(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7005576号
(P7005576)

(45)発行日　令和4年1月21日(2022.1.21)

(24)登録日　令和4年1月7日(2022.1.7)

(51)国際特許分類
G06F 21/55 (2013.01)

FI
G06F 21/55 380

請求項の数 20 （全18頁）

(21)出願番号　特願2019-203511(P2019-203511)
(22)出願日　令和1年11月8日(2019.11.8)
(65)公開番号　特開2020-87453(P2020-87453A)
(43)公開日　令和2年6月4日(2020.6.4)
審査請求日　令和1年11月8日(2019.11.8)
(31)優先権主張番号　16/194,342
(32)優先日　平成30年11月18日(2018.11.18)
(33)優先権主張国・地域又は機関
米国(US)
前置審査

(73)特許権者　508197206
新唐科技股▲ふん▼有限公司
台湾新竹科學工業園區新竹市研新三路４號
(74)代理人　100102923
弁理士　加藤 雄二
(72)発明者　ジブ ヘルシュマン
イスラエル ジヴァットシュムエル市 ラハヴァットイラン通り１４
審査官　宮司 卓佳

最終頁に続く

(54)【発明の名称】　小型オーバーヘッドランダムプリチャージを使用してサイドチャネル攻撃を防犯する電子デバイス

(57)【特許請求の範囲】
【請求項１】
少なくとも一つの入力及び少なくとも一つの出力を有する組み合わせ論理回路と、
複数の連続する周波数期間で前記組み合わせ論理回路の前記少なくとも一つの出力信号をサンプリングする少なくとも一つのステートサンプリングコンポーネントと、
保護回路と、を備え、
前記保護回路は、前記複数の周波数期間ごとに、
前記周波数期間における前記ステートサンプリングコンポーネントのサンプリング時間前に、所定の持続時間で前記組み合わせ論理回路の前記少なくとも一つの入力にランダムデータを提供し始める動作と、
前記ランダムデータを提供した後に、前記組み合わせ論理回路の前記少なくとも一つの入力に関数型データを提供するように変更して、前記ステートサンプリングコンポーネントにサンプリングをさせる動作とを実行することにより、前記組み合わせ論理回路を保護する、
前記組み合わせ論理回路における前記少なくとも一つの入力と前記少なくとも一つの出力との何れかの信号経路における転送遅延は、前記所定の持続時間以上であり、前記ステートサンプリングコンポーネントの前記サンプリング時間前に、前記所定の持続時間で前記ランダムデータが提供し始められることを特徴とする電子デバイス。
【請求項２】
前記ランダムデータ及び前記関数型データは、前記ステートサンプリングコンポーネント

に入力され、前記転送遅延は前記所定の持続時間以上であるので、前記ステートサンプリングコンポーネントは、前記ランダムデータをサンプリングしないで、前記関数型データのみをサンプリングすることを特徴とする請求項１に記載の電子デバイス。
【請求項３】
前記組み合わせ論理回路は、少なくとも前記所定の持続時間に設定されるホールドタイム余裕度を有することを特徴とする請求項１に記載の電子デバイス。
【請求項４】
前記組み合わせ論理回路は、前記ホールドタイム余裕度を少なくとも前記所定の持続時間に設定するための少なくとも一つの信号経路に挿入される遅延ユニットを少なくとも一つ含むことを特徴とする請求項３に記載の電子デバイス。
【請求項５】
暗号化動作を実行するための第１の暗号化エンジン及び第２の暗号化エンジンを更に含み、前記保護回路は、前記第１の暗号化エンジンを使用して前記ランダムデータを生成するときは前記第２の暗号化エンジンを使用せず、かつ前記第２の暗号化エンジンを使用して前記ランダムデータを生成するときは前記第１の暗号化エンジンを使用せずに前記暗号化動作を実行することを特徴とする請求項１に記載の電子デバイス。
【請求項６】
前記保護回路は、前記複数の周波数期間ごとに前記ランダムデータを複数回修正するために用いられることを特徴とする請求項１に記載の電子デバイス。
【請求項７】
前記ランダムデータ及び前記関数型データを提供するためのタイミングは、前記電子デバイスにより事前に設定され、前記電子デバイスは、前記組み合わせ論理回路の独立性能に基づいて前記タイミングを事前に設定することを特徴とする請求項１に記載の電子デバイス。
【請求項８】
前記保護回路は、前記組み合わせ論理回路の実際的な性能に基づいて、前記ランダムデータ及び前記関数型データを提供するためのタイミングを適応的に修正することを特徴とする請求項１に記載の電子デバイス。
【請求項９】
前記保護回路は、前記タイミングを適応的に修正するので、前記ランダムデータを提供する動作期間を改善することを特徴とする請求項８に記載の電子デバイス。
【請求項１０】
前記関数型データを前記組み合わせ論理回路における前記少なくとも一つの入力に提供する前に、前記組み合わせ論理回路は、全ての前記信号経路における前記ランダムデータの転送を先に完了することを特徴とする請求項１に記載の電子デバイス。
【請求項１１】
電子デバイスにおける少なくとも一つの入力及び少なくとも一つの出力を有する組み合わせ論理回路を保護する方法であって、
複数の連続する周波数期間において、少なくとも一つのステートサンプリングコンポーネントを使用して前記組み合わせ論理回路における前記少なくとも一つの出力信号をサンプリングすることと、
前記複数の周波数期間ごとに、以下のようなステップを行って前記組み合わせ論理回路を保護すること、とを含み、
行うステップは、
前記周波数期間における前記ステートサンプリングコンポーネントのサンプリング時間前に、所定の持続時間で前記組み合わせ論理回路の前記入力にランダムデータを提供し始めるステップと、
前記ランダムデータを提供した後に、前記組み合わせ論理回路の入力に関数型データを提供するように変更して、前記ステートサンプリングコンポーネントにサンプリングをさせるステップと、を含み、

前記組み合わせ論理回路における前記少なくとも一つの入力と前記少なくとも一つの出力との何れかの信号経路における転送遅延は、前記所定の持続時間以上であり、前記ステートサンプリングコンポーネントの前記サンプリング時間前に、前記所定の持続時間で前記ランダムデータが提供し始められることを特徴とする電子デバイスにおける少なくとも一つの入力及び少なくとも一つの出力を有する組み合わせ論理回路を保護する方法。

【請求項１２】

前記ランダムデータ及び前記関数型データは、前記ステートサンプリングコンポーネントに入力され、前記転送遅延は前記所定の持続時間以上であるので、前記ステートサンプリングコンポーネントは、前記ランダムデータをサンプリングしないで、前記関数型データのみをサンプリングすることを特徴とする請求項１１に記載の方法。

【請求項１３】

前記組み合わせ論理回路は、少なくとも前記所定の持続時間に設定されるホールドタイム余裕度を有することを特徴とする請求項１１に記載の方法。

【請求項１４】

前記組み合わせ論理回路は、前記ホールドタイム余裕度を少なくとも前記所定の持続時間に設定するための少なくとも一つの信号経路に挿入される遅延ユニットを少なくとも一つ含むことを特徴とする請求項１３に記載の方法。

