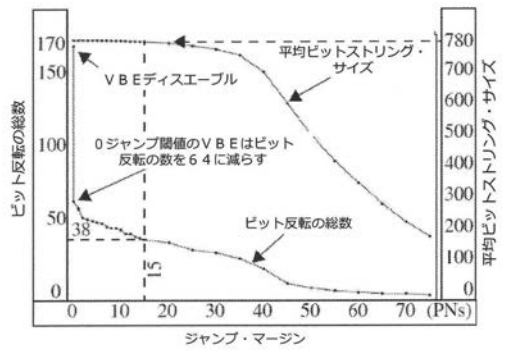

FIG. 5

【図６】

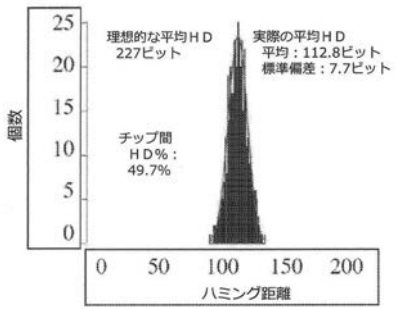

FIG. 6

【図７】

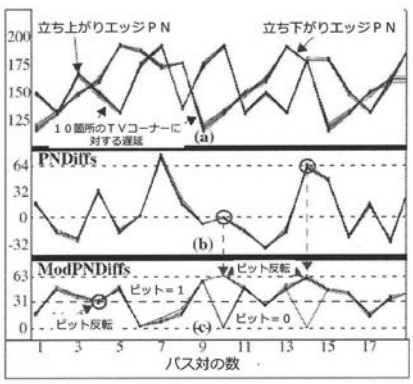

FIG. 7

【図８】

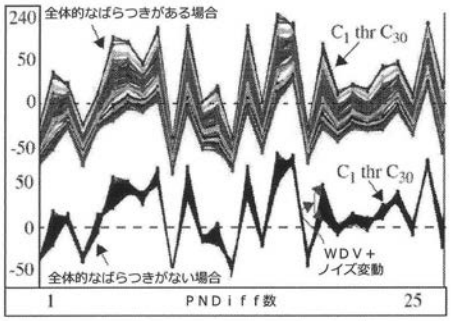

FIG. 8

【図９】

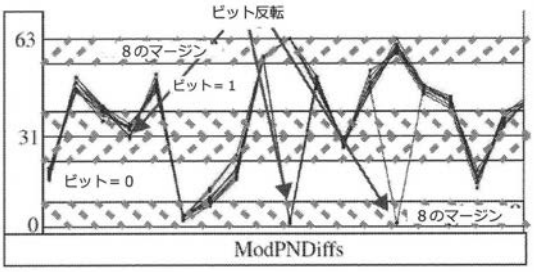

FIG. 9

【図１０Ａ】

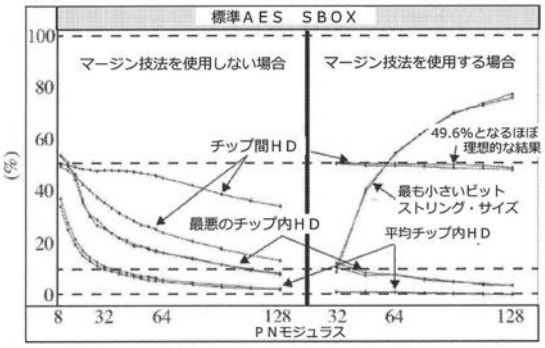

FIG. 10A FIG. 10B

【図１０Ｂ】

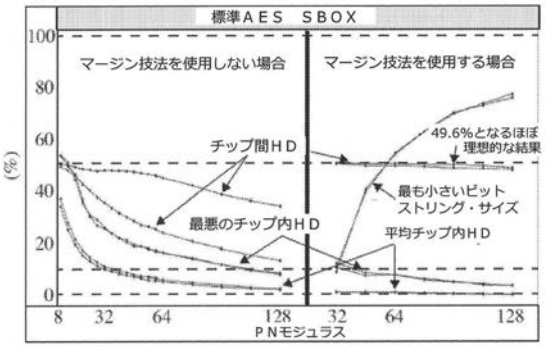

FIG. 10A FIG. 10B

【図１１Ａ】

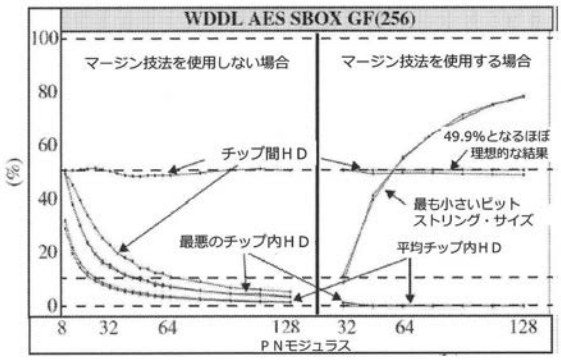

FIG. 11A FIG. 11B

【図１１Ｂ】

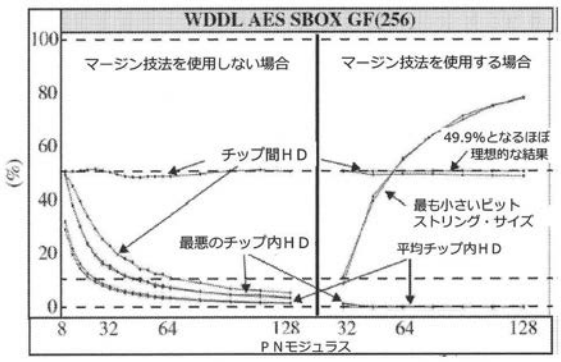

FIG. 11A FIG. 11B

【図１２】

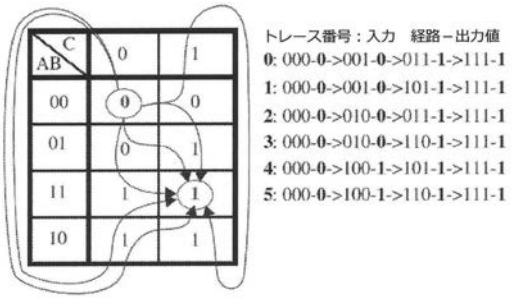

FIG. 12

【図１３】

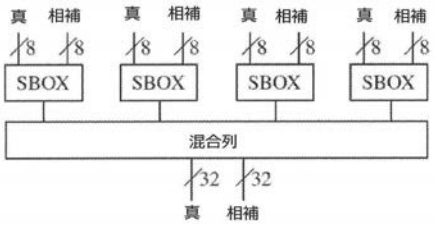

FIG. 13

【図１４】

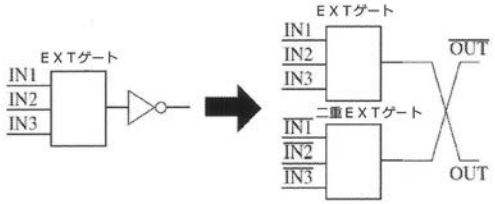

FIG. 14

【図１５】

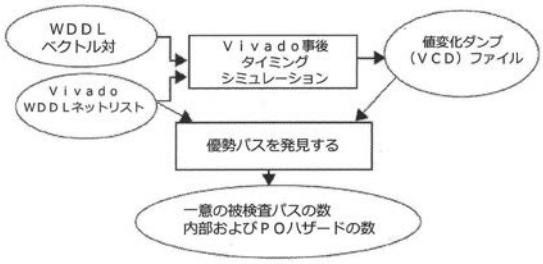

FIG. 15

【図１６】

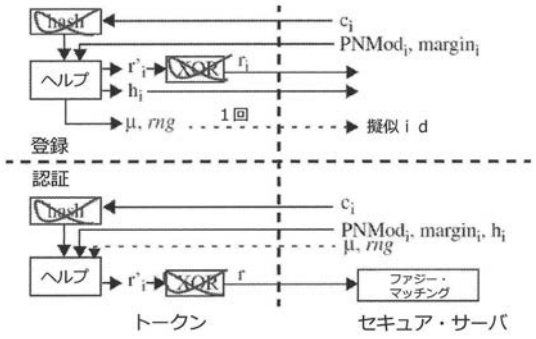

FIG. 16

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/065909

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/73(2013.01)i, G06F 21/70(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/73; G06F 1/26; G06F 21/72; G06F 21/70

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal), Google search engine & keywords: physically unclonable function, path delay, difference value, supply voltage regulator, bit flips, bitstring

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JAMES C. AARESTAD. `A hardware-embedded, delay-based PUF engine designed for use in cryptographic and authentication applications' July 2013, pp. 1-79. <URL : http://hdl.handle.net/1928/23304> See pages 30-73.	1-22
