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

特許第4917478号
(P4917478)

(45)発行日　平成24年4月18日(2012.4.18)　(24)登録日　平成24年2月3日(2012.2.3)

(51)Int.Cl.			F I		
G06F	7/58	(2006.01)	G06F	7/58	A
G09C	1/00	(2006.01)	G09C	1/00	650B
H03K	3/84	(2006.01)	H03K	3/84	Z
B60R	25/04	(2006.01)	B60R	25/04	602

請求項の数 8　(全 14 頁)

(21)出願番号　特願2007-139199 (P2007-139199)
(22)出願日　平成19年5月25日 (2007.5.25)
(65)公開番号　特開2008-293339 (P2008-293339A)
(43)公開日　平成20年12月4日 (2008.12.4)
審査請求日　平成22年3月5日 (2010.3.5)

(73)特許権者　000141901
株式会社ケーヒン
東京都新宿区西新宿一丁目２６番２号
(73)特許権者　000005326
本田技研工業株式会社
東京都港区南青山二丁目１番１号
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100108578
弁理士　高橋　詔男
(74)代理人　100101465
弁理士　青山　正和
(74)代理人　100094400
弁理士　鈴木　三義

最終頁に続く

(54)【発明の名称】乱数発生装置及び車両制御装置

(57)【特許請求の範囲】
【請求項１】
過去に発生した乱数を基に新たな乱数を発生する第１乱数発生部を備え、当該第１乱数発生部が発生した乱数を外部に出力する乱数発生装置において、
前記第１乱数発生部が発生する乱数とは異なる乱数を発生する第２乱数発生部と、
電源供給が開始されてから最初の乱数を発生する場合に、前記第１乱数発生部が発生する乱数に対して前記第２乱数発生部が発生する乱数を用いた所定の演算を行い、当該演算により得られた乱数を外部に出力する演算部と
を備えることを特徴とする乱数発生装置。
【請求項２】
電源が供給されている間のみ前記第１乱数発生部が発生した乱数を記憶する揮発性メモリを備え、
前記第１乱数発生部は、前記揮発性メモリに記憶された乱数を基に新たな乱数を発生し、且つ発生した当該乱数を前記揮発性メモリに記憶させる
ことを特徴とする請求項１記載の乱数発生装置。
【請求項３】
電源供給が停止されても前記第２乱数発生部が発生した乱数を記憶することができる不揮発性メモリを備え、
前記第２乱数発生部は、前記第１乱数発生部の乱数発生法とは異なる乱数発生法で、前記不揮発性メモリに記憶された乱数を基に新たな乱数を発生する