【請求項１５】

前記電子デバイスは、暗号化動作を実行するための第１の暗号化エンジン及び第２の暗号化エンジンを含み、

前記ランダムデータを生成するステップは、

前記保護回路は、前記第１の暗号化エンジンを使用して前記ランダムデータを生成するときは前記第２の暗号化エンジンを使用せず、かつ前記第２の暗号化エンジンを使用して前記ランダムデータを生成するときは前記第１の暗号化エンジンを使用せずに前記暗号化動作を実行することを含むこと、

を特徴とする請求項１１に記載の方法。

【請求項１６】

前記複数の周波数期間ごとに前記ランダムデータを複数回修正することを更に含むことを特徴とする請求項１１に記載の方法。

【請求項１７】

前記電子デバイスの前記組み合わせ論理回路の独立性能に基づいて、前記ランダムデータ及び前記関数型データを提供するためのタイミングを事前に設定することを更に含むことを特徴とする請求項１１に記載の方法。

【請求項１８】

前記組み合わせ論理回路の実際的な性能に基づいて、前記ランダムデータ及び前記関数型データを提供するためのタイミングを適応的に修正することを更に含むことを特徴とする請求項１１に記載の方法。

【請求項１９】

前記タイミングを適応的に修正するステップは、

前記ランダムデータを提供する動作期間を改善することを含む

ことを特徴とする請求項１８に記載の方法。

【請求項２０】

続き関数型データが前記組み合わせ論理回路の前記少なくとも一つの入力に提供される前に、前記組み合わせ論理回路の全ての前記信号経路における前記ランダムデータの転送を完了することを特徴とする請求項１１に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は電子回路のデータセーフティの技術分野に関し、特にサイドチャネル攻撃(side-channel attacks) を防犯する方法及びシステムに関する。

【背景技術】
【０００２】
近年、例えばサイドチャネル攻撃など、電子デバイスから情報を取得するための様々な技術が発展されている。このような攻撃は通常、許可されていない者により実行され、電子デバイスに保存された機密情報をアクセスされる。サイドチャネル攻撃の原理は、主に論理デバイスの状態遷移時に多くのエネルギーを消耗することに基づく。サイドチャネル攻撃は、情報が保存された電子デバイスに電気的に接触する必要がなく、非侵襲的測定電子デバイスからの電子信号及び/又は放射線を介して、情報を取得する。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
現在、電子デバイスをサイドチャネル攻撃から防犯する様々な対策が講じられている。例えば、２０１２年２月にSouthampton大学の電気資金学院の物理応用科学系のBaddam氏が発表された「Hardware Level countermeasure Against Differential Power Analysis」という名の博士論文に記載された幾つかの対策の中で、特にデュアルレールプリチャージ(Dual Rail Precharge，DRP)回路という方法が注目されている。
【課題を解決するための手段】
【０００４】
本発明の一つの実施例により、本発明の電子デバイスは、組み合わせ論理回路と、少なくとも一つのステートサンプリングコンポーネントと、保護回路と、を備え、組み合わせ論理回路は、少なくとも一つの入力及び少なくとも一つの出力を有し、少なくとも一つのステートサンプリングコンポーネントは、複数の連続する周波数期間で組み合わせ論理回路の少なくとも一つの出力信号をサンプリングするように構成され、保護回路は、ステートサンプリングコンポーネントが周波数期間のサンプリング時間前に、所定の持続時間で前記組み合わせ論理回路の少なくとも一つの入力にランダムデータを提供し始め、及び前記ランダムデータを提供した後で、前記組み合わせ論理回路の少なくとも一つの入力に関数型データを提供しように変更し、前記ステートサンプリングコンポーネントにより少なくとも一つの入力信号をサンプリングする作動を行って組み合わせ論理回路を保護し、前記組み合わせ論理回路の前記入力と前記出力とのいずれかの信号経路における転送遅延は前記所定の持続時間以上であり、前記ステートサンプリングコンポーネントの前記サンプリング時間前に、前記ランダムデータが前記所定の持続時間で提供し始められることを特徴とする。
【０００５】
一つの実施例により、ランダムデータ及び前記関数型データは、入力として前記ステートサンプリングコンポーネントに提供されており、前記転送遅延が前記所定の持続時間以上であるので、前記ステートサンプリングコンポーネントは、前記ランダムデータをサンプリングすることなく、前記関数型データだけをサンプリングする、いくつかの実施例では、組み合わせ論理回路は、少なくとも前記所定の持続時間に設定されるホールドタイム余裕度（hold-time margin）を有し、別の実施例では、組み合わせ論理回路は、少なくとも一つの信号経路に挿入されて、前記ホールドタイム余裕度を少なくとも前記所定の持続時間に設定する少なくとも一つの遅延ユニットを有し。
【０００６】
一つの実施例では、電子デバイスは暗号化動作を実行するために、少なくとも第１の暗号化エンジン及び第２の暗号化エンジンを含んでも良い。前記保護回路は、前記第１の暗号化エンジンを使用して前記ランダムデータを生成するときは前記第２の暗号化エンジンを使用せず、かつ前記第２の暗号化エンジンを使用して前記ランダムデータを生成するときは前記第１の暗号化エンジンを使用せずに前記暗号化動作を実行する。
【０００７】
一つの実施例では、保護回路は、前記複数の周波数期間ごとに前記ランダムデータを複数回修正する。別の実施例において、前記ランダムデータ及び前記関数型データを提供する

ためのタイミングは、前記電子デバイスにより事前に設定され、前記電子デバイスは、前記組み合わせ論理回路の独立性能に基づいて前記タイミングを事前に設定する。更に別の実施例において、保護回路は、前記組み合わせ論理回路の実際的な性能に基づいて、適応的に前記ランダムデータ及び前記関数型データを提供するためのタイミングを修正する。更に別の実施例において、保護回路は、適応的に前記タイミングを修正して、前記ランダムデータを提供する動作期間を改善する。更に別の実施例において、続き関数型データが前記組み合わせ論理回路の少なくとも一つの入力に提供される前に、前記組み合わせ論理回路は、全ての信号経路における前記ランダムデータの転送を完了する。

【０００８】

本発明の一つの実施例により、本発明の少なくとも一つの入力及び少なくとも一つの出力を有する組み合わせ論理回路を保護する方法であって、複数の連続する周波数期間で、少なくとも一つのステートサンプリングコンポーネントを使って前記組み合わせ論理回路の前記出力信号をサンプリングすることと、周波数期間ごとに、以下のようなステップを行って前記組み合わせ論理回路を保護すること、とを含み、前記組み合わせ論理回路を保護することは、前記周波数期間の前記ステートサンプリングコンポーネントのサンプリング時間前に、所定の持続時間でランダムデータを前記組み合わせ論理回路の前記入力に提供し始めるステップと、前記ランダムデータを提供した後で、前記組み合わせ論理回路の入力に関数型データを提供しように変更して、前記ステートサンプリングコンポーネントをサンプリングさせるステップと、を有し、前記組み合わせ論理回路における入力と出力とのいずれかの信号経路における転送遅延が前記所定の持続時間以上であり、前記ステートサンプリングコンポーネントの前記サンプリング時間前に、前記ランダムデータが前記所定の持続時間で提供し始められることを特徴とする。

