(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2020-512571
(P2020-512571A)
(43)公表日　令和2年4月23日(2020.4.23)

(51)Int.Cl.			F I			テーマコード（参考）
G09C	1/00	(2006.01)	G09C	1/00	650B	
G06F	7/58	(2006.01)	G06F	7/58	620	

審査請求 有　予備審査請求 未請求　（全 17 頁）

(21)出願番号　特願2019-528722 (P2019-528722)
(86)(22)出願日　平成29年11月21日 (2017.11.21)
(85)翻訳文提出日　令和1年6月11日 (2019.6.11)
(86)国際出願番号　PCT/EP2017/079862
(87)国際公開番号　WO2018/099760
(87)国際公開日　平成30年6月7日 (2018.6.7)
(31)優先権主張番号　102016223695.4
(32)優先日　平成28年11月29日 (2016.11.29)
(33)優先権主張国・地域又は機関
ドイツ(DE)

(71)出願人　399023800
コンティネンタル・テーベス・アクチエンゲゼルシヤフト・ウント・コンパニー・オッフェネ・ハンデルスゲゼルシヤフト
ドイツ連邦共和国、６０４８８　フランクフルト・アム・マイン、ゲーリッケストラーセ，７
(74)代理人　100069556
弁理士　江崎　光史
(74)代理人　100111486
弁理士　鍛冶澤　實
(74)代理人　100173521
弁理士　篠原　淳司

最終頁に続く

(54)【発明の名称】車両ネットワークの制御ユニットのために乱数を提供する方法及びその方法を実施する車両ネットワーク

(57)【要約】
本発明は、車両ネットワーク１を介して通信する制御ユニット２，３，４，５のために乱数を提供する方法に関し、集約コンポーネント７．１、メモリユニット７．２及び分配コンポーネント７．３を有する乱数発生器７が準備され、それぞれ少なくとも一つのエントロピー源２．１０，３．１０，４．１０を備えた複数の制御ユニット２．３．４が構成され、それらの生データが車両ネットワーク１を介して集約コンポーネント７．１に伝送され、非決定論的に生じるような、並びに最小限のエントロピーを含むような組み合わされた生データだけを認定された生データとして使用することによって、エントロピー源２．１０，３．１０，４．１０の組み合わされた生データの品質保証が実行され、これらの認定された生データが暗号一方向関数を用いて集約されたデータブロックに変換されて、乱数としてメモリユニット７．２に安全に保存され、最終的に、このメモリユニット７．２に安全に保存された乱数が、分配コンポーネント７．３を用いて、車両ネットワーク１を介して制御ユニット４，５に伝送される。

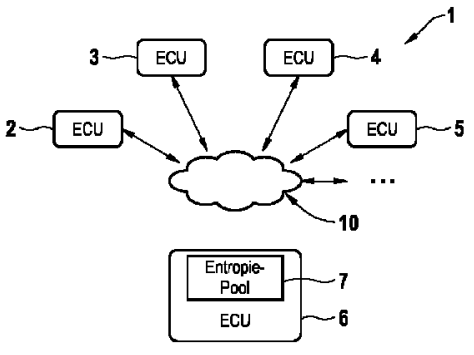


Fig. 1

【特許請求の範囲】
【請求項１】
車両ネットワーク（１）を介して通信する制御ユニット（２，３，４，５）のために乱数を提供する方法であって、
ａ）これらの制御ユニット（４，５）に乱数を伝送するために、車両ネットワーク（１）と接続される乱数発生器（７）を準備する工程であって、この乱数発生器（７）が集約コンポーネント（７．１）、メモリユニット（７．２）及び分配コンポーネント（７．３）を有する工程と、
ｂ）それぞれ少なくとも一つのエントロピー源（２．１０，３．１０，４．１０）を備えた複数の制御ユニット（２．３．４）を構成する工程であって、これらのエントロピー源（２．１０，３．１０，４．１０）から生成された生データが乱数を生成するために、車両ネットワーク（１）を介して乱数発生器（７）の集約コンポーネント（７．１）に伝送される工程と、
ｃ）これらのエントロピー源（２．１０，３．１０，４．１０）から集約コンポーネント（７．１）に伝送されて来た生データを組み合わせる工程と、
ｄ）非決定論的に生じるような、並びに最小限のエントロピーを含むような組み合わされた生データだけを認定された生データとして使用することによって、エントロピー源（２．１０，３．１０，４．１０）の組み合わされた生データの品質保証を実行する工程と、
ｅ）これらの認定された生データを暗号一方向関数を用いて集約されたデータブロックに変換することによって、これらの認定された生データを後処理する工程と、
ｆ）この集約されたデータブロックを乱数としてメモリユニット（７．２）に安全に保存する工程と、
ｇ）分配コンポーネント（７．３）を用いて、このメモリユニット（７．２）に保存された乱数を車両ネットワーク（１）を介して制御ユニット（４，５）に伝送する工程と、
を有する方法。
【請求項２】
本方法の前記の工程ｇに基づき、各乱数が一度だけ伝送される、請求項１に記載の方法。
【請求項３】
本方法の前記の工程ｂにより、乱数発生器（７）も、少なくとも一つのエントロピー源（７．４０，７．５０）を有するように構成される、請求項１又は２に記載の方法。
【請求項４】
エントロピー源（２．１０，３．１０，４．１０，７．４０，７．５０）として、車両で用いられるセンサーの測定の不正確さが使用される、請求項１から３までのいずれか一つに記載の方法。
【請求項５】
センサーとして、エンジン回転数センサー、車両のハンドルの操舵運動を検出するセンサー、レーダーセンサー、少なくとも一つの光センサー及び車両のブレーキペダルの位置を検出するセンサーの中の一つ以上が使用される、請求項４に記載の方法。
【請求項６】
前記のセンサーの測定の不正確さが測定されて、ビット数値としてデジタル化され、このビット数値のｎ個の最下位ビットが生データとして使用される、請求項４又は５に記載の方法。
【請求項７】
エントロピー源（２．１０，３．１０，４．１０、７．４０，７．５０）として、車両のデータバス（１０）のバス信号及び車両の制御システムの制御信号の中の一つ以上が使用される、請求項１から６までのいずれか一つに記載の方法。
【請求項８】
前記のデータバス（１０）上の同じタイプの二つの非周期情報の間の時間長がエントロピー源（２．１０，３．１０，４．１０、７．４０，７．５０）として使用される、請求