ことを特徴とする請求項２記載の乱数発生装置。
【請求項４】
前記第２乱数発生部は、電源供給が開始されてから最初の乱数を発生する場合にのみ新たな乱数を発生し、且つ発生した当該乱数を前記不揮発性メモリに記憶させることを特徴とする請求項３記載の乱数発生装置。
【請求項５】
前記第２乱数発生部は、前記不揮発性メモリに記憶された乱数を基に、線形合同法により新たな乱数を発生することを特徴とする請求項４記載の乱数発生装置。
【請求項６】
前記第２乱数発生部が発生した乱数を前記不揮発性メモリに記憶させるのに要する時間に応じた乱数を発生する第３乱数発生部を備え、
前記演算部は、前記第２乱数発生部が発生する乱数に加えて前記第３乱数発生部が発生する乱数を用いた所定の演算を、前記第１乱数発生部が発生する乱数に対して行う
ことを特徴とする請求項４又は請求項５記載の乱数発生装置。
【請求項７】
ユーザが所持するキーに登録された識別コードと車両に予め登録された識別コードとの照合結果に基づいて、車両に関する所定の制御を行う車両制御装置において、
前記車両に設けられるバッテリから電源供給がなされる請求項１から請求項６の何れか一項に記載の乱数発生装置を備えており、前記キーの識別コード及び前記車両の識別コードを暗号化するために前記乱数発生装置が発生した乱数を用いることを特徴とする車両制御装置。
【請求項８】
前記車両に関する所定の制御は、前記車両に設けられたエンジンの始動制御であり、
前記乱数発生装置は、前記バッテリからの電源供給が開始された後の最初のエンジン始動指示があった場合に、最初の乱数を発生することを特徴とする請求項７記載の車両制御装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、過去に発生した乱数を基に新たな乱数を発生する乱数発生装置、及び当該乱数発生装置を備える車両制御装置に関する。
【背景技術】
【０００２】
近年、車両の盗難を防止するため、或いはユーザの利便性を向上するために、ユーザにより携帯されるキー（例えば、イグニッションキー）に登録されたＩＤコード（識別コード）と、予め車両側に登録されたＩＤコードとの照合結果に基づいて、エンジンの始動制御、錠の開閉制御、その他の車両に関する各種制御を行う車両制御装置が一般化している。この車両制御装置は、キーに登録されているＩＤコードの漏洩を防止しつつ両ＩＤコードの照合を可能にするため、キーに登録されたＩＤコードと車両側に登録されたＩＤコードとを暗号化するための乱数を発生する乱数発生装置を備えている。
【０００３】
以下の特許文献１には、前回発生した乱数をバックアップＲＡＭ（Random Access Memory）に一時書き込み、この書き込んだ乱数を用いて新たな乱数を生成する乱数発生装置の一例が開示されている。この乱数発生装置は、過去に発生した乱数の全てが消去されるのを防止するため、乱数の演算回数が所定値に達したら、その時の乱数をＥＥＰＲＯＭ（Electronically Erasable and Programmable Read Only Memory）等の不揮発性メモリに書き込み、バックアップＲＡＭの異常時には不揮発性メモリに書き込まれた乱数の前回値を基に今回の乱数を発生している。
【特許文献１】特許第３４９６５４７号公報
【発明の開示】

【発明が解決しようとする課題】
【０００４】
ところで、バッテリの取り外し等によりバッテリからの電源供給が停止した場合（バッテリキャンセルが行われた場合）には、乱数発生の規則性が解析しやすい状態になり、セキュリティ性が低下する虞がある。例えば、上記の特許文献１に開示された技術においては、バッテリキャンセルが行われた場合には不揮発性メモリに書き込まれた乱数を用いて新たな乱数を発生させているところ、不揮発性メモリに既に書き込まれている乱数の更新が生じない時間間隔でバッテリキャンセルを繰り返せば、理論上は乱数の発生規則が解析可能であるとも考えられる。実際上は、乱数の発生規則を解析するのは極めて困難であり、ＩＤコードの漏洩が生ずる可能性は極めて低いが、セキュリティ性が高いことに越したことはない。
【０００５】
また、ＥＥＰＲＯＭ等の不揮発性メモリは書き換え回数に制限があるという問題がある。上記の特許文献１では、乱数の演算回数が所定値に達した場合にのみ不揮発性メモリへの書き込みを行うことにより不揮発性メモリへの書き換え回数を低減しているが、販売されてしまった車両の使用年数は様々であり、長期に亘って使用される場合には予め予定された不揮発性メモリの書き換え回数を越えて書き換えが行われる可能性も考えられる。ここで、不揮発性メモリの書き換えが不可能になった場合であって、バックアップメモリにも異常が生じた場合を想定すると、同じ乱数が作成されることが考えられ、これによりセキュリティ性が低下する虞がある。このように、従来はセキュリティ性の低下を防止する観点からは対策が十分ではあるとはいえず、十分な対策を行う必要がある。
【０００６】
本発明は上記事情に鑑みてなされたものであり、セキュリティ性を向上させることを主たる目的とし、加えて不揮発性メモリの書き換え回数を低減することができる乱数発生装置、及び当該乱数発生装置を備える車両制御装置を提供することを目的とする。
【課題を解決するための手段】
【０００７】
上記課題を解決するために、本発明の乱数発生装置は、過去に発生した乱数を基に新たな乱数を発生する第１乱数発生部（２１）を備え、当該第１乱数発生部が発生した乱数を外部に出力する乱数発生装置において、前記第１乱数発生部が発生する乱数とは異なる乱数を発生する第２乱数発生部（２２）と、電源供給が開始されてから最初の乱数を発生する場合に、前記第１乱数発生部が発生する乱数に対して前記第２乱数発生部が発生する乱数を用いた所定の演算を行い、当該演算により得られた乱数を外部に出力する演算部（２３）とを備えることを特徴とする。
この発明によると、電源供給が開始されてから最初の乱数を発生させる場合に、第１乱数発生部で発生した乱数に対し、第２乱数発生部で発生した乱数を用いた所定の演算が行われ、この演算により得られた乱数が外部に出力される。
また、本発明の乱数発生装置は、電源が供給されている間のみ前記第１乱数発生部が発生した乱数を記憶する揮発性メモリ（１３）を備え、前記第１乱数発生部は、前記揮発性メモリに記憶された乱数を基に新たな乱数を発生し、且つ発生した当該乱数を前記揮発性メモリに記憶させることを特徴としている。
また、本発明の乱数発生装置は、電源供給が停止されても前記第２乱数発生部が発生した乱数を記憶することができる不揮発性メモリ（１５）を備え、前記第２乱数発生部は、前記第１乱数発生部の乱数発生法とは異なる乱数発生法で、前記不揮発性メモリに記憶された乱数を基に新たな乱数を発生することを特徴としている。
また、本発明の乱数発生装置は、前記第２乱数発生部が、電源供給が開始されてから最初の乱数を発生する場合にのみ新たな乱数を発生し、且つ発生した当該乱数を前記不揮発性メモリに記憶させることを特徴としている。
また、本発明の乱数発生装置は、前記第２乱数発生部が、前記不揮発性メモリに記憶された乱数を基に、線形合同法により新たな乱数を発生することを特徴としている。