A	JIM AARESTAD et al. `HELP: A Hardware-Embedded Delay PUF' IEEE Design & Test, 29 May 2013, Volume 30, Issue 2, pp. 17-25. <URL : http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6461918> See pages 18-24.	1-22
A	JING JU et al. `Bit string analysis of Physical Unclonable Functions based on resistance variations in metals and transistors' In: 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, June 2012, pp. 13-20. <URL : http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6224312> See pages 15-20.	1-22
A	US 2014-0325237 A1 (INTRINSIC ID B.V.) 30 October 2014 See paragraphs [0201]-[0229]; and figures 3a-4.	1-22
A	US 2014-0201851 A1 (QUALCOMM INCORPORATED) 17 July 2014 See paragraphs [0035]-[0049]; and figures 2-4.	1-22

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 March 2016 (30.03.2016)	**01 April 2016 (01.04.2016)**

Name and mailing address of the ISA/KR	Authorized officer
International Application Division Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea	CHIN, Sang Bum
Facsimile No. +82-42-481-8578	Telephone No. +82-42-481-8398

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2015/065909

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0325237 A1	30/10/2014	CN 104521177 A	15/04/2015
		EP 2789116 A2	15/10/2014
		KR 10-2014-0099327 A	11/08/2014
		WO 2013-083415 A2	13/06/2013
		WO 2013-083415 A3	22/08/2013
US 2014-0201851 A1	17/07/2014	US 9015500 B2	21/04/2015
		WO 2014-113255 A1	24/07/2014

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(74)代理人 100118902
弁理士 山本 修
(74)代理人 100106208
弁理士 宮前 徹
(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100173565
弁理士 末松 亮太
(72)発明者 プラスクエリック，ジェームス
アメリカ合衆国ニューメキシコ州８７１２２，アルバカーキ，コロナド・アベニュー・ノースイースト ９６２１

Ｆターム(参考) 5J104 AA07 GA01 GA05 KA15