項７に記載の方法。
【請求項９】
エントロピー源（２．１０，３．１０，４．１０、７．４０，７．５０）として、暗号計算の結果が使用される、請求項１から８までのいずれか一つに記載の方法。
【請求項１０】
暗号計算として、ハッシュ和、メッセージ認証コード（ＭＡＣ）、署名及び暗号化されたデータの中の一つ以上が使用される、請求項９に記載の方法。
【請求項１１】
本方法の前記の工程ｄに基づく品質保証が統計的な解析方法により実行される、請求項１から１０までのいずれか一つに記載の方法。
【請求項１２】
本方法の前記の工程ｆに基づく集約されたデータブロックの保存が、所与の演算モードを有する暗号化アルゴリズムを用いた安全な保存として実行される、請求項１から１１までのいずれか一つに記載の方法。
【請求項１３】
複数の通信する制御ユニット（２，３，４，５）を有する、乱数を提供する車両ネットワーク（１）であって、
制御ユニット（４，５）に乱数を伝送するために車両ネットワーク（１）と接続された乱数発生器（７）であって、集約コンポーネント（７．１）、メモリユニット（７．２）及び分配コンポーネント（７．３）を有する乱数発生器（７）と、
それぞれ少なくとも一つのエントロピー源（２．１０，３．１０，４．１０）を備えた複数の制御ユニット（２，３，４）であって、これらのエントロピー源（２．１０，３．１０，４．１０）から生成された生データが乱数を生成するために、車両ネットワーク（１）を介して乱数発生器（７）の集約コンポーネント（７．１）に伝送することが可能である制御ユニットと、
を有し、
この集約コンポーネント（７．１）は、エントロピー源（２．１０，３．１０，４．１０）から伝送されて来た生データを組み合わせて、非決定論的に生じるような、並びに最小限のエントロピーを有するような組み合わされた生データだけを認証された生データとして使用可能とすることによって、これらの組み合わされた生データに品質保証を施すように構成され、
この集約コンポーネント（７．１）が認証された生データを後処理するように構成され、その後処理では、これらの認証された生データが、暗号一方向関数を用いて、集約されたデータブロックに変換することが可能であるとともに、このデータブロックが、乱数としてメモリユニット（７．２）に保存することが可能であり、
このメモリユニット（７．２）は、分配コンポーネント（７．３）を用いて、車両ネットワーク（１）を介して、保存された乱数を制御ユニット（４，５）に伝送するように構成される、
車両ネットワーク。
【請求項１４】
前記の乱数発生器（７）が少なくとも一つのエントロピー源（７．４０，７．５０）を備えるように構成される、請求項１３に記載の車両ネットワーク（１）。
【請求項１５】
制御ユニット（２，３，４）の前記の少なくとも一つのエントロピー源（２．１０，３．１０，４．１０）が、エントロピーエージェント（２．１，３．１，４．１）内に配置され、これらのエントロピーエージェント（２．１，３．１，４．１）が、単方向通信接続部（ａ１，ａ２，ａ３）を介して、乱数発生器（７）の集約コンポーネント（７．１）と接続される、請求項１３又は１４に記載の車両ネットワーク（１）。
【請求項１６】
乱数発生器（７）の前記の少なくとも一つのエントロピー源（７．４０，７．５０）が

、単方向通信接続部（ａ４，ａ５）を介して乱数発生器（７）の集約コンポーネント（７．１）と接続されたエントロピーエージェント（７．４０，７．５０）内に配置される、請求項１４又は１５に記載の車両ネットワーク（１）。