【図面の簡単な説明】

【０００９】

【図１】本発明の一つの実施例におけるサイドチャネル攻撃を防犯する可能なセーフティ電子デバイスを示すブロック図である。

【図２】図１における電子デバイスの信号タイミング図である。

【図３】図１における電子デバイスの信号タイミング図である。

【図４】本発明の一つの実施例における均一化の遅延を有する組み合わせ論理回路を示すブロック図である。

【図５Ａ】本発明の一つの実施例における互いに接続された二つの暗号化エンジンを含む乱数生成器を示すブロック図である。

【図５Ｂ】図５Ａの乱数生成器に用いられる別のマルチプレクサを示すブロック図である。

【図６】本発明の更に別の実施例におけるサイドチャネル攻撃を防犯するセーフティ電子デバイスを示すブロック図である。

【発明を実施するための形態】

【００１０】

以下、図面及び実施例に基づいて本発明の実施形態を説明する。

【実施例１】

【００１１】

本発明の実施例は、電子デバイスをサイドチャネル攻撃から防犯する改善方法及び回路に関わる。本明細書に記載された技術は、例えばセキュアメモリコンポーネントや内蔵コントローラのような多種類のセーフティデバイスに応用できる。

【００１２】

実施例において、セーフティ電子デバイスは組み合わせ論理回路を含む。組み合わせ論理回路は、通常、関数型データに所定のセーフティ動作を行う複数の互いに接続された論理レベルを含む。組み合わせ論理回路は、関数型データを受信して少なくとも一つの入力を処理し、かつ少なくとも一つの出力で処理の結果を提供する。少なくとも一つのフリップフロップ（ＦＦ）又は他のステートサンプリングコンポーネントは、複数の連続する周波数期間で組み合わせ論理回路の出力信号をサンプリングする。サンプリングされた信号は

、次の周波数期間で入力になる。

【００１３】

セーフティデバイスは更に組み合わせ論理回路をサイドチャネル攻撃から保護する保護回路を含む。いくつかの実施例では、保護回路は、周波数期間ごとにランダムデータと関数型データとを組み合わせ論理回路の入力に交互に提供する。本発明において、ランダムデータの種類は擬似ランダムデータも含む。よって、組み合わせ論理回路は、一部の周波数期間でランダムデータを処理し、他の周波数期間で関数型データを処理する。ランダムデータの処理は、組み合わせ論理回路の瞬時消費電力を有効にランダム化できるため、攻撃者は、組み合わせ論理回路の消費電力又は放射電力を検出することにより機密情報を再構築することが困難である。

【００１４】

本発明の技術提案において、関数型データ及びランダムデータは、同じ信号経路で転送され、同じフリップフロップを通過する。所定の周波数期間において、保護回路は、通常、フリップフロップのサンプリング時間前に、上記周波数期間において組み合わせ論理回路の入力にランダムデータを特定の持続時間で提供し始める。この後で、保護回路は、組み合わせ論理回路の入力に関数型データを提供しように変更して、フリップフロップをサンプリングさせる。

【００１５】

ランダムデータを先に提供する利点は、組み合わせ論理回路がランダムデータを処理する時間の割合を増やして、消費電力をより適切にランダム化できることである。一方、ランダムデータを先に提供するリスクは、フリップフロップがタイミングの変異により関数型データをサンプリングしない可能性があるが、ランダムデータをサンプリングすることである。具体的には、組み合わせ論理回路における少なくとも一つの信号経路の転送遅延は、フリップフロップのサンプリング時間前のランダムデータが始まる持続時間より少ない場合、フリップフロップはランダムデータをサンプリングする。

【００１６】

いくつかの実施例では、保護回路及び/又は組み合わせ論理回路の設計は、以上のような状況を避けることができる。つまり、本発明の設計は、組み合わせ論理回路におけるいずれかの経路の転送遅延が、ＦＦ（フリップフロップ）のサンプリング時間前のランダムデータが始まる持続時間以上であることを保証できる。この制限で、ランダムデータがＦＦのサンプリング時間で組み合わせ論理回路の入力に提供されても、フリップフロップもランダムデータをサンプリングしなく、関数型データだけをサンプリングする。

【００１７】

いくつかの実施例では、組み合わせ論理回路のホールドタイム余裕度に適切な下限値を設定すると、上記限定を満たすことができる。下限値を設定することは、組み合わせ論理回路における信号経路の転送遅延を均一化することに相当する。一つの実施例において、少なくとも一つの信号経路（通常は、最も小さい転送遅延を有する経路）に遅延ユニットを挿入することにより、転送遅延の均一化を実現する。

【００１８】

本発明に記載される技術は、サイドチャネル攻撃に対する防犯を提供する。いくつかの実施例では、セーフティデバイスが有する暗号化エンジンでランダムデータを生成する。また、ホールドタイム及び/又はタイム余裕度の設置する期間でランダムデータを提供するので、本発明の技術提案は周波数の速度に影響がない、或いは影響が小さい。最も実用的な状況で、ランダムデータ及び関数型データの入力時間は重複しても良いが、組み合わせ論理回路での転送経路は異なる。この時間重複の方法は、消費電力のランダム化を向上できるので、安全性が向上される。また、本発明の技術は、関数型データが組み合わせ論理回路に提供される周波数期間の割合を低減できるので、セーフティデバイスの静電気漏れも低減される。

