(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6169776号
(P6169776)

(45)発行日　平成29年7月26日(2017.7.26)　(24)登録日　平成29年7月7日(2017.7.7)

(51)Int.Cl.　F I
G06F 21/72 (2013.01)　G06F 21/72
G06F 1/04 (2006.01)　G06F 1/04 302

請求項の数 43　(全 15 頁)

(21)出願番号　特願2016-501029(P2016-501029)
(86)(22)出願日　平成26年3月10日(2014.3.10)
(65)公表番号　特表2016-514332(P2016-514332A)
(43)公表日　平成28年5月19日(2016.5.19)
(86)国際出願番号　PCT/US2014/022655
(87)国際公開番号　WO2014/164512
(87)国際公開日　平成26年10月9日(2014.10.9)
審査請求日　平成29年2月15日(2017.2.15)
(31)優先権主張番号　13/801,375
(32)優先日　平成25年3月13日(2013.3.13)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　クリス・ティリ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】クロック改竄を検出するための装置および方法

(57)【特許請求の範囲】

【請求項１】

クロック改竄を検出するための方法であって、

複数のリセット可能遅延線セグメントを設けるステップであって、最小遅延時間に関連付けられるリセット可能遅延線セグメントと最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる、設けるステップと、

クロックに関連付けられるクロック評価期間中に単調信号を与えるステップと、

それぞれが1または0の論理値のいずれかを有する個々の複数の遅延した単調信号を生成するために、前記複数のリセット可能遅延線セグメントのそれぞれを用いて前記単調信号を遅延させるステップと、

前記クロックを用いて、前記複数の遅延した単調信号を用いてクロック誤りを検出する評価回路をトリガするステップとを含む、クロック改竄を検出するための方法。

【請求項２】

リセット期間中に前記リセット可能遅延線セグメントをリセットするステップをさらに含み、前記リセット期間は前記クロック評価期間に先行する、請求項1に記載のクロック改竄を検出するための方法。

【請求項３】

前記クロックを用いて前記評価回路をトリガするステップは、前記クロック評価期間の最後のクロックエッジを用いて前記評価回路をトリガするステップを含む、請求項1に記

載のクロック改竄を検出するための方法。
【請求項４】
前記評価回路は、前記複数の遅延した単調信号内の1の数が、所定のしきい値より大きな値だけ水位数と異なるか否かを判断する、請求項1に記載のクロック改竄を検出するための方法。
【請求項５】
前記水位数は、1つまたは複数の先行するクロック評価期間からの遅延した単調信号に基づいて求められる、請求項4に記載のクロック改竄を検出するための方法。
【請求項６】
前記複数のリセット可能遅延線セグメントは遅延線に沿ってタップを備える、請求項1に記載のクロック改竄を検出するための方法。
【請求項７】
前記複数のリセット可能遅延線セグメントは並列遅延線を備える、請求項1に記載のクロック改竄を検出するための方法。
【請求項８】
クロック改竄を検出するための装置であって、
クロックに関連付けられるクロック評価期間中に単調信号を与えるための手段と、
最小遅延時間と最大遅延時間との間に離散的に増加する遅延時間を有する複数の遅延した単調信号を生成するために、前記単調信号を遅延させるための手段であって、前記複数の遅延した単調信号のそれぞれが、1または0の論理値のいずれかを有する、手段と、
前記複数の遅延した単調信号を用いてクロック誤りを検出する、評価するための手段と、
評価するための前記手段をトリガするための手段とを備える、クロック改竄を検出するための装置。
【請求項９】
リセット期間中に前記単調信号を遅延させるための前記手段をリセットするための手段をさらに備え、前記リセット期間は前記クロック評価期間に先行する、請求項8に記載のクロック改竄を検出するための装置。
【請求項１０】
評価するための前記手段をトリガするための前記手段は、前記クロック評価期間の最後のクロックエッジを用いて評価するための前記手段をトリガする、請求項8に記載のクロック改竄を検出するための装置。
【請求項１１】
評価するための前記手段は、前記複数の遅延した単調信号内の1の数が、所定のしきい値より大きな値だけ水位数と異なるか否かを判断する、請求項8に記載のクロック改竄を検出するための装置。
【請求項１２】
前記水位数は、1つまたは複数の先行するクロック評価期間からの遅延した単調信号に基づいて求められる、請求項11に記載のクロック改竄を検出するための装置。
【請求項１３】
前記単調信号を遅延させるための前記手段は遅延線に沿ったタップを含む、請求項8に記載のクロック改竄を検出するための装置。
【請求項１４】
前記単調信号を遅延させるための前記手段は並列遅延線を含む、請求項8に記載のクロック改竄を検出するための装置。
【請求項１５】
クロック改竄を検出するための装置であって、
クロックに関連付けられるクロック評価期間中に単調信号を与える回路と、
それぞれが1または0の論理値のいずれかを有する個々の複数の遅延した単調信号を生成するために前記単調信号を遅延させる複数のリセット可能遅延線セグメントであって、最