【請求項１７】

少なくとも一つの制御ユニット（４，５）が、乱数を伝送するために、単方向通信接続部（ｂ１，ｂ２）を介して乱数発生器の分配コンポーネントと接続された乱数収集部（４．２、５．２）を有する、請求項１３から１６までのいずれか一つに記載の車両ネットワーク（１）。

【請求項１８】

少なくとも一つのエントロピー源（２．１０，３．１０，４．１０，７．４０，７．５０）が車両のセンサーである、請求項１３から１７までのいずれか一つに記載の車両ネットワーク（１）。

【請求項１９】

少なくとも一つのエントロピー源（２．１０，３．１０，４．１０，７．４０，７．５０）が車両のデータバス（１０）である、請求項１３から１８までのいずれか一つに記載の車両ネットワーク（１）。

【請求項２０】

少なくとも一つのエントロピー源（２．１０，３．１０，４．１０，７．４０，７．５０）が車両の暗号計算ユニットである、請求項１３から１９までのいずれか一つに記載の車両ネットワーク（１）。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、車両ネットワークを介して通信する制御ユニットのために乱数を提供する方法に関する。本発明は、更に、本発明による方法を実施する車両ネットワークに関する。

【背景技術】

【０００２】

近年、車両は、各機能ユニットを制御するために車両に搭載された多数の制御ユニット（電子制御ユニット：ＥＣＵ）を備えている。それらのＥＣＵは、協力して動作するために、それぞれ車両に搭載されたネットワーク（車両ネットワーク）を介して互いに接続されている。それらのＥＣＵの制御とそれらのＥＣＵの間の通信のために、通常は好適なハードウェアと協働して相応の機能を実行するソフトウェアベースのアプリケーションが使用されている。その場合、そのようなアプリケーションを権限の無いアクセスから保護することが益々重要になっている。それ故、それらのＥＣＵの相互の安全な通信及び外部の通信相手（例えば、サーバー又は別の車両）との安全な通信と鍵交換プロトコルに関して、暗号用の安全な乱数に対する需要が高まっている。それらは、車両のスタート後の出来る限り短い時間内（通常は１００ｍｓ以内）に入手しなければならない。

【０００３】

マイクロコントローラなどのネットワークノードの決定論的システムでは、乱数を生成するための十分なエントロピーを収集することは非常に難しい。そのことは、特に、そのようなマイクロコントローラを含む制御ユニットを備えた車両ネットワークにも当てはまる。

【０００４】

安全な乱数を生成するために、乱数を短時間内に提供するとの要求を解決する真乱数発生器（ＴＲＮＧ：Ｔｒｕｅ　Ｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ）をそれぞれ個々の制御ユニットに取り付けることが知られている。しかし、それらは、多くの場合、スタートプロセス後に速く、十分に良好な乱数を提供することができず、更に、ＥＣＵ毎のコストを上昇させる可能性が有る。

【０００５】

乱数発生器（ＲＮＧ）の重要な特徴は、そのエントロピー、即ち、乱数発生器により生

成される乱数のランダム性と予測不可能性である。
【０００６】
乱数発生器を実現するために、得られる「ランダム性」（エントロピー）を決めるエントロピー源、即ち、非決定論的に動作するシステムが用いられる。更に、エントロピー源からランダムに変動する量を測定するための抽出メカニズムが必要であり、それを用いて、出来る限り多くのエントロピーを「収集」すべできある。最終的に、エントロピー源又は抽出メカニズムの非ランダム性を補正するために、そのようなエントロピー源から供給される生データが処理される。
【発明の概要】
【発明が解決しようとする課題】
【０００７】
本発明の課題は、車両のスタート後の出来る限り短い時間内で入手可能であるとともに、安価に実現可能である、車両内のコンポーネントで暗号用に使用される、車両ネットワークを介して通信する制御ユニットのために安全な乱数を提供する方法を実現することがである。更に、本発明の課題は、本発明による方法を実施する車両ネットワークを提供することがである。
【課題を解決するための手段】
【０００８】
前記の第一の課題は、請求項１の特徴を有する方法により解決される。
【０００９】
この本発明による車両ネットワークを介して通信する制御ユニットのために乱数を提供する方法は、
ａ）これらの制御ユニットに乱数を伝送するために、車両ネットワークと接続された乱数発生器を準備する工程であって、この乱数発生器が集約コンポーネント、メモリユニット及び分配コンポーネントを有する工程と、
ｂ）それぞれ少なくとも一つのエントロピー源を備えた複数の制御ユニットを構成する工程であって、これらのエントロピー源により生成された、乱数を生成するための生データが、車両ネットワークを介して乱数発生器の集約コンポーネントに伝送される工程と、
ｃ）これらのエントロピー源から集約コンポーネントに伝送されて来た生データを組み合わせる工程と、
ｄ）非決定論的に生じるような、並びに最小限のエントロピーを含むような組み合わされた生データだけを認定された生データとして使用することによって、エントロピー源の組み合わされた生データの品質保証を実行する工程と、
ｅ）これらの認定された生データを暗号一方向関数を用いて集約されたデータブロックに変換することによって、これらの認定された生データを後処理する工程と、
ｆ）この集約されたデータブロックを乱数としてメモリユニットに安全に保存する工程と、
ｇ）分配コンポーネントを用いて、このメモリユニットに保存された乱数を車両ネットワークを介して制御ユニットに伝送する工程と、
を有する。
【００１０】
この本発明による方法により、異なるエントロピー源から安全な乱数を生成して、車両ネットワークの中央ネットワークコンポーネントとしての乱数発生器に持続的に、秘匿して、改竄に対して安全な形で保存する、ＥＣＵを備えた車両ネットワークが実現され、その結果、この安全な乱数をメモリユニット内に予め保持することは、車両ネットワークのスタート時間が短い場合に、十分なエントロピーを有する乱数を入手しておき、それらの乱数を暗号演算のために車両ネットワークを介して別の制御ユニットに提供するとの作用を奏する。
【００１１】
そのような乱数発生器のメモリユニット内に安全な乱数を予め保持することによって、