【００１９】

以下、本発明における実施例及び関連する性能折衷案をそれぞれに説明する。

【００２０】
システムの説明
図１は本発明の一つの実施例におけるサイドチャネル攻撃を防犯する可能なセーフティ電子デバイス２０を示すブロック図である。一つの実施例において、セーフティ電子デバイス２０は、例えば暗号化回路を整合するメモリコンポーネント、又は暗号化や検証回路を含む内蔵コントローラ（ＥＣ）或いは基板管理コントローラ(ＢＭＣ)、又は他の任意の適切なセーフティ電子デバイスなどの集積回路（ＩＣ）を含んでも良い。
【００２１】
この例では、セーフティ電子デバイス２０は組み合わせ論理回路２４を含む。組み合わせ論理回路２４は、少なくとも一つの入力Ｍ１及び少なくとも一つの出力Ｄ１を有し、かつ入力Ｍ１を介して入力データが保存されたデジタル入力信号を受け取り、出力Ｄ１を介して出力データが保存されたデジタル出力信号を出力する。組み合わせ論理回路２４は、例えば論理ゲートなどの複数の互いに接続された論理レベルＬを含む。論理レベルＬは、組み合わせ論理回路２４の指定関数を実行し、又は入力Ｍ１を出力Ｄ１に変換する。純粋に論理的な組み合わせとして、組み合わせ論理回路２４は、記憶機能を有しない、例えば出力Ｄ１の処理は入力Ｍ１の現在の数値のみ依存する。
【００２２】
セーフティ電子デバイス２０は、複数の連続する周波数期間で組み合わせ論理回路２４の出力Ｄ１をサンプリングするための少なくとも一つのフリップフロップ（ＦＦ）２８を更に含む。ここでのフリップフロップ２８とは、組み合わせ論理回路２４の現在の状態をサンプリングするための「ステートサンプリングコンポーネント」である。別の実施例において、ステートサンプリングコンポーネントは、複数のラッチと、スタティックランダムアクセスメモリ（ＳＲＡＭ）ユニットと、又は他の任意の適切なメモリユニットとを含んでも良い。サンプリングされた各出力は、ロジックhigh(logic high)又はロジックlow(logic low)であっても良い。
【００２３】
フリップフロップ２８は、クロックツリーからの周波数信号Ｃ１（サンプリング周波数とも呼ばれる）により制御される。この例では、フリップフロップ２８は、出力Ｄ１の周波数信号Ｃ１の期間ごとの上がりエッジでサンプリングするが、これは単なる例であり、本発明はこれに限定されない。サンプリングされた出力（内部の組み合わせ論理回路を通過することなく、セーフティ電子デバイス２０のみとしての出力は含まれない）は、Ｑ１で示す。サンプリングされた出力Ｑ１は、組み合わせ論理回路２４の次の周波数期間での入力信号として、マルチプレクサ３２を介して組み合わせ論理回路２４の入力Ｍ１に提供される。
【００２４】
いくつかの実施例では、組み合わせ論理回路２４は、特定のセーフティ動作を実行する、又は機能を確立するために用いられる。組み合わせ論理回路２４は、例えば乗算段、暗号化、復号化、マーキング又は検証処理の反復、或いは他の任意の適切なセーフティ動作に関連する回路などを含んでも良い。
【００２５】
十分な保護がない限り、攻撃者は、組み合わせ論理回路２４の瞬時消費電力を検出して機密情報を不正に取得することができる。攻撃者は、例えばセーフティ電子デバイス２０の電源供給装置から消費した瞬時消費電力、又はセーフティ電子デバイス２０からの電磁の瞬時電力を検出する可能性がある。
【００２６】
いくつかの実施例では、セーフティ電子デバイス２０は、セーフティ電子デバイス２０をサイドチャネル攻撃から保護する保護回路を更に含む。
【００２７】
この例では、保護回路は、ランダムデータＲ１（ランダムデータもランダムプリチャージデータ（random pre-charging data, RPD）で示す）又は擬似ランダムデータのワード

ストリーム(word stream)を生成する乱数生成器（ＲＮＧ）３６と、ランダムデータＲ１（RPD）及びサンプリングされた関数型データＱ１を交互に入力Ｍ１を駆動するマルチプレクサ（MUX）３２と（なお、組み合わせ論理回路２４が出力する関数型データ（ALD）は演算データとも呼ばれる）、クロックツリーCRに位置する遅延ユニットDLY１、DLY２及びDLY３と、SRのフリップフロップSRFFと、を備える。

【００２８】

以上の保護回路が備えるデバイスは、周波数信号Ｃ１（フリップフロップ２８に用いられる）とMUX制御信号S1（マルチプレクサ３２に用いられる）との相対的なタイミングを制御する。通常、クロックツリーCRはDLY１を含み、以下、DLY２及びDLY３の設計選択について説明する。この例では、DLY２は、DLY１とDLY３との差だ。

【００２９】

組み合わせ論理回路２４における遅延ユニットは、図４に示す態様であってもよい。
ランダムプリチャージの技術を使用してサイドチャネル攻撃を防犯する。

【００３０】

以上のように、保護回路は、組み合わせ論理回路２４の入力を関数型データ（ALD）及びランダムデータ（RPD）で交互に駆動する。前記交互の行為は、周波数期間ごとに実行する。つまり、周波数期間ごとには、RPDが組み合わせ論理回路２４に入力された期間と、ALDが組み合わせ論理回路２４に入力された期間とを含む。これらの入力に応答して、各論理レベルLは、周波数期間の一部の期間でランダムデータを処理し、他の期間で関数型データを処理する。よって、組み合わせ論理回路２４の瞬時消費電力をランダム化できるため、攻撃者は、消費電力又は放射電力を検出することにより関数型データ（ALD）を再構築することが困難である。

【００３１】

いくつかの実施例では、条件を満たすタイミングに応じて、保護回路は、正確なタイミングを選択してランダムデータ（RPD）を組み合わせ論理回路２４に入力し、かつ関数型データ（ALD）を組み合わせ論理回路２４に入力する。

【００３２】

周波数期間ごとには、関数型データが安定してサンプリング可能になる前に（例えば、フリップフロップのこの周波数期間のサンプリング時間前に）、ランダムデータは、組み合わせ論理回路２４の入力に提供される。つまり、MUX制御信号S1は、マルチプレクサ３２を制御して周波数信号Ｃ１の上がりエッジの前で、乱数生成器３６の出力を入力Ｍ１に転送する。

【００３３】

しかしながら、フリップフロップ２８は、ランダムデータ（RPD）をサンプリングすることなく、関数型データ（ALD）だけをサンプリングする。

【００３４】

この二つの条件を満たすためには、組み合わせ論理回路２４におけるいずれかの経路の信号転送時間（転送遅延ともいう）を十分に長くする必要がある。組み合わせ論理回路２４における少なくとも一つの経路の転送路遅延が少なすぎると、ランダムデータは、フリップフロップ２８のサンプリング時間前に、出力Ｄ１に転送され、サンプリングされる。

【００３５】

具体的には、図２に示すように、入力Ｍ１のランダムデータからフリップフロップ２８のサンプリングする（周波数信号Ｃ１の上がりエッジ）までの持続時間は、DLY３に等しい。フリップフロップ２８がランダムデータをサンプリングされないことを保証するために、組み合わせ論理回路２４における入力Ｍ１から出力Ｄ１までのいずれかの経路の最小転送時間は、DLY３以上である必要がある。

【００３６】

図２は、図１におけるセーフティ電子デバイス２０の信号タイミング図であり、上から下に向かって時間軸に以下の信号を表示している、
周波数信号Ｃ１は、フリップフロップ２８に提供される。この例では、フリップフロップ