また、本発明の乱数発生装置は、前記第２乱数発生部が発生した乱数を前記不揮発性メモリに記憶させるのに要する時間に応じた乱数を発生する第３乱数発生部（２５）を備え、前記演算部は、前記第２乱数発生部が発生する乱数に加えて前記第３乱数発生部が発生する乱数を用いた所定の演算を、前記第１乱数発生部が発生する乱数に対して行うことを特徴としている。

本発明の車両制御装置は、ユーザが所持するキー（Ｋ）に登録された識別コード（Ｃ１）と車両に予め登録された識別コード（Ｃ２）との照合結果に基づいて、車両に関する所定の制御を行う車両制御装置（１）において、前記車両に設けられるバッテリから電源供給がなされる上記の何れかに記載の乱数発生装置を備えており、前記キーの識別コード及び前記車両の識別コードを暗号化するために前記乱数発生装置が発生した乱数を用いることを特徴としている。

また、本発明の車両制御装置は、前記車両に関する所定の制御が、前記車両に設けられたエンジンの始動制御であり、前記乱数発生装置は、前記バッテリからの電源供給が開始された後の最初のエンジン始動指示があった場合に、最初の乱数を発生することを特徴としている。

【発明の効果】

【０００８】

本発明によれば、電源供給が開始されてから最初の乱数を発生させる場合に、第１乱数発生部で発生した乱数に対し、第２乱数発生部で発生した乱数を用いた所定の演算を行って得られた乱数を外部に出力しているため、例えば電源供給が再開された時に同じ乱数が発生するといった事態を防止することができ、この結果としてセキュリティ性を向上させることができる。

また、不揮発性メモリに対する乱数の書き込みは、電源供給が開始されてから最初の乱数を発生する場合にのみ行っているため、不揮発性メモリの書き換え回数を極めて低減することができる。

【発明を実施するための最良の形態】

【０００９】

以下、図面を参照して本発明の実施形態による乱数発生装置及び車両制御装置について詳細に説明する。

【００１０】

〔第１実施形態〕

図１は、本発明の第１実施形態による乱数発生装置及び車両制御装置の要部構成を示すブロック図である。尚、図１においては、本発明の第１実施形態による車両制御装置としての車両制御ユニット１に加えて、イモビユニット２、スイッチ群３、センサ群４、インジェクタ５、点火装置６、及びバッテリ７も併せて図示しており、これらの各ブロックは車両に搭載される。まず、図１に示すこれらの各ブロックについて概説する。