制御ユニットは、個別の乱数発生器を必要とせず、それによって、車両ネットワークのコストを低減することができる。更に、この中央の乱数発生器を用いた乱数の生成に関する中央集中アーキテクチャは、別のエントロピー源の後補充、或いは例えば、セキュリティアップデート過程における乱数発生器のソフトウェアの変更を容易にする。

【００１２】

本発明の有利な改善構成では、乱数の反復使用を防止するために、本方法の工程ｇに基づき、各乱数が一度だけ伝送される。

【００１３】

別の有利な実施形態は、乱数発生器も少なくとも一つのエントロピー源を備えるように構成されると規定する。エントロピー源の数の増加によって、それらにより生成される乱数のランダム性と予測不可能性を改善することができる。

【００１４】

本発明の有利な実施形態では、エントロピー源として、車両で用いられるセンサーの測定の不正確さが使用される。これは、有利には、エンジン回転数センサー、車両のハンドルの操舵運動を検出するセンサー、レーダーセンサー、少なくとも一つの光センサー、車両のブレーキペダルの位置を検出するセンサーの中の一つ以上に関する。

【００１５】

エントロピー源としてセンサーを使用する場合、その測定の不正確さが測定されて、ビット数値としてデジタル化され、このビット数値のｎ個の最下位ビットが生データとして使用される。

【００１６】

更に、改善構成では、エントロピー源として、車両のデータバスのバス信号及び／又は車両の制御システムの制御信号を使用することができる。そのために、有利には、データバス上の同じタイプの二つの非周期情報の間の時間長が使用される。

【００１７】

最後に、改善構成では、エントロピー源として、暗号計算の結果を使用することができる。そのために、有利には、暗号計算として、ハッシュ和、メッセージ認証コード（ＭＡＣ）、署名及び暗号化されたデータの中の一つ以上が使用される。

【００１８】

本発明の別の有利な改善構成では、本方法の工程ｄによる品質保証が統計的な解析方法により実行される。そのために、選定されたデータが非決定論的に生じるとともに、そうでない場合には廃棄されること、即ち、エントロピー源から供給される生データが等しく分布しなければならず、統計的な歪み又は統計的なパターンを含まないことを保証する所定の行列が用いられる。これらの要件は、周知の統計的な解析方法を使用することによって保証される。更に、選定された生データは、或る最小限のエントロピーを有する場合に初めて更に処理される。そのために、等分布に関して検査された生データは、エントロピーを高めるために、暗号ハッシュ関数により混合されて圧縮される。

【００１９】

本方法の工程ｆにおける生成された乱数を集約されたデータブロックとして安全に保存することは、乱数発生器の分配コンポーネントを用いて分配される前に、所定の演算モードを有する暗号化アルゴリズムを用いて実行される。これによって、乱数の秘匿性と完全性が制御ユニットによって使用されるまで保証される。

【００２０】

前記の第二の課題は、請求項１３の特徴を有する車両ネットワークにより解決される。

【００２１】

そのような多数の通信する制御ユニットを備えた、乱数を提供する車両ネットワークは、

乱数を制御ユニットに伝送するために、車両ネットワークと接続された一つの乱数発生器であって、集約コンポーネント、メモリユニット及び分配コンポーネントを有する乱数発生器と、