は、周波数信号Ｃ１の上がりエッジで組み合わせ論理回路２４の出力Ｄ１をサンプリングする。フリップフロップ２８のサンプリング時点は、４０で示す。

【００３７】

MUX制御信号S1は、マルチプレクサ３２を制御する。この例では、MUX制御信号S1はロジックhighである場合に、マルチプレクサ３２は、乱数生成器３６が生成したランダムデータＲ１を出力することを選択する。MUX制御信号S1はロジックlowである場合に、マルチプレクサ３２は、フリップフロップの出力端Ｑが出力したサンプリングされた関数型データＱ１を出力することを選択する。マルチプレクサ３２は、時点４４でランダムデータを提供し始める（MUX制御信号S1は、ロジックlowからロジックhighに切り替える）。

【００３８】

関数型データＱ１は、サンプリング時点４０でのフリップフロップ２８が関数型データ（ALD）をサンプリングした結果である。複数の連続する周波数期間における関数型データは、ALD１、ALD２、ALD３で示し、これで類推する。

【００３９】

入力Ｍ１は、マルチプレクサ３２から組み合わせ論理回路２４に転送される。前述のように、入力Ｍ１の信号はMUX制御信号S1によりランダムデータ（RPD）及び関数型データ（ALD）の間で交互にされる。連続する周波数期間において、ランダムデータはRPD1、RPD２、RPD３…で示し、これで類推する。

【００４０】

出力Ｄ１は、組み合わせ論理回路２４の出力である。この例では、組み合わせ論理回路２４における異なる経路は異なる遅延を有する。よって、いくつかの時点では、図にXXXXXで示し、出力Ｄ１の信号には、瞬時データ、ランダムデータ及び関数型データの混合が乗せられる。他の時点では、出力Ｄ１の全ての信号には、安定非瞬時的なランダムデータ（RPD）又は安定非瞬時的な関数型データ（ALD）だけが乗せられる。

【００４１】

図に示すように、組み合わせ論理回路２４は、周波数期間ごとにおける一つの明らかな時点でランダムデータを処理し、周波数期間における他の時点で関数型データを処理する。よって、組み合わせ論理回路２４の瞬時消費電力及び放射電力をランダム化できるため、電子デバイスをサイドチャネル攻撃から防犯する。

【００４２】

組み合わせ論理回路２４は、周波数期間におけるかなり長い時点でランダムデータを処理するが、フリップフロップ２８は、ランダムデータをサンプリングすることなく、関数型データだけをサンプリングする。この結果は、関数型データＱ１（時点４０で出力D1をサンプリングしたサンプリングのバージョンである）を観察することにより得られる。

【００４３】

図３は、図１におけるセーフティ電子デバイス２０の信号タイミング図である。図２の例に対して、図３の例は、より積極的な設計方法を示し、これはサイドチャネル攻撃に対するより高い防犯を提供するために、組み合わせ論理回路２４における遅延の均一化に対してより高い要求を持っている。

【００４４】

図３において、ランダムデータは、組み合わせ論理回路24の最大転送時間においてT_RPD_maxで示す。ランダムデータは、組み合わせ論理回路24の最小転送時間においてT_RPD_minで示す。関数型データは、組み合わせ論理回路24の最大転送時間においてT_ALD_maxで示す。関数型データは、組み合わせ論理回路24の最小転送時間においてT_ALD_minで示す。図において、設置タイム余裕度及びホールドタイム余裕度が示されている。

【００４５】

入力Ｍ１におけるランダムデータは、RPD0、RPD１…で示し、出力D1におけるランダムデータは、RPDD0、RPDD1…で示す。組み合わせ論理回路24は、RPD及びRPDD0を変更する可能性があるので、RPDの数値は、対応するRPDD0の数値と異なる可能性がある。

【００４６】

図１及び図３に示す実施例により、RPDDは周波数信号Ｃ１の立ち下がりエッジの付近で安定していることが分かった。よって、別の実施例において、次の期間における擬似ランダムデータとして、RPDDは立ち下がりエッジのフリップフロップでサンプリングすることができる。更に別の実施例において、Ｒ１のランダム化を強化するために、RPDDは乱数生成器３６の出力と「排他的又は(XOR)」の処理を行ってもよい。組み合わせ論理回路24は、回路クリティカルセットパス遅延を低減することなく、単一の周波数期間において二つのデータ（具体的には、一つの時点でALDを処理し、別の時点でRPDを処理する）を処理できる。

【００４７】

図２と図３は、周波数信号Ｃ１（或いはサンプリング周波数とも呼ばれる）に対して、MUX制御信号S1のタイミング及びパルス幅（例えば、ランダムデータと関数型データとの交互出力）をどのように設定するかの二つの例を示す。他のタイミング及びパルス幅の設定も使用できる。以下、MUX制御信号S1を定義するための制限及び設計上の考慮事項を説明する。

【００４８】

説明しやすいために、図においては、マルチプレクサ３２及びフリップフロップ２８の転送遅延を無視すると仮定する。周波数信号Ｃ２及びＣ３から導出されるMUX制御信号S1のSRFFでは、入力端（Ｒ）をリセットする優先度は入力端（Ｓ）を設定する優先度より高いと仮定する。説明しやすいために、この例でのMUX制御信号S1の立ち下がりエッジとＣ１の上がりエッジとは重複している。しかしながら、本発明はこの関係に限定されない、他の関係を有しても良い。例えば、MUX制御信号S1の立ち下がりエッジはＣ１の上がりエッジより遅くても良いが、ALDの最大転送時間はMUX制御信号S1の立ち下がりエッジからのみ始まり、Ｃ１の上がりエッジで終わるので、この時のクリティカルセットタイミングが影響を受ける可能性がある。また、MUX制御信号S1の立ち下がり時間を遅延すると、ランダムデータの持続時間を高めることができる、例えば、保護の程度を高めることができる代償として、組み合わせ論理回路２４に対してより厳しい設定時間が必要だ。

【００４９】

いくつかの実施例では、図１の配置は、セーフティ電子デバイス２０において複数に作成でき、かつそれぞれに組み合わせ論理回路２４の異なる部分に応用される。つまり、組み合わせ論理回路２４は複数の部分に分けられてもよく、例えば、タイミング及び/又は物理的に近い部分によって分けられる。保護回路の個別例は、各部分に結合されても良い、かつ個別のマルチプレクサ及び個別のマルチプレクサコントローラを含んでも良い、DLY１、DLY２及び/又はDLY3などの異なる遅延の値を有する可能性もある。

【００５０】

いくつかの実施例では、フリップフロップの出力負荷を最低に低減するために、複数のフリップフロップ２８とマルチプレクサ３２との物理的な距離は、最小値に保たれ、よって、漏電を最低に低減する。また、例えば、図６に示すように、DRPやマスクなどの追加の対策を用いってフリップフロップ２８の漏電を回避する。

【００５１】

組み合わせ論理回路における遅延を均一化により、ランダムデータ及び関数型データを交互に使用し、関数型データのみサンプリングすることを保証する。

【００５２】

以上のように、フリップフロップ２８が出力D1でランダムデータをサンプリングしないことを確保するために、組み合わせ論理回路２４における最小転送時間は、フリップフロップ２８のサンプリング時間前のランダムデータが入力Ｍ１で始まる持続時間以上である必要がある。例えば、図２に示す構造では、前記持続時間は、時点４４（MUX制御信号S1において）と時点４０（信号Ｃ１において）との持続時間だ。組み合わせ論理回路２４におけるいずれかの経路の転送遅延は、前記持続時間以上である必要がある。