小遅延時間に関連付けられるリセット可能遅延線セグメントと最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる、複数のリセット可能遅延線セグメントと、
前記クロックによってトリガされ、前記複数の遅延した単調信号を用いてクロック誤りを検出する評価回路とを備える、クロック改竄を検出するための装置。
【請求項１６】
前記リセット可能遅延線セグメントはリセット期間中にリセットされ、前記リセット期間は前記クロック評価期間に先行する、請求項15に記載のクロック改竄を検出するための装置。
【請求項１７】
前記評価回路は、前記クロック評価期間の最後のクロックエッジによってトリガされる、請求項15に記載のクロック改竄を検出するための装置。
【請求項１８】
前記評価回路は、前記複数の遅延した単調信号内の1の数が、所定のしきい値より大きい値だけ水位数と異なるか否かを判断してクロック誤りを検出する、請求項15に記載のクロック改竄を検出するための装置。
【請求項１９】
前記水位数は、1つまたは複数の先行するクロック評価期間からの遅延した単調信号に基づいて求められる、請求項18に記載のクロック改竄を検出するための装置。
【請求項２０】
前記複数のリセット可能遅延線セグメントは遅延線に沿ってタップを備える、請求項15に記載のクロック改竄を検出するための装置。
【請求項２１】
前記複数のリセット可能遅延線セグメントは並列遅延線を備える、請求項15に記載のクロック改竄を検出するための装置。
【請求項２２】
クロック改竄を検出するための装置であって、
クロックに関連付けられる第1のクロック評価期間中に第1の単調信号を与える第1の回路と、
個々の第1の複数の遅延した単調信号を生成するためにそれぞれが前記第1の単調信号を遅延させる、第1の複数のリセット可能遅延線セグメントであって、最小遅延時間に関連付けられるリセット可能遅延線セグメントと最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる、第1の複数のリセット可能遅延線セグメントと、
前記クロックに関連付けられる第2のクロック評価期間中に第2の単調信号を与える第2の回路であって、前記第2のクロック評価期間は前記第1のクロック評価期間とは異なる時間をカバーする、第2の回路と、
個々の第2の複数の遅延した単調信号を生成するためにそれぞれが前記第2の単調信号を遅延させる、第2の複数のリセット可能遅延線セグメントであって、最小遅延時間に関連付けられるリセット可能遅延線セグメントと最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる、第2の複数のリセット可能遅延線セグメントと、
前記クロックによってトリガされ、前記第1の複数の遅延した単調信号または前記第2の複数の遅延した単調信号を用いてクロック誤りを検出する評価回路とを備える、クロック改竄を検出するための装置。
【請求項２３】
電圧改竄を検出するための方法であって、
複数のリセット可能遅延線セグメントを設けるステップであって、最小遅延時間に関連付けられるリセット可能遅延線セグメントと最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する

遅延時間に関連付けられる、設けるステップと、
評価期間中に単調信号を与えるステップと、
それぞれが1または0の論理値のいずれかを有する個々の複数の遅延した単調信号を生成するために、前記複数のリセット可能遅延線セグメントをそれぞれ用いて、前記単調信号を遅延させるステップと、
クロックを用いて、前記複数の遅延した単調信号を用いて電圧異常を検出する評価回路をトリガするステップとを含む、電圧改竄を検出するための方法。
【請求項２４】
リセット期間中に前記リセット可能遅延線セグメントをリセットするステップをさらに含み、前記リセット期間は前記評価期間に先行する、請求項23に記載の電圧改竄を検出するための方法。
【請求項２５】
前記クロックを用いて前記評価回路をトリガするステップは、前記評価期間の最後のクロックエッジを用いて前記評価回路をトリガするステップを含む、請求項23に記載の電圧改竄を検出するための方法。
【請求項２６】
前記評価回路は、前記複数の遅延した単調信号内の1の数が、所定のしきい値より大きな値だけ水位数と異なるか否かを判断する、請求項23に記載の電圧改竄を検出するための方法。
【請求項２７】
前記水位数は、1つまたは複数の先行する評価期間からの遅延した単調信号に基づいて求められる、請求項26に記載の電圧改竄を検出するための方法。
【請求項２８】
前記複数のリセット可能遅延線セグメントは遅延線に沿ってタップを備える、請求項23に記載の電圧改竄を検出するための方法。
【請求項２９】
前記複数のリセット可能遅延線セグメントは並列遅延線を備える、請求項23に記載の電圧改竄を検出するための方法。
【請求項３０】
電圧改竄を検出するための装置であって、
評価期間中に定常状態の単調信号を与えるための手段と、
最小遅延時間と最大遅延時間との間に離散的に増加する遅延時間を有する複数の遅延した単調信号を生成するために、前記単調信号を遅延させるための手段であって、前記複数の遅延した単調信号のそれぞれが、1または0の論理値のいずれかを有する、手段と、
前記複数の遅延した単調信号を用いて電圧異常を検出する、評価するための手段と、
評価するための前記手段をトリガするための手段とを備える、電圧改竄を検出するための装置。
【請求項３１】
リセット期間中に前記単調信号を遅延させるための前記手段をリセットするための手段をさらに備え、前記リセット期間は前記評価期間に先行する、請求項30に記載の電圧改竄を検出するための装置。
【請求項３２】
評価するための前記手段をトリガするための前記手段は、前記評価期間の最後のクロックエッジを用いて評価するための前記手段をトリガする、請求項30に記載の電圧改竄を検出するための装置。
【請求項３３】
評価するための前記手段は、前記複数の遅延した単調信号内の1の数が、所定のしきい値より大きな値だけ水位数と異なるか否かを判断する、請求項30に記載の電圧改竄を検出するための装置。
【請求項３４】