【００１１】

車両制御ユニット１は、ユーザが所持するイグニッションキーＫに登録されたＩＤコード（識別コード）Ｃ１と車両に予め登録されたＩＤコードＣ２との照合結果に基づいて、エンジン（図示省略）の始動制御等の各種制御を行う。尚、本実施形態では、上記のＩＤコードＣ２は、車両制御ユニット１が備えるＥＥＰＲＯＭ１５に記憶されている。イモビユニット２は、イグニッションキーＫのＩＤコードＣ１を読み取る読取装置Ｒが設けられたキーシリンダＫＣと、読取装置Ｒで読み取られたＩＤコードＣ１を暗号化する暗号化装置ＥＤとを備えており、イグニッションキーＫに登録されたＩＤコードＣ１を読み取って車両制御ユニット１から送信される乱数を用いて暗号化を行い、暗号化したＩＤコード（以下、セキュリティ解除コードＣ１１という）を車両制御ユニット１に送信する。

【００１２】

スイッチ群３は、例えばブレーキスイッチやサイドスタンドスイッチ等のエンジン制御に係る各種スイッチを備えている。また、センサ群４は、例えば水温センサ、吸気管圧センサ、ブレーキセンサ、及び大気圧センサ等のエンジン制御に係る各種センサを備えてい

る。インジェクタ５及び点火装置６は車両のエンジンに設けられており、車両制御ユニット１の制御の下で燃料噴射や点火を実行する。バッテリ７は、図１に示す車両制御ユニット１及びイモビユニット２に直流電源を供給するとともに、不図示のスタータ等にも直流電源を供給する。

【００１３】

次に、車両制御ユニット１について詳細に説明する。図１に示す通り、車両制御ユニット１は、ＣＰＵ（中央処理装置）１１、ＲＡＭ１２、バックアップＲＡＭ１３（揮発性メモリ）、ＲＯＭ１４、ＥＥＰＲＯＭ１５（不揮発性メモリ）、通信インターフェイス（Ｉ／Ｆ）回路１６、入力Ｉ／Ｆ回路１７、Ａ／Ｄ変換器１８、出力Ｉ／Ｆ回路１９、及び電源監視回路２０を備えており、これらはバスＢ１を介して相互に接続されている。尚、上記のＣＰＵ１１、バックアップＲＡＭ１３、ＥＥＰＲＯＭ１５、及びバスＢ１から、本発明の第１実施形態による乱数発生装置が構成されている。

【００１４】

ＣＰＵ１１は、ＲＯＭ１４に記憶された各種制御プログラムを実行して車両制御ユニット１の動作を統括して制御する。具体的には、スイッチ群３の状態やセンサ群４の検出結果に応じて、インジェクタ５による燃料噴射や点火装置６による点火を制御する。また、ＣＰＵ１１は、イグニッションキーＫに登録されたＩＤコードＣ１と車両に予め登録されたＩＤコードＣ２とを暗号化するために用いる乱数を発生するとともに、イモビユニット２から送信される暗号化されたＩＤコードＣ１（セキュリティ解除コードＣ１１）と、暗号化されたＩＤコードＣ２（以下、照合コードＣ１２という）との照合を行い、その照合結果に基づいて、インジェクタ５による燃料噴射や点火装置６による点火を制御することにより、エンジンの始動制御を行う。

【００１５】

図１に示す通り、ＣＰＵ１１がＲＯＭ１４に記憶された制御プログラムを実行することにより、ＣＰＵ１１には第１乱数発生部２１、第２乱数発生部２２、演算部２３、及び暗号化部２４が実現される。第１乱数発生部２１は、バックアップＲＡＭ１３に記憶された過去の乱数を基に新たな乱数を発生する。例えば、第１乱数発生部２１は、所定時間（例えば、１０ｍｓｅｃ）を計時する優先度の低いタイマ（フリーランタイマ）を実行させ、計時された時間（乱数値）をバックアップＲＡＭ１３に記憶された過去の乱数に加算して新たな乱数を発生する。ここで、フリーランタイマは優先度が低いため、その起動タイミングは優先度が高い他の処理の処理タイミングに依存してばらつく。第１乱数発生部２１は、フリーランタイマの起動タイミングのばらつきを利用して乱数を発生するものである。