【００５３】

いくつかの実施例では、上記のような組み合わせ論理回路２４におけるいずれかの経路の

転送遅延は、所定の持続時間より多いことを確保するための制限は、組み合わせ論理回路２４を実現する集積回路の設計期間に応用できる。例えば、集積回路の設計期間において、組み合わせ論理回路２４におけるホールドタイム余裕度の数値は、少なくとも所定の持続時間に設定されても良い。ホールドタイム余裕度は、通常、正確なタイミングを確保する余裕度より大きい。

【００５４】

普通に言えば、集積回路の設計におけるいずれかのステージにおいて、例えば、回線合成(synthesis) のステージ、放置&配線(P&R)のステージ、又は他のステージで、転送遅延に下限値を設定しても良い。

【００５５】

通常、意図的に組み合わせ論理回路２４における少なくとも一つの最速信号経路の転送遅延を高めることにより、転送遅延における下限値の設定を実現する。転送遅延における所定の持続時間より高い他の経路については、変更する必要がない。いくつかの実施例では、セキュリティが必要とされない特定の信号経路、例えば機密情報を転送しない経路も、転送遅延の均一化する考慮範囲から除外される。

【００５６】

均一化の動作は、異なる経路間の転送遅延の差を低減できる。よって、「組み合わせ論理回路２４における多種の経路の転送遅延の下限値を設定する」というの動作は、「組み合わせ論理回路２４における多種の経路の転送遅延を均一化する」という動作に相当する。組み合わせ論理回路２４における多種の経路の転送遅延が均一するほど、より高いホールドタイム余裕度を有することができる。上記で説明したように、ホールドタイム余裕度は、消費電力をランダム化するが、ランダムデータがサンプリングされないようにランダムデータを挿入できる。

【００５７】

転送遅延を十分に高く確保する一つの方法は、組み合わせ論理回路２４におけるいくつかの論理レベルの間に遅延ユニットを挿入することである。

【００５８】

図４は、本発明の一つの実施例における均一化の遅延を有する組み合わせ論理回路２４を示すブロック図である。この非常に簡略化された例では、組み合わせ論理回路２４における論理レベルは、G1、G2及びG3の三つの論理ゲートを含む。論理ゲートごとには、特定の転送遅延を有する。組み合わせ論理回路２４における多種の経路の転送遅延を均一化ために、二つの遅延ユニット４８が組み合わせ論理回路２４の回路設計に挿入されても良い。遅延ユニットDLY_G1の効果は、論理ゲートG1の転送遅延に近似し、遅延ユニットDLY_G２の効果は、論理ゲートG２の転送遅延に近似する。よって、組み合わせ論理回路２４における三つの信号経路は、ほぼ同じ遅延を有する。

【００５９】

例えばDLY_G1、DLY_G２及びDLY_G３の遅延ユニットは、任意の適切な方式で実現できる、例えば、ダミー論理ユニット、バッファユニット、又は配線（例えば、より長い配線）を使用しても良い。

【００６０】

図４は、本発明を説明ための実施例である。別の実施例において、他の任意の適切な技術は、組み合わせ論理回路２４における多種の信号経路の転送遅延を均一化できる。

【００６１】

一つの実施例では、以下の擬似コード(pseudo-code)は遅延を均一化できる、

・集積回路の設計及びそのタイミングの制限条件を静的タイミング解析ツールにロードする、例えばsynopsys社のPrimeTime又はIC compiler、

・回路設計のトレードオフによってタイミング均一化の制限条件（TBL）を設定する、

・組み合わせ論理回路２４における出力ピンごとについて、

・このピンを通過する最小のスラックを有するタイミング経路を取得する、

・必要に応じて、遅延ユニットを増やして、最小経路タイミングのスラックが TBL より

小さくなるまで遅延を増やす。

【００６２】

上記プロセスは、例えば、回路設計における低速シミュレーション条件で設計の後ルーティング段階(post-routing stage)で実行できる、低速シミュレーション条件は、例えば、高温、低電圧、低速セルプロセスコーナーモデル(slow cell process corner model)、高容量配線又はその組み合わせを含む。

【００６３】

また、回路設計のタイミング最適化ツールで設置タイム余裕度に対して適切な下限値を設定することは遅延の均一化を改善でき、なお、回路設計のタイミングの需要を満たすために必要な設置タイム余裕度を超える。例えば、(i) 遅延を低減する（後は均一化が必要）、及び(ii)最長と最短経路の間のプロセス変動を低減できるので、設置タイムを制限するのは有利である。

【００６４】

乱数生成器の構成例

各実施例では、乱数生成器３６は任意の適切なアナログ及び/又はデジタル回路で実現できる。乱数生成器３６は、必ずしも周波数で駆動する必要がない、アナログノイズ源で実現しても良い。別の実施例では、乱数生成器３６は、全デジタルハードウェアで実現でき、例えば、周波数論理を使用して擬似ランダムデータ列を生成する。いくつかの実施例では、乱数生成器３６は、セーフティ電子デバイス２０の固有するセキュリティ関連回路、例えばセキュア・ハッシュ・アルゴリズム(SHA)、又は高度暗号化規格(AES)暗号化エンジンを再利用しても良い。この場合には、毎回ランダムシードでSHA又は高度暗号化規格を実行したほうがいい。

【００６５】

図５Ａは、本発明の一つの実施例における乱数生成器３６を実現するための乱数生成器を示すブロック図である。この実施例は、SHA及びAESを採用したセーフティ電子デバイス２０のサイドチャネル攻撃対策以外のセキュリティ動作に使用することができる。

【００６６】

図５Ａに示す例では、乱数生成器は互いに接続された二つの乱数生成器（以下、暗号化エンジンを呼ぶ）を含む、図５Ａの左側に示す高度暗号化規格(AES)暗号化エンジンはAES論理回路５２及びフリップフロップ５６を含み、右側に示すSHA暗号化エンジンはSHA論理回路６０及びフリップフロップ６４を含む。マルチプレクサ６８は、フリップフロップ５６と６４の出力を受け取り、かつAES論理回路52の入力にマルチタスクを処理する。図５Ａにおいて、信号AES_NOISE_EN（図５Ａには、AES NOISE ENで示す）はAESノイズを起動し、信号SHA_NOISE_EN（図５Ａには、SHANOISE ENで示す）はSHAノイズを起動する。