前記水位数は、1つまたは複数の先行する評価期間からの遅延した単調信号に基づいて求められる、請求項33に記載の電圧改竄を検出するための装置。

【請求項３５】

前記単調信号を遅延させるための前記手段は遅延線に沿ったタップを含む、請求項30に記載の電圧改竄を検出するための装置。

【請求項３６】

前記単調信号を遅延させるための前記手段は並列遅延線を含む、請求項30に記載の電圧改竄を検出するための装置。

【請求項３７】

電圧改竄を検出するための装置であって、

評価期間中に単調信号を与える回路と、

それぞれが1または0の論理値のいずれかを有する個々の複数の遅延した単調信号を生成するために前記単調信号を遅延させる複数のリセット可能遅延線セグメントであって、最小遅延時間に関連付けられるリセット可能遅延線セグメントと最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる、複数のリセット可能遅延線セグメントと、

クロックによってトリガされ、前記複数の遅延した単調信号を用いて電圧異常を検出する評価回路とを備える、電圧改竄を検出するための装置。

【請求項３８】

前記リセット可能遅延線セグメントがリセット期間中にリセットされ、前記リセット期間は前記評価期間に先行する、請求項37に記載の電圧改竄を検出するための装置。

【請求項３９】

前記評価回路は、前記評価期間の最後のクロックエッジを用いてトリガされる、請求項37に記載の電圧改竄を検出するための装置。

【請求項４０】

前記評価回路は、前記複数の遅延した単調信号内の1の数が、所定のしきい値より大きい値だけ水位数と異なるか否かを判断して前記電圧異常を検出する、請求項37に記載の電圧改竄を検出するための装置。

【請求項４１】

前記水位数は、1つまたは複数の先行する評価期間からの遅延した単調信号に基づいて求められる、請求項40に記載の電圧改竄を検出するための装置。

【請求項４２】

前記複数のリセット可能遅延線セグメントは遅延線に沿ってタップを備える、請求項37に記載の電圧改竄を検出するための装置。

【請求項４３】

前記複数のリセット可能遅延線セグメントは並列遅延線を備える、請求項37に記載の電圧改竄を検出するための装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は一般に、プロセッサのクロックおよび/または供給電圧の改竄を検出することに関する。

【背景技術】

【０００２】

計算システムの暗号計算は、クロックおよび/または電源電圧に一時的なスパイク(またはグリッチ)を引き起こし、計算結果に誤りを差し込むことによって攻撃されることがある。また、攻撃は、不完全な計算による誤った値が計算システムのレジスタ内にサンプリングされるほど計算時間を十分に短縮するようにクロック周波数を高めることがある。さらに、攻撃は、システムをより容易に攻撃するために計算システムのバスを低速にすることがある。

【０００３】
それゆえ、効率的で、費用対効果があるようにプロセッサのクロックおよび/または供給電圧の改竄を検出するための技法が必要とされている。
【発明の概要】
【課題を解決するための手段】
【０００４】
本発明の一態様は、クロック改竄を検出するための方法に属することができる。その方法では、複数のリセット可能遅延線セグメントが設けられる。最小遅延時間に関連付けられるリセット可能遅延線セグメントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。クロックに関連付けられるクロック評価期間中に単調信号が与えられる。複数のリセット可能遅延線セグメントのそれぞれを用いて、単調信号を遅延させて、個々の複数の遅延した単調信号を生成する。クロックを用いて、複数の遅延した単調信号を用いてクロック誤りを検出する評価回路をトリガする。
【０００５】
本発明のさらに詳細な態様では、その方法はさらに、リセット期間中にリセット可能遅延線セグメントをリセットすることを含むことができる。リセット期間はクロック評価期間に先行することができる。クロックを用いて評価回路をトリガすることは、クロック評価期間の最後のクロックエッジを用いて、評価回路をトリガすることを含むことができる。
【０００６】
本発明の他のさらに詳細な態様では、複数の遅延した単調信号のそれぞれは1または0のいずれかとすることができる。評価回路は、複数の遅延した単調信号内の1の数が、所定のしきい値より大きい値だけ水位数と異なるか否かを判断することができる。水位数は、1つまたは複数の先行するクロック評価期間からの遅延した単調信号に基づいて求めることができる。複数のリセット可能遅延線セグメントは、遅延線に沿ってタップを備えることができる。代替的には、複数のリセット可能遅延線セグメントは並列遅延線を備える。
【０００７】
本発明の別の態様は、クロック改竄を検出するための装置に属することができ、その装置は、クロックに関連付けられるクロック評価期間中に単調信号を与えるための手段と、最小遅延時間と最大遅延時間との間に離散的に増加する遅延時間を有する個々の複数の遅延した単調信号を生成するために、複数のリセット可能遅延線セグメントを用いて単調信号を遅延させるための手段と、クロックを用いて、複数の遅延した単調信号を用いてクロック誤りを検出する評価回路をトリガするための手段とを備える。
【０００８】
本発明の別の態様は、クロック改竄を検出するための装置に属することができ、その装置は、単調信号を与える回路と、複数のリセット可能遅延線セグメントと、評価回路とを備える。その回路は、クロックに関連付けられるクロック評価期間中に単調信号を与える。複数のリセット可能遅延線セグメントは、単調信号を遅延させて、個々の複数の遅延した単調信号を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価回路はクロックによってトリガされ、複数の遅延した単調信号を用いてクロック誤りを検出する。
【０００９】
本発明の別の態様は、クロック改竄を検出するための装置に属することができ、その装置は、第1の回路と、第1の複数のリセット可能遅延線セグメントと、第2の回路と、第2の複数のリセット可能遅延線セグメントと、評価回路とを備える。第1の回路は、クロックに関連付けられる第1のクロック評価期間中に第1の単調信号を与える。第1の複数のリセット可能遅延線セグメントはそれぞれ、第1の単調信号を遅延させて、個々の第1の複数の遅延した単調信号を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメ

ントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。第2の回路は、そのクロックに関連付けられる第2のクロック評価期間中に第2の単調信号を与える。第2のクロック評価期間は、第1のクロック評価期間とは異なる時間をカバーする。第2の複数のリセット可能遅延線セグメントはそれぞれ第1の単調信号を遅延させて、個々の第2の複数の遅延した単調信号を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価回路はクロックによってトリガされ、第1の複数の遅延した単調信号または第2の複数の遅延した単調信号を用いて、クロック誤りを検出する。

【００１０】

本発明の一態様は、電圧改竄を検出するための方法に属することができる。その方法では、複数のリセット可能遅延線セグメントが設けられる。最小遅延時間に関連付けられるリセット可能遅延線セグメントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価期間中に単調信号が与えられる。複数のリセット可能遅延線セグメントのそれぞれを用いて、単調信号を遅延させて、個々の複数の遅延した単調信号を生成する。クロックを用いて、複数の遅延した単調信号を用いて電圧異常を検出する評価回路をトリガする。

【００１１】

本発明のさらに詳細な態様では、その方法はさらに、リセット期間中にリセット可能遅延線セグメントをリセットすることを含むことができる。リセット期間は評価期間に先行することができる。クロックを用いて評価回路をトリガすることは、評価期間の最後のクロックエッジを用いて、評価回路をトリガすることができる。

【００１２】

本発明の他のさらに詳細な態様では、複数の遅延した単調信号のそれぞれは1または0のいずれかを含む。評価回路は、複数の遅延した単調信号内の1の数が、所定のしきい値より大きい値だけ水位数と異なるか否かを判断することができる。水位数は、1つまたは複数の先行するクロック評価期間からの遅延した単調信号に基づいて求めることができる。複数のリセット可能遅延線セグメントは、遅延線に沿ってタップを備えることができる。代替的には、複数のリセット可能遅延線セグメントは並列遅延線を備える。

【００１３】

本発明の別の態様は、電圧改竄を検出するための装置に属することができ、その装置は、評価期間中に単調信号を与えるための手段と、最小遅延時間と最大遅延時間との間に離散的に増加する遅延時間を有する個々の複数の遅延した単調信号を生成するために、複数のリセット可能遅延線セグメントを用いて単調信号を遅延させるための手段と、クロックを用いて、複数の遅延した単調信号を用いて電圧異常を検出する評価回路をトリガするための手段とを備える。

【００１４】

本発明の別の態様は電圧改竄を検出するための装置に属することができ、その装置は、単調信号を与える回路と、複数のリセット可能遅延線セグメントと、評価回路とを備える。その回路は、評価期間中に単調信号を与える。複数のリセット可能遅延線セグメントは、単調信号を遅延させて、個々の複数の遅延した単調信号を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価回路がクロックによってトリガされ、複数の遅延した単調信号を用いて、電圧異常を検出する。

【図面の簡単な説明】

【００１５】

【図１】本発明による、クロック改竄を検出するための方法の流れ図である。

【図２】クロック改竄または電圧改竄を検出するための装置のブロック図である。
【図３】クロック信号およびリセット信号の概略図である。
【図４】並列の遅延線セグメントの概略図である。
【図５】直列の遅延線セグメントの概略図である。
【図６】評価回路内の検出回路の概略図である。
【図７】一様でないデューティサイクルを有するクロックを検出するためのデュアル遅延線を有する回路の概略図である。
【図８】本発明による、電圧改竄を検出するための方法の流れ図である。
【発明を実施するための形態】
【００１６】
「例示的」という言葉は、例、事例、または例示としての役割を果たすことを意味するように本明細書で使用される。「例示的」として本明細書で説明される任意の実施形態は、必ずしも他の実施形態よりも好ましいか、または有利であると解釈されるべきではない。
【００１７】
図1、図2および図3を参照すると、本発明の一態様は、クロック改竄を検出するための方法100に属することができる。その方法では、複数のリセット可能遅延線セグメント210が設けられる(ステップ110)。最小遅延時間に関連付けられるリセット可能遅延線セグメント210-1と最大遅延時間に関連付けられるリセット可能遅延線セグメント210-Nとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。クロックCLKに関連付けられるクロック評価期間310中に単調信号220が与えられる(ステップ120)。複数のリセット可能遅延線セグメントのそれぞれを用いて、単調信号を遅延させて、個々の複数の遅延した単調信号230を生成する(ステップ130)。クロックを用いて、複数の遅延した単調信号を用いてクロック誤りを検出する評価回路240をトリガする(ステップ140)。
【００１８】
本発明のより詳細な態様では、方法100はさらに、リセット期間320中にリセット信号RSTを用いてリセット可能遅延線セグメント210をリセットすることを含む。リセット期間は、クロック評価期間310に先行することができる。クロックCLKを用いて評価回路240をトリガすることは、クロック評価期間の最後のクロックエッジを用いて、評価回路をトリガすることができる。
【００１９】
本発明の他のさらに詳細な態様では、複数の遅延した単調信号230のそれぞれが1または0のいずれかとすることができる。評価回路240は、複数の遅延した単調信号内の1の数が、所定のしきい値より大きい値だけ水位数と異なるか否かを判断することができる。水位数は、1つまたは複数の先行するクロック評価期間310からの遅延した単調信号に基づいて求めることができる。
【００２０】
図4を参照すると、複数のリセット可能遅延線セグメント210は、セグメント化された並列の遅延線を備えることができる。1つの遅延線セグメントは、最小の遅延した単調信号を生成する1つの遅延素子だけを有し得る。別の遅延線セグメントは、最大の遅延した単調信号230-Nを生成するN個の遅延素子を有し得る。遅延線内のANDゲートはそれぞれ、遅延素子間の線をリセットして遅延線を初期の既知の状態に設定するリセット入力RSTを有することができる。
【００２１】
図5を参照すると、複数のリセット可能遅延線セグメント210は遅延線に沿ってタップを備えることができる。セグメント化された遅延線は、線に沿って複数のタップを有し、個々の遅延した単調信号230を生成することができる。評価信号EVALが、遅延線間のANDゲートを用いて線セグメントをリセットすることができる。評価信号は、クロック信号CLK、たとえば、クロック信号の半分から形成することができる。