それぞれ少なくとも一つのエントロピー源を備え、これらのエントロピー源により生成された、乱数を生成するための生データを車両ネットワークを介して乱数発生器の集約コンポーネントに伝送することが可能である複数の制御ユニットと、
を有し、
この集約コンポーネントは、エントロピー源から伝送されて来た生データを組み合わせて、非決定論的に生じるとともに、最小限のエントロピーを有するような組み合わされた生データだけが認定された生データとして使用可能であるとすることによって、これらの組み合わされた生データに品質保証を施すように構成され、
この集約コンポーネントは、これらの認定された生データが、暗号一方向関数を用いて集約されたデータブロックに変換することが可能であり、このデータブロックが乱数としてメモリユニットに安全に保存することが可能であるように、これらの認定された生データを後処理するように構成され、
このメモリユニットは、分配コンポーネントを用いて、保存された乱数を車両ネットワークを介して制御ユニットに伝送するように構成される。
【００２２】
この本発明による車両ネットワークは、本発明による方法と関連して実現される有利な特性も有する。
【００２３】
本発明による車両ネットワークの有利な実施形態は、従属請求項１４～２０の特徴により与えられる。
【００２４】
以下において、添付図面を参照して、本発明による車両ネットワークの実施例に基づき、本発明による方法を記述して説明する。
【図面の簡単な説明】
【００２５】
【図１】本発明による方法を実施する本発明による車両ネットワークの実施例の模式図
【図２】図１の車両ネットワークの詳細な模式図
【図３】図２の車両ネットワークの乱数発生器を用いて乱数を生成する模式図
【発明を実施するための形態】
【００２６】
図１は、本発明による車両ネットワーク１の構造を図示しており、この車両ネットワーク１を用いて、本発明による乱数を提供する方法が実現される。
【００２７】
この車両ネットワーク１は、複数の制御ユニット（ＥＣＵ）２，３，４及び５と、乱数発生器７を有する一つの制御ユニット６とから構成される。これらの制御ユニットは、データバス１０、例えば、ＣＡＮバスを介して互いに通信する。
【００２８】
以下において「エントロピープール」と称し、同じく符号７により表示する乱数発生器７を用いて、乱数が生成されて、それらの乱数は、必要に応じて暗号演算のために所定の制御ユニットに提供するために予め保持される。
【００２９】
そのようなエントロピープール７は、例えば、図１に図示されている通り、一つの制御ユニット６に、ソフトウェアコンポーネントとして統合することができる。そのために、既に存在する制御ユニット６又はそのような目的のために実現された制御ユニット６を使用することができる。
【００３０】
図２は、車両ネットワーク１の構造を詳細に図示している。それによると、エントロピープール７は、以下の主要コンポーネントから構成される。
集約コンポーネント７．１、
安全なメモリとして実現されたメモリユニット７．２、及び

分配コンポーネント。

【００３１】

図２では、乱数の生成に必要なエントロピー源は、幾つかの制御ユニット、即ち、制御ユニット２，３及び４において実現されており、そのために、これらの制御ユニット２，３及び４は、コンポーネントとして、少なくとも一つのエントロピー源を含むエントロピーエージェントを有する。そのように、一つのエントロピー源２．１０を備えた制御ユニット２のエントロピーエージェント２．１、二つのエントロピー源３．１０及び３．１１を備えた制御ユニット３のエントロピーエージェント３．１、並びに一つのエントロピー源４．１０を備えた制御ユニット４のエントロピーエージェント４．１が実現される。

【００３２】

エントロピープール７も、上述した主要コンポーネント以外に、一つのエントロピー源７．４０又は二つのエントロピー源７．５０及び７．５１を備えた二つのエントロピーエージェント７．４及び７．５を有する。

【００３３】

これらの制御ユニット２，３及び４のエントロピーエージェント２．１，３．１，４．１とエントロピープール７のエントロピーエージェント７．４及び７．５は、単方向接続部ａ１，ａ２，ａ３及びａ４，ａ５を介して、エントロピープール７の集約コンポーネント７．１と接続されている。これらの通信接続部ａ１～ａ５を介して、エントロピーエージェントの相応のエントロピー源の乱数の生成に必要な生データが、これらの集約コンポーネント７．１に伝送される。

【００３４】

暗号計算を実行するための乱数を必要とする制御ユニットは、コンポーネントとして、乱数収集部を有する。そのように、制御ユニット４は乱数収集部４．２を有し、制御ユニット５は乱数収集部５．２を有する。これらの乱数収集部４．２及び５．２は、それぞれ単方向接続部ｂ１及びｂ２を介して、エントロピープール７の分配コンポーネント７．３と接続されている。この分配コンポーネント７．３を用いて、通信接続部ｂ１及びｂ２を介して、メモリユニット７．２に保存された乱数が乱数収集部４．２及び乱数収集部５．２に伝送される。

【００３５】

図２から、車両ネットワーク１が、エントロピーエージェントを備えたエントロピーの製造部として実現された制御ユニットを有するとともに、乱数の消費部としてのみ出現する、従って、乱数収集部だけを備え、エントロピーエージェントを備えていない制御ユニットを有することが分かる。そのように、エントロピーの製造部としての二つの制御ユニット２及び３は、エントロピーエージェント２．１及び３．１だけを備える一方、乱数の消費部としての制御ユニット５は、乱数収集部５．２だけを備える。それに対して、制御ユニット４は、エントロピーの製造部としても、乱数の消費部としても出現しており、従って、エントロピーエージェント４．１と乱数収集部４．２の両方を備える。