【００６７】

いくつかの実施例における一部の期間では、セーフティ電子デバイス２０は、SHA暗号化エンジンを使用せず、AES暗号化エンジンを使用し、他の期間では、セーフティ電子デバイス２０は、AES暗号化エンジンを使用せず、SHA暗号化エンジンを使用する。これらの実施例では、使用されない乱数生成器は、乱数生成器36として再利用されてランダムデータ(RPD)を生成してもよい。つまり、セーフティ電子デバイス２０はSHA暗号化エンジンを使用しないでAES暗号化エンジンを使用する場合には、SHA暗号化エンジンはRPDを生成するために使用される。セーフティ電子デバイス２０はAES暗号化エンジンを使用しないでSHA暗号化エンジンを使用する場合には、AES暗号化エンジンはRPDを生成するために使用される。

【００６８】

フリップフロップ５６及び６４は、AES及びSHA暗号化エンジンの内部のバッファを表してもよく、必ずしもメインモジュール出力に結合されない（例えば、高度暗号化標準パスワード又はＳＨＡの処理）。よって、対応する暗号化エンジンを実行する時に、これらの数値は周波数期間ごとに変更できる。

【００６９】
信号AES_NOISE_EN及び信号SHA_NOISE_ENは、対応する暗号化エンジンに入ることができ、「ノイズ」の状態に入ると、暗号化エンジンは、停止するまで乱数の生成を維持するために、ますます多くなるデータを処理し続ける、例えば、NOISE_ENの信号リセットまで。マルチプレクサ６８及び７２は、図１のマルチプレクサ３２と類似する。
【００７０】
図５Ｂは、図５Ａの乱数生成器に用いられるマルチプレクサ６８及び７２の別の配置を示すブロック図である。乱数生成器の他の部分は、変更されない。
【００７１】
図５Ａと図５Ｂの乱数生成器の配置は、あくまで例示であり、本発明はこれに制限されない、他の任意の適切な方式でも使用できる。例えば、乱数生成器（RNG）は、少なくとも二つの任意の種類の暗号化エンジンの組み合わせで実現でき、例えば、Rivest-Shamir-Adleman(RSA) 暗号化エンジン、Elliptic－CurveCryptography（ECC）暗号化エンジン又はCRC暗号化エンジンを使用する。
【００７２】
追加の対策の統合
図６は、本発明の更に別の実施例におけるサイドチャネル攻撃を防犯するセーフティ電子デバイスを示すブロック図である。図６は、図１～３の保護機構が追加のセキュリティ対策と組み合わせることができることを証明できる。図６は、一つの組み合わせ可能な対策を例として示す。
【００７３】
この例では、フリップフロップ２８から読み取られる及びフリップフロップ２８に書き込まれるデータは、一つの追加の乱数生成器８０でマスクされる。フリップフロップ２８のサンプリングする前に、乱数生成器８０により生成されたランダムデータMDは、組み合わせ論理回路２４の出力Dと組み合わせ、例えば、ビット相互排他又はゲート(bitwise XOR)を使用して組み合わせる。この他、追加のフリップフロップ８４は、ランダムデータMDをサンプリングする。組み合わせ論理回路２４の入力を駆動する前に、フリップフロップ８４が出力したサンプリングデータMQは、マルチプレクサ３２のサンプリングされた出力と組み合わせ、例えば、ビット相互排他又はゲートを使用して組み合わせる。
【００７４】
追加の実施例及び変形例
いくつかの実施例では、周波数期間ごとに、乱数生成器３６はランダムデータを複数回修正する。例えば、図２の入力M1を参照し、間隔RPDにおけるランダムデータの数値は、少なくとも一回変更される。
【００７５】
いくつかの実施例では、ランダムデータ及び関数型データを提供するタイミングは一定的ではない。タイミングを修正することにより、周波数期間におけるランダムデータを提供する期間の割合、及び周波数期間における関数型データを提供する期間の残りの割合を制御できる。フリップフロップのサンプリング時間（例えば、図２と３に示す時点４０）前のランダムデータが始まる（例えば、図２と３に示す時点４４）持続時間も制御できる。図１に示す配置では、例えば、遅延ユニットDLY3を修正することにより、上記タイミングを修正してもよい。
【００７６】
本発明において、「ランダムデータ及び関数型データを提供するタイミング」とは、周波数期間におけるランダムデータ（例えば、時点４４）からフリップフロップのサンプリング時間（例えば、時点４０）までのサイズ及び/又は位置である。
【００７７】
いくつかの実施例では、電子デバイスにおける組み合わせ論理回路の独立性能に応じて、ランダムデータ及び関数型データを提供するタイミングの設定は、セーフティ電子デバイス２０ごとに独立する。例えば、この設定は、独立セーフティ電子デバイス間のホールド

タイム余裕度の統計的な違いを利用でき、例えば、プロセス変動を利用する。
【００７８】
例えば、セーフティ電子デバイス２０における組み合わせ論理回路２４は、高い設置タイム余裕度及び低いホールドタイム余裕度を有することが考えられる。前記独立セーフティ電子デバイス２０において、タイミングは、フリップフロップのサンプリング時間（例えば、時点４０）後にランダムデータを提供し始め、かつフリップフロップのサンプリング時間（例えば、時点４０）後にランダムデータの提供を停止するように設定されてもよい。上記順番の設定は任意の適切な時間で実行でき、例えば、セーフティ電子デバイス２０の製造又は最終のテストの時に実行する。この設定は、回路補正やトレーニングシーケンスと見なす場合がある。
【００７９】
また、セーフティ電子デバイス２０において、組み合わせ論理回路の現在の実際の性能に応じて、保護回路は、ランダムデータ及び関数型データを提供するタイミングと時間的に適合できる。例えば、この適合は、例えば温度、電圧又はその他の動作条件による違いなど、時間の経過に伴う転送遅延の違いを利用できる。この適合は、コンポーネント間の違い(device-to-devicevariations)も利用できる。
【００８０】
一つの実施例では、組み合わせ論理回路２４の出力（Ｄ１）を監視することにより、保護回路は、組み合わせ論理回路２４の入力（Ｍ１）に予め定義トレーニングシーケンスを提供し、及び組み合わせ論理回路２４のホールドタイム余裕度（信号経路の転送遅延間の均一化程度に等しい）を推定し、かつタイミング（例えば、ＤＬＹ２及びＤＬＹ３のタイミング）を設定できる。例えば、上記順番の適合は、電源投入時またはリセット時に実行され、及び/又は毎回組み合わせ論理回路２４を使用して暗号化動作が行われる前に、定期的に実行されてもよい。
【００８１】
この実施例では、ホールドタイム余裕度が高い場合、周波数期間のより先の部分（フリップフロップのサンプリング時間前に）にランダムデータを提供することで、安全性を向上する。その他の時間で、ホールドタイム余裕度が低い場合、ランダムデータが周波数期間のより遅い部分（フリップフロップのサンプリング時間前に）に提供される必要があるが、この場合には、設定余裕度は通常より高いので、ランダムデータがデータのサンプリング時間後に提供されてもよい。
【００８２】
通常の実施例では、例えば、プロセス変動、電圧変動及び温度変動により組み合わせ論理回路２４の最も遅い転送時間を起こす場合、低速プロセス-電圧-温度(PVT)コーナーでホールドタイム余裕度は高い。この条件では、周波数期間のより先の部分（フリップフロップのサンプリング時間のより前に）にランダムデータを提供することで、安全性を向上する。同じ方式により、高速プロセス電圧温度(PVT)コーナーでホールドタイム余裕度が小さくなり、ランダムデータが周波数期間のより後の部分（リップフロップのサンプリング時間前に）に提供されてもよい。
【００８３】
ランダムデータ及び関数型データを提供するタイミングを適合する利点を証明ために、以下の数値が考えられる。組み合わせ論理回路２４の最小転送時間は、低速ＰＶＴコーナーで１０nsと、高速ＰＶＴコーナーで６nsと仮定され、組み合わせ論理回路２４の最大転送時間は、低速ＰＶＴコーナーで２０nsと、高速ＰＶＴコーナーで１２nsと仮定される。
【００８４】
この場合には、保護回路は遅延ユニットＤＬＹ２及びＤＬＹ３の適応的な補正を実行できるため、低速ＰＶＴコーナーでフリップフロップのサンプリング時間（例えば、時点４０）前の１０ns（例えば、時点４４）からフリップフロップのサンプリング時間（例えば、時点４０）までランダムデータ（ＲＰＤ）を提供することができる。高速ＰＶＴコーナーでフリップフロップのサンプリング時間（例えば、時点４０）前の６ns（例えば、時点４