【００２２】
図6を参照すると、評価回路は、それぞれが1つのフリップフロップまたは一対のフリップフロップを有する検出回路を用いて、クロックに応答して、リセット可能遅延線セグメントごとに個々の遅延した単調信号230-Nをラッチすることができる。
【００２３】
単調な0から1への遷移は、リセット演算子を導入することによって達成することができる。各リセット演算子は、リセット段階中に検知回路の個々の遅延線を、任意の設定違反から独立して既知の状態にリセットすることができ、一方、検知回路は評価段階中に検知する。リセット演算子を用いない場合、予想より低い周波数を検出する検知回路は、未知の状態であることがある。リセット演算子を実現する幾つかの方法がある。図4および図5に示されるように、遅延線にANDゲートが挿入されてもよい。ANDゲートの一方の入力が、単調な0から1への信号によって駆動されてよく、他方の入力が、否定リセット信号によって駆動され得る。各ANDゲートによって、評価期間中に単調な0から1への信号を伝搬させながら、リセット期間内に遅延線のその部分をリセットできるようになる。
【００２４】
本発明の技法は、予想より速いクロック周波数、および予想より遅いクロック周波数を検出することができる。また、単調信号の設定時間違反を検出して、予想より速い周波数またはグリッチを検知することもできる。適応的環境不感センサを設けるために、設定時間違反の数の著しい変化を検出することができる。温度のような通常の環境変化に起因するわずかな違いは、所定の検出しきい値の範囲内にある。改竄(周波数および/または電圧)に起因する違反の大きな違いは、所定の検出しきい値から外れることになる。
【００２５】
最も長い伝搬遅延を有する回路がトリガされるとき、クロック不在条件が検出され得る。直ちに応答するために非同期回路によってこのトリガが用いられるか、または後にクロックが戻ったときにシステムが応答するために、状態ビットを設定することができる。
【００２６】
非常に高い定常状態の周波数検出は、最も短い遅延線のリセット演算子間の遅延によって決まる。この遅延線をリセットするのに要する時間が短いほど、遅延線をリセットするために実際に割り当てられる時間を短くすることができる。他の検知回路のリセット演算子間の遅延はそれほど厳密でなくてもよく、最も高い許容な動作周波数によって決定することができる。
【００２７】
幾つかの技法を用いて、変化する設定違反の数が著しいか否かを検出することができる。1つの方法は、各検出回路の状態とその回路の先行する状態とのXOR演算を実行し、「1」の数をしきい値と比較することである。別の方法は、STA(静的タイミング解析)を用いて、または較正段階中に、予想される周波数に対応する特定の検出回路を決定することである。この特定の回路は水位としての役割を果たす。短い遅延線に関連付けられる回路ほど、「0」を測定することになり、長い遅延線に関連付けられる回路ほど、「1」を測定することになる。高水位マークおよび低水位マークがトリガとしての役割を果たすことができる。
【００２８】
幾つかの変形を容易に実施できることに留意されたい。一例として、検出/検知回路は、単調な1から0への遷移に依存することができ、その回路は1にリセットすることができる。別の例として、その回路は単調な1から0の遷移および0から1への遷移をインターリーブすることができる。別の例として、リセット演算子はMUXを用いて実現することができ、リセット信号に基づいて、MUXは単調信号とリセット値とのいずれかを選択する。別の例として、バッファ、インバータ対または単調信号遷移を保証する任意の回路から、遅延線を構成することができる。別の例として、クロック不在検出を省くことができる。別の例として、リセット段階の最後に「高速」線(または任意の他の線)をサンプリングして、その回路が完全にリセットされたことを確認することができる。別の例として、検出回路