【００３６】

単方向通信接続部ａ１，ａ２，ａ３及びｂ１，ｂ２は、データバス１０又は別個の通信構成により実現することができる。

【００３７】

乱数を作るために、エントロピープール７は、それに対応する制御ユニット２，３及び４に実装されたエントロピー源２．１０，３．１０，３．１１及び４．１０と独自のエントロピー源７．４０，７．５０及び７．５１の両方を使用する。

【００３８】

これらのエントロピー源を実現するために、異なるランダム事象を用いることができる。

【００３９】

そのようなランダム事象は、例えば、車両で用いられるセンサーのアナログ測定の不正確さなどの物理現象に基づくものであるとすることができる。これらの測定の不正確さは

、通常非決定論的な周囲の影響に起因するので、エントロピー源として使用することができる。それには、例えば、車両内の次のセンサーが適している：
エンジン回転数センサー、
操舵運動を検出するセンサー、
レーダーセンサー、
光センサー、
ブレーキペダルの位置を検出するセンサー。
【００４０】
そのようなセンサーをエントロピー源として使用する場合、それらの測定の不正確さが測定されて、ビット数値としてデジタル化され、このビット数値のｎ個の最下位ビットが生データとして使用される。そのような生データが、例えば、データバス１０上を全てのネットワーク参加者に送信された場合、エントロピープールのエントロピーエージェント７．４及び７．５からのこれらのデータも、データバス１０から直接取り出して、更なる処理のために、集約コンポーネント７．１に伝送することができる。
【００４１】
例えば、データバス１０、或いは制御システム、例えば、車両の快適化システム又は支援システムなどの車両ネットワーク１のコンポーネントで生じる事象もエントロピー源として使用することができる。
【００４２】
そのように、例えば、ＣＡＮバスとして実現されたデータバス１０を使用する場合、ＣＡＮバス上の同じタイプの二つの非周期情報の間における経過時間は、その複雑な決定論的プロセスのために、予測が難しく、そのため、エントロピー源として使用することができる。そのような非決定論的情報は、次の三つの異なるカテゴリーに分類することができる：
ａ）データバス上で所定の非巡回情報タイプの値が出現する間の時間スロット、例えば、
所定のブレーキ値の出現に関する時間スロット、
ウインドウガラスの上下操作の間の時間、
燃料タンク蓋の開放操作の間の時間スロット、
所定の変速段を使用する時間、
ｂ）データバス上における所定の情報又は複数の情報タイプのシーケンスの一連の所定の値の間の時間スロット、例えば、
所定のブレーキ値パターンの間の時間スロット、
一連の変速段の所定の切換パターンと変速切換時における変速段の滞留時間、
ｃ）データバス上における、情報の真の値に注目すること無く互いに独立した情報タイプの所定のシーケンスの時間長、例えば、
走行開始時（加速、変速、給油の混合形態）の所定のパターン
【００４３】
例えば、空調設備などの快適化システムの制御システムをエントロピー源として使用する場合、その制御において測定された、目標値と実際値の間の差が検出される。
【００４４】
最後に、暗号計算の結果は、大抵は高いエントロピーを有するので、保護すべき特性（秘匿性、完全性、信憑性）の安全を保証するために、暗号計算の結果をエントロピー源として使用することも可能である。暗号計算の結果の例は、
ハッシュ和、
メッセージ認証コード（ＭＡＣ）、
署名、
暗号化されたデータ、
である。
【００４５】
基本的に、そのような暗号計算を実行する車両内の各所にエントロピーエージェントを

搭載することが考えられ、それは車両製造業者に依存する。値の反復使用が起こり得ないような暗号方法及び暗号プロトコルだけをエントロピーの生成に使用すべきである。

【００４６】

例えば、ＣＡＮバス上における所定の情報の完全性をメッセージ認証コードを用いて保護する場合、エントロピープール７内のエントロピーエージェント７．４又は７．５のそれに対応する情報を、そのオブジェクトＩＤに基づき直接特定して取り出すことができる。そして、エントロピーエージェント７．４又は７．５は、ＭＡＣを抽出して、集約コンポーネント７．１に転送することができる。

【００４７】

例えば、ＴＬＳなどのプロトコルにより、インターネットを介した車両ネットワーク１の制御ユニットとバックエンドの通信を暗号化する場合、その制御ユニット内のエントロピーエージェントが、その通信の暗号文をエントロピーを取得するために利用して、集約コンポーネント７．１に転送することができる。

【００４８】

エントロピープール７の集約コンポーネント７．１に伝送されて来たデジタル生データは、図３により模式的図示されている通り、処理して、乱数としての適用可能性に関して認証しなければならない。図３によると、「センサー」、「バス信号／制御信号」及び「暗号計算」の異なるエントロピー源の生データは、非決定論的に生じないような、並びに最小限のエントロピーを有するような、異なるエントロピー源からの組み合わされた生データだけを認証された生データとして使用することによって、品質保証を施される。それに続いて、これらの認証された生データは、後処理部に供給された後、これらの認証されるとともに、後処理された生データが安全なメモリとして実現されたメモリユニット７．２に乱数として保存される。