４）からフリップフロップのサンプリング時間（例えば、時点４０）後の８nsまでＲＰＤを提供することができる。

【００８５】

上記内容において、ランダムデータ及び関数型データを提供するタイミングの設定は、ランダムデータを提供する動作期間（周波数期間の割合）を改善し、かつランダムデータがサンプリングされないことを確保することを目的としている。この条件は、関数型データを提供する動作期間（周波数期間の割合）を最低に低減できる。よって、セーフティ電子デバイス２０の静電気漏れも低減できる。

【００８６】

分かり易いために、図１、４、５A、５B及び６に示すセーフティ電子デバイス、組み合わせ論理回路及び乱数生成器の配置は例のみである。他の実施例では、別の任意の適切な配置も使用できる。各実施例では、セーフティ電子デバイス、組み合わせ論理回路及び/又は乱数生成器は任意の適切なハードウェアで実現でき、例えば、少なくとも一つの個別コンポーネント、少なくとも一つの特殊なアプリケーション集積回路(ASIC)及び/又は少なくとも一つのフィールド・プログラマブル論理ゲート・アレイ(FPGA)を使用してもよい。

【００８７】

本発明のいくつかの実施例を説明したが、発明の範囲を限定することは意図していない。これら実施例は、本発明の要旨を逸脱しない範囲で、種々の置き換え、変更を行うことができる。

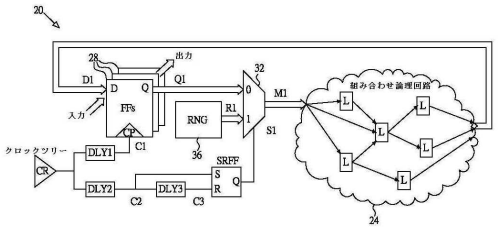
【符号の説明】

【００８８】

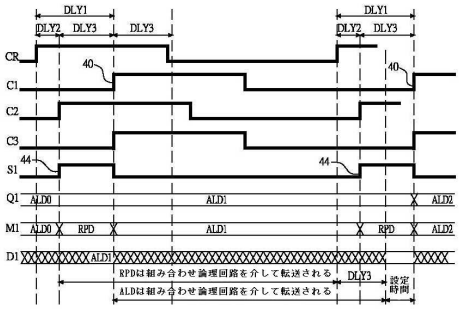
２０…セーフティ電子デバイス
２４…組み合わせ論理回路
２８、５６、６４、８４、FF…フリップフロップ
３２，６８，７２…マルチプレクサ
３６，８０、RNG…乱数生成器
４０，４４…時点
４８、DLY_G1、DLY_G２、DLY1、DLY２、DLY３…遅延ユニット
５２…AES論理回路
６０…SHA論理回路
ALD、ALD１、ALD２、ALD３…関数型データ
C1,C2,C3…周波数信号
CR…クロックツリー
G1,G2,G3…論理ゲート
L…論理レベル
M1…入力
MQ…サンプリングデータ
Q,D,D1…出力
Q1…関数型データ
R1,RPD、RPD１、RPD２、RPD３、RPDD、RPDD０、RPDD１、MD…ランダムデータ
S1…MUX制御信号
SRFF…SRのフリップフロップ
T_ALD_max…最大転送時間
T_ALD_min…最小転送時間
T_RPD_max…最大転送時間
T_RPD_min…最小転送時間

【図面】

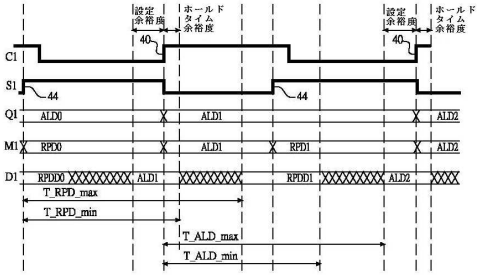
【図１】



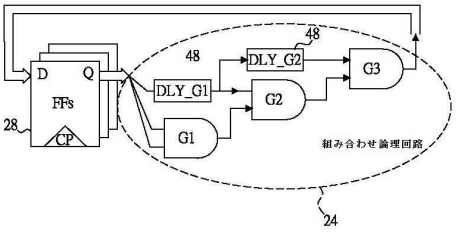
【図２】



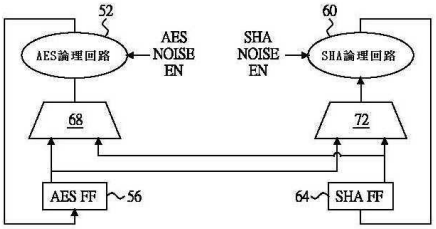
【図３】



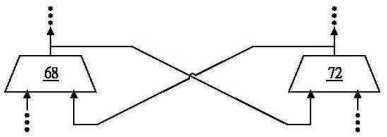
【図４】



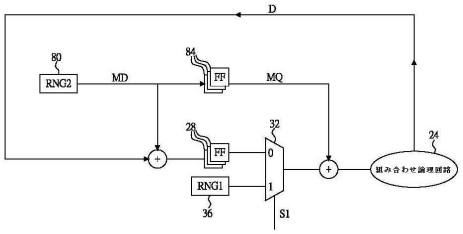
【図５Ａ】



【図５Ｂ】



【図６】



フロントページの続き

(56)参考文献　　米国特許出願公開第２０１７／００６１１２１（ＵＳ，Ａ１）
特開２０１４－０４９８９１（ＪＰ，Ａ）
特開２０１０－２１９６６６（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５