は、一方が高水位線、もう一方が低水位線である2つの遅延線セグメントのみを有するように縮小することができる。

【００２９】

本発明の別の態様は、クロック改竄を検出するための装置に属することができ、その装置は、クロックCLKに関連付けられるクロック評価期間310中に単調信号220を与えるための手段250と、最小遅延時間と最大遅延時間との間に離散的に増加する遅延時間を有する個々の複数の遅延した単調信号230を生成するために、複数のリセット可能遅延線セグメントを用いて単調信号を遅延させるための手段210と、クロックCLKを用いて、複数の遅延した単調信号を用いてクロック誤りを検出する評価回路240をトリガするための手段240とを備える。

【００３０】

本発明の別の態様は、クロック改竄を検出するための装置に属することができ、その装置は、単調信号220を与える回路250と、複数のリセット可能遅延線セグメント210と、評価回路240とを備える。回路250は、クロックCLKに関連付けられるクロック評価期間310中に単調信号を与える。複数のリセット可能遅延線セグメントは、単調信号を遅延させて、個々の複数の遅延した単調信号230を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメント210-1と最大遅延時間に関連付けられるリセット可能遅延線セグメント210-Nとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価回路240はクロックCLKによってトリガされ、複数の遅延した単調信号を用いてクロック誤りを検出する。

【００３１】

一様でないデューティサイクルを有するクロック信号を、一方がクロック信号によって駆動され、もう一方が否定クロック信号(negated clock signal)によって駆動されるデュアル回路を用いることによって検出することができる。デュアル回路を用いない場合、リセット期間を長くするが、評価期間を一定に保持することによって、周波数を検出できないほど下げることができる。デュアル回路手法によれば、一方の回路が、この長い時間間隔中に評価段階にあるのを保証される。

【００３２】

図7をさらに参照すると、本発明の別の態様は、クロック改竄を検出するための装置に属することができ、その装置は、第1の回路750Aと、第1の複数のリセット可能遅延線セグメント710と、第2の回路750Bと、第2の複数のリセット可能遅延線セグメント720と、評価回路240とを備える。第1の回路は、クロックに関連付けられる第1のクロック評価期間中に第1の単調信号を与える。第1の複数のリセット可能遅延線セグメントはそれぞれ、第1の単調信号を遅延させて、個々の第1の複数の遅延した単調信号を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。第2の回路は、そのクロックに関連付けられる第2のクロック評価期間中に第2の単調信号を与える。インバータ730によって強制されることがあるように、第2のクロック評価期間は、第1のクロック評価期間とは異なる時間をカバーする。第2の複数のリセット可能遅延線セグメントはそれぞれ第1の単調信号を遅延させて、個々の第2の複数の遅延した単調信号を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメントと、最大遅延時間に関連付けられるリセット可能遅延線セグメントとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価回路はクロック(たとえば、EVAL)によってトリガされ、第1の複数の遅延した単調信号または第2の複数の遅延した単調信号を用いて、クロック誤りを検出する。マルチプレクサ760が、評価回路に与えられるために、第1の複数の遅延した単調信号または第2の複数の遅延した単調信号のいずれがアクティブであるかを選択することができる。

【００３３】

本発明の技法は、スタティックCMOSを用いる組合せロジックに基づいて実現することが

でき、それはプロセッサの既存の回路集積に基づいて相対的にコスト効率が良い。遅延線の数と、マルチ周波数プランサポートとを適応させることによって、遅延線のプロセス変化、電圧変化および温度変化の検出補償を達成することができる。誤り攻撃において用いられる電圧スパイクも検出することができる。これらの電圧スパイクは電圧を低下させ、回路の動作を遅くし、結果として、不完全な計算がレジスタ内にサンプリングされることがある。代替的には、電圧の増加が回路の動作を速くし、結果として、予想外の計算または結果がレジスタ内にサンプリングされることがある。

【００３４】

図2、図3および図8を参照すると、本発明の別の態様は、電圧改竄を検出するための方法800に属することができる。その方法では、複数のリセット可能遅延線セグメント210が設けられる(ステップ810)。最小遅延時間に関連付けられるリセット可能遅延線セグメント210-1と最大遅延時間に関連付けられるリセット可能遅延線セグメント210-Nとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価期間310中に単調信号220が与えられる(ステップ820)。複数のリセット可能遅延線セグメントのそれぞれを用いて、単調信号を遅延させて、個々の複数の遅延した単調信号230を生成する(ステップ830)。クロックを用いて、複数の遅延した単調信号を用いて電圧異常を検出する評価回路240をトリガする(ステップ840)。

【００３５】

本発明のより詳細な態様では、方法800はさらに、リセット期間320中にリセット信号RSTを用いてリセット可能遅延線セグメント210をリセットすることを含む。リセット期間は評価期間310に先行することができる。クロックCLKを用いて評価回路220をトリガすることは、評価期間の最後のクロックエッジを用いて、評価回路をトリガすることができる。

【００３６】

本発明の他のさらに詳細な態様では、複数の遅延した単調信号230はそれぞれ、1または0のいずれかを含むことができる。評価回路240は、複数の遅延した単調信号内の1の数が、所定のしきい値より大きい値だけ水位数と異なるか否かを判断することができる。水位数は、1つまたは複数の先行するクロック評価期間310からの遅延した単調信号に基づいて求めることができる。複数のリセット可能遅延線セグメントは、遅延線に沿ってタップを備えることができる。代替的には、複数のリセット可能遅延線セグメントは並列遅延線を備える。