【００４９】

異なるエントロピー源からの組み合わせである、この品質保証を実行するために使用される生データは、所定の行列により評価され、その場合、エントロピー源から提供される生データが等しく分布するとともに、統計的な歪み又は統計的なパターンを含まないことを以下で列挙する検定方法を用いて保証される。この選定された行列は、選定された生データが非決定論的に生じるとともに、そうでない場合には廃棄されることを保証する。更に、収集されたエントロピーデータは、それらが或る最小限のエントロピーを有する場合にのみ再処理のために解放される。そのために、等分布に関して検査された生データは、エントロピーを高めるために、暗号ハッシュ関数により混合されて、圧縮される。一般的には、乱数を決定するための全ての統計的及び決定論的なオンライン検定方法をそのために使用することができる。例えば、次の検定方法をそのために使用することができる。

正規分布を決定するためのカイ二乗検定、シリアル検定、

分布の歪みを確定するためのミニマム検定、バースデイ検定、フリークエンシー検定、

反復パターンを検知するための行列階数検定、重複和検定、

正規分布に一致しない分布の類似度を決定するための相関検定、コルモゴロフ・スミルノフ検定。

【００５０】

これらの前記の通り認証された生データは、後処理のために、暗号一方向関数を用いて、乱数として使用される、集約されたデータブロックに変換される。ブロック暗号モード構造に基づく全ての暗号ハッシュ関数及び一方向関数をそのために使用することができる。一方向関数ｆの場合、その関数の与えられた関数値ｆ（ｘ）からそれに対応するｘ値を見つけるための実施可能な方法は実際には存在しない。

【００５１】

そのような暗号一方向関数は、例えば、次の通りである。

ａ）全ての任意のビット長に関するハッシュ関数、

ＳＨＡ－１、

ＳＨＡ－２、

ＳＨＡ－３、
ＳＨＡＫＥ、
ＰＩＰＥＭＤ、
Ｐｈｏｔｏｎ、
Ｓｐｏｎｇｅｎｔなど、或いは
ｂ）（使用するブロック暗号に依存しない）ブロック暗号モード構造、
デイビス・メイヤー構造、
マティアス・メイヤー構造、
宮口・プレネール構造など。

【００５２】

エントロピー源から得られる生データの最後の処理工程は、集約されたデータブロックとして生成された乱数をエントロピープール７のメモリユニット７．２に安全に保存することである。この安全な保存は、消費部として実現された制御ユニット４及び５で使用するまで乱数の秘匿性と完全性を保証しなければならない。それは、特別な演算モードを有する暗号化アルゴリズムを使用することによって保証することができる。一つの演算モードは、暗号化アルゴリズムを用いた一つ又は複数の平文と暗号ブロックの処理を規定する、ブロック暗号の所定の使用形態である。次の通り、異なる演算モードを列挙する。
ａ）ブロック暗号に依存しない特別な演算モードを有するブロック暗号、例えば、
ＳＩＶモード、
ＣＣＭモード、
ＣＭＡＣメッセージ認証モード、
ＣＢＣ－ＭＡＣ、
Ｏ－ＭＡＣ、
Ｐ－ＭＡＣなど。
ｂ）認証された暗号方式、例えば、
シーザーコンテストの現在の全ての参加者（ｈｔｔｐｓ：／／ｃｏｍｐｅｔｉｔｉｏｎｓ．ｃｒ．ｙｐ．ｔｏ／ｃａｅｓａｒ．ｈｔｍｌ）
ＧＣＭモード、
ＯＣＢモードなど。
ｃ）非対称署名・暗号方法、例えば、
ＥＣＩＥＳ、
ＤＳＡ、
ＥＣＤＳＡ、
ＲＳＡなど。

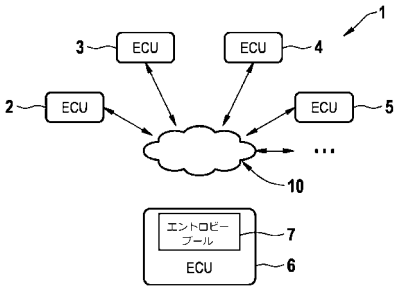
【００５３】

そのようにして生成された乱数は、分配コンポーネント７．３により消費部（即ち、乱数収集部を備えた制御ユニット）に分配するために、メモリユニット７．２に予め保持される。

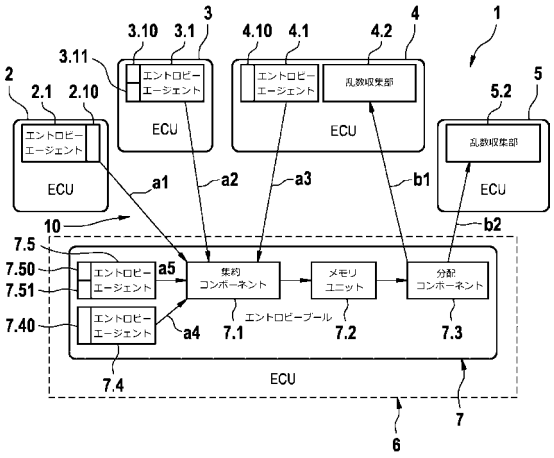
【００５４】

この分配コンポーネント７．３は、生成された乱数が消費部の乱数収集部コンポーネントに分配されることを保証するとともに、メモリユニット７．２がその時々の乱数を保有しない時の更なる出力を阻止する。更に、分配コンポーネント７．３は、乱数が消費部としての制御ユニット４及び５に一度だけ伝送されることを保証し、それによって、乱数の反復使用が防止される。