【００３７】

本発明の別の態様は、電圧改竄を検出するための装置に属することができ、その装置は、評価期間310中に単調信号220を与えるための手段250と、最小遅延時間と最大遅延時間との間に離散的に増加する遅延時間を有する個々の複数の遅延した単調信号230を生成するために複数のリセット可能遅延線セグメントを用いて単調信号を遅延させるための手段210と、クロックを用いて、複数の遅延した単調信号を用いて電圧異常を検出する評価回路240をトリガするための手段240とを備える。

【００３８】

本発明の別の態様は、電圧改竄を検出するための装置に属することができ、その装置は、単調信号220を与える回路250と、複数のリセット可能遅延線セグメント210と、評価回路240とを備える。回路250は、評価期間310中に単調信号を与える。複数のリセット可能遅延線セグメントは、単調信号を遅延させて、個々の複数の遅延した単調信号230を生成する。最小遅延時間に関連付けられるリセット可能遅延線セグメント210-1と最大遅延時間に関連付けられるリセット可能遅延線セグメント210-Nとの間のリセット可能遅延線セグメントはそれぞれ、離散的に増加する遅延時間に関連付けられる。評価回路240はクロックCLKによってトリガされ、複数の遅延した単調信号を用いて電圧異常を検出する。

【００３９】

上記の説明を通して開示される回路は、デスクトップコンピュータもしくはラップトップコンピュータ、タブレット、モバイルデバイス、セルラー電話などのコンピューティングシステムに含まれ得る。当業者は、本明細書で開示される実施形態に関連して説明され

る様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップが、電子ハードウェアとして、またはハードウェアとコンピュータソフトウェアとの組合せとして実現され得ることはさらに理解されよう。そのような機能がハードウェアとして実現されるか、またはソフトウェアとして実現されるかは、具体的な適用例およびシステム全体に課される設計制約によって決まる。当業者は、説明された機能を具体的な適用例ごとに様々な方法で実現することができるが、そのような実現の決定は、本発明の範囲からの逸脱を生じるものと解釈されるべきではない。

【００４０】

本明細書に開示される実施形態に関連して説明される様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタルシグナルプロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別のゲートもしくはトランジスタロジック、個別のハードウェア構成要素、または本明細書に説明される機能を実行するように設計されるそれらの任意の組合せと統合され得る。汎用プロセッサはマイクロプロセッサとすることができるが、代替形態では、プロセッサは任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることができる。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPおよびマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実現することもできる。

【００４１】

本明細書で開示される実施形態に関連して説明される方法またはアルゴリズムのステップは、直接ハードウェアで具現されるか、ハードウェアと、プロセッサによって実行されるソフトウェアモジュールとの組合せで具現され得る。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体内に存在することができる。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、かつ記憶媒体に情報を書き込むことができるようにプロセッサに結合される。代替形態では、記憶媒体は、プロセッサと一体にすることができる。プロセッサおよび記憶媒体はASIC内に存在することができる。そのASICはユーザ端末内に存在することができる。代替形態では、プロセッサおよび記憶媒体は、コンピューティングシステム/ユーザ端末内に個別の構成要素として存在することができる。

【００４２】

開示された実施形態の上記の説明は、任意の当業者が本発明を作製または使用することを可能にするために提供される。これらの実施形態への様々な修正が当業者には容易に明らかになり、本明細書において規定された一般原理は、本発明の趣旨または範囲を逸脱することなく他の実施形態に適用することができる。したがって、本発明は、本明細書に示される実施形態に限定されるのではなく、本明細書において開示される原理および新規の特徴に矛盾しない最も広い範囲を与えられるべきである。