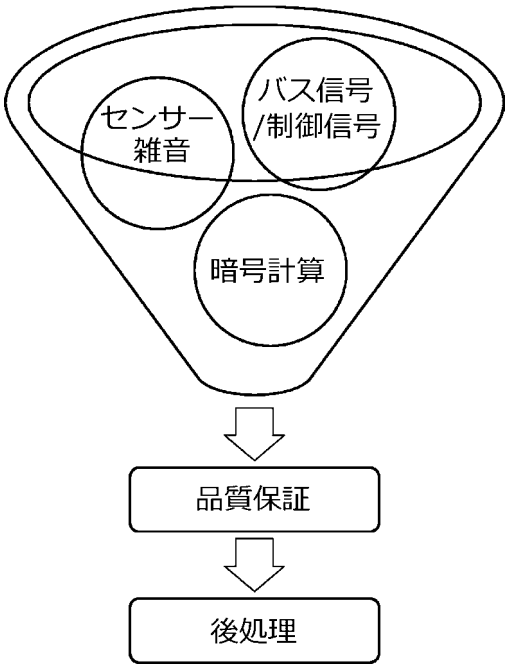
【図１】


1
3
ECU
ECU
4
2
ECU
ECU
5
...
10
エントロピープール
7
ECU
6

【図２】


3
3.10
3.1
4
4.10
4.1
4.2
1
3.11
2
2.1
2.10
5
5.2
エントロピーエージェント
乱数収集部
ECU
a1
a2
a3
b1
b2
10
7.5
7.50
7.51
7.40
a5
a4
集約コンポーネント
メモリユニット
分配コンポーネント
エントロピープール
7.1
7.2
7.3
7.4
7
6

【図３】


センサー雑音
バス信号/制御信号
暗号計算
品質保証
後処理

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/079862

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/58 H04W4/48
ADD.

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 H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/301803 A1 (BOENISCH VOLKER [DE] ET AL) 22 October 2015 (2015-10-22) paragraph [0026] - paragraph [0030] paragraph [0046] - paragraph [0065] -----	1-20
A	US 8 015 224 B1 (CHAICHANAVONG PANU [US] ET AL) 6 September 2011 (2011-09-06) column 6, line 1 - line 59 column 8, line 1 - line 40 -----	1-20
A	US 2009/323967 A1 (PEIRCE KENNETH L [US] ET AL) 31 December 2009 (2009-12-31) paragraph [0035] - paragraph [0041] -----	1-20

☐ 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
5 February 2018	16/02/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Tenbieg, Christoph

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/079862

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015301803 A1	22-10-2015	US 2015301803 A1	22-10-2015
		US 2016077804 A1	17-03-2016
US 8015224 B1	06-09-2011	NONE	
US 2009323967 A1	31-12-2009	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/079862

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F7/58 H04W4/48
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H04W

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2015/301803 A1 (BOENISCH VOLKER [DE] ET AL) 22. Oktober 2015 (2015-10-22) Absatz [0026] - Absatz [0030] Absatz [0046] - Absatz [0065] -----	1-20
A	US 8 015 224 B1 (CHAICHANAVONG PANU [US] ET AL) 6. September 2011 (2011-09-06) Spalte 6, Zeile 1 - Zeile 59 Spalte 8, Zeile 1 - Zeile 40 -----	1-20
A	US 2009/323967 A1 (PEIRCE KENNETH L [US] ET AL) 31. Dezember 2009 (2009-12-31) Absatz [0035] - Absatz [0041] -----	1-20

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
5. Februar 2018	16/02/2018

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Tenbieg, Christoph

2

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/079862

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2015301803 A1	22-10-2015	US 2015301803 A1	22-10-2015
		US 2016077804 A1	17-03-2016
US 8015224 B1	06-09-2011	KEINE	
US 2009323967 A1	31-12-2009	KEINE	

フロントページの続き

(81)指定国・地域　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,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,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

(72)発明者　フェルバー・ペーター
ドイツ連邦共和国、６４２８９　ダルムシュタット、レーンリング、１３０
(72)発明者　ユンク・ベルンハルト
ドイツ連邦共和国、８９０７５　ウルム、ヴェルデンベルクヴェーク、１６
(72)発明者　シュテッティンガー・マルク・ゼバスティアン・パトリック
ドイツ連邦共和国、６５３７５　エーストリッヒ－ヴィンケル、ゲンスバウムストラーセ、４