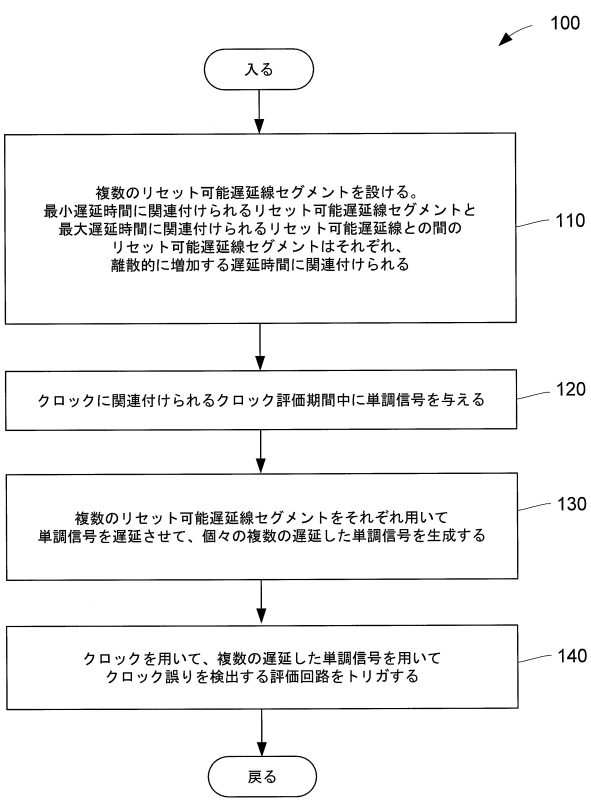
【符号の説明】

【００４３】

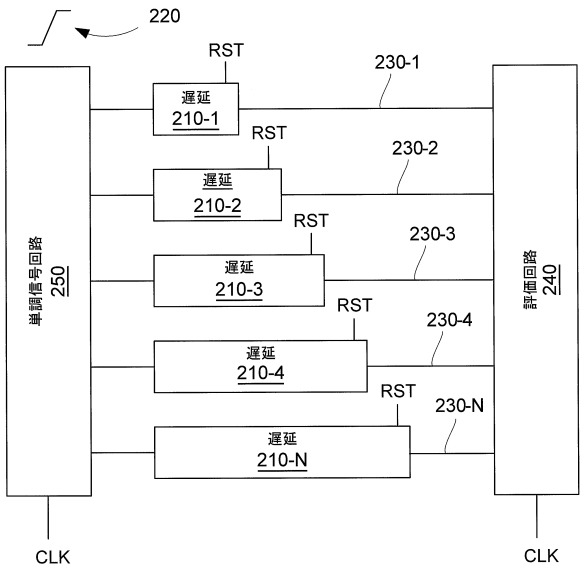
100　方法
210　リセット可能遅延線セグメント
210　遅延させるための手段
210-1　リセット可能遅延線セグメント
210-N　リセット可能遅延線セグメント
220　単調信号
230　単調信号
230-N　単調信号
240　評価回路
240　トリガするための手段

250　回路
250　与えるための手段
310　クロック評価期間
320　リセット期間
710　第1の複数のリセット可能遅延線セグメント
720　第2の複数のリセット可能遅延線セグメント
730　インバータ
750A　第1の回路
750B　第2の回路
760　マルチプレクサ
800　方法

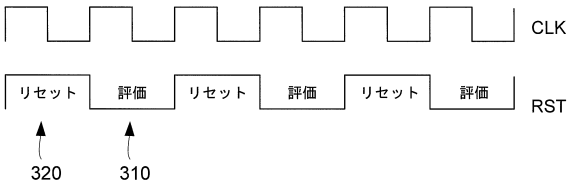
【図１】



【図２】



【図３】



【図４】

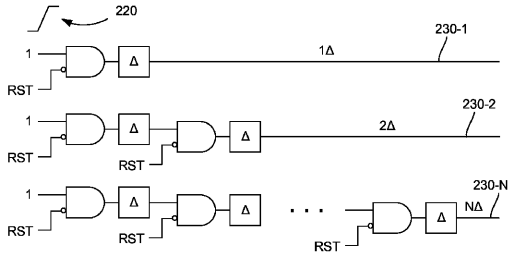


FIG. 4

【図５】

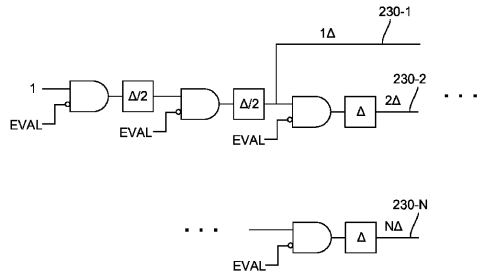


FIG. 5

【図６】

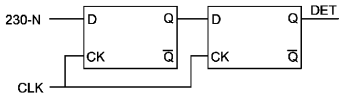


FIG. 6

【図７】

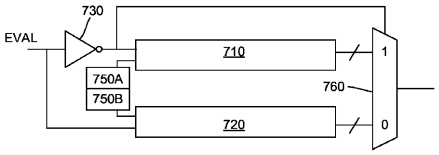
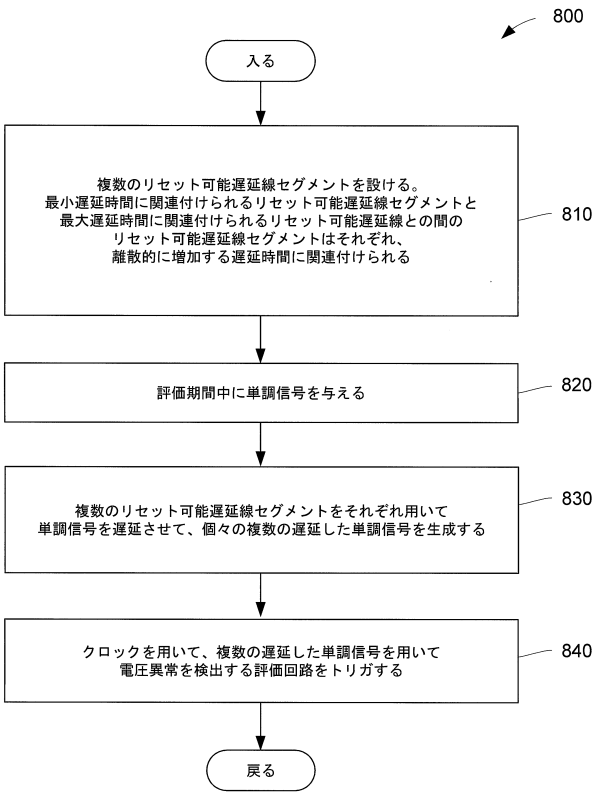


FIG. 7

【図８】



フロントページの続き

(72)発明者　マシュー・スコット・マグレガー
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ユコン・タオ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　行田　悦資

(56)参考文献　米国特許第７２３３１８２（ＵＳ，Ｂ１）
特開平７－８４６６７（ＪＰ，Ａ）
国際公開第２００４／０９２９３２（WO，Ａ１）
特表２０１６－５１１６０６（ＪＰ，Ａ）
特開昭６３－０７９１２１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／７２
Ｇ０６Ｆ　１／０４