【００１６】

第２乱数発生部２２は、ＥＥＰＲＯＭ１５に記憶された過去の乱数を基に、第１乱数発生部２１が発生する乱数とは異なる新たな乱数を発生する。例えば、第２乱数発生部２２は線形合同法により新たな乱数を発生する。ここで、線形合同法とは、以下の（１）式で表すことができる乱数発生法である。

$$X_n = (A \cdot X_{n-1} + B) \bmod M \quad \cdots\cdots (1)$$

【００１７】

上記（１）式において、右辺中のX_{n-1}は前回発生した（過去に発生した）乱数であり、左辺のX_nは今回発生する新たな乱数である。また、右辺中のＡ，Ｂ，Ｍは、０＜Ａ＜Ｍ，０＜Ｂ＜Ｍなる関係が満たされる任意の定数である。尚、変数ｎは１以上の整数である。上記（１）式から、新たな乱数X_nは、前回の乱数X_{n-1}に定数Ａを乗算した上で定数Ｂを加算して得られる値に対して定数Ｍの剰余演算（mod）を行うことにより求められることが分かる。

【００１８】

演算部２３は、バッテリ７からの電源供給が開始されてから最初の乱数を発生する場合に、第１乱数発生部２１が発生する乱数に対して第２乱数発生部２２が発生する乱数を用いた所定の演算を行う。演算部２３が行う演算としては、加算、減算、乗算、除算、所定

の多項式を用いた演算、高次関数を用いた演算、その他の任意の演算を用いることができる。演算部２３を用いて上記の演算を行うのはセキュリティ性を向上させるためである。つまり、バッテリ７からの電源供給が開始された直後には同じ乱数が作成されることが考えられ、或いは乱数発生の規則性が解析しやすい状態になるため、２種類の乱数を発生させて所定の演算を施すことで、第三者による乱数の解析を困難にしてセキュリティ性の向上を図っている。尚、以下では、説明を簡単にするために、演算部２３は、第１乱数発生部２１で発生した乱数と第２乱数発生部２２で発生した乱数とを加算する演算を行う場合を例に挙げて説明する。

【００１９】

暗号化部２４は、暗号化装置ＥＤが行う暗号化アルゴリズムと同じ暗号化アルゴリズムにより、第１乱数発生部２１が発生した乱数又は演算部２３が出力する乱数を用いてＥＥＰＲＯＭ１５に記憶されたＩＤコード１５の暗号化を行う。ＣＰＵ１１は、イモビユニット２から送信されてくるセキュリティ解除コードＣ１１と、暗号化部２４から出力される照合コードＣ１２とを照合し、両者が一致した場合にインジェクタ５による燃料噴射や点火装置６による点火を制御することにより、エンジンの始動制御を行う。

【００２０】

ＲＡＭ１２は、バッテリ７からの電源供給が行われている間のみ記憶内容を保持することができる揮発性メモリであり、ＣＰＵ１１の各種演算結果や車両制御に用いられる各種制御情報を一時的に記憶する。尚、バッテリ７からＲＡＭ１２に対する電源供給は、イグニッションキーＫがキーシリンダＫＣに差し込まれてキースイッチ（図示省略）がオン状態になっている間に行われ、キースイッチがオフ状態になると停止する。

【００２１】

バックアップＲＡＭ１３は、第１乱数発生部２１が発生した乱数を記憶する。このバックアップＲＡＭ１３は、ＲＡＭ１２と同様の揮発性メモリであるが、ＲＡＭ１２とは異なりバッテリ７からの電源が常時供給されている。つまり、上記のキースイッチがオン状態であるかオフ状態であるかに拘わらずバックアップＲＡＭ１３にはバッテリ７から電源が供給され続けて記憶内容が保持されるが、バッテリキャンセルが行われた場合にはバックアップＲＡＭ１３に対する電源供給が停止して記憶内容が消去される。

【００２２】

ＲＯＭ１４は、ＣＰＵ１１によって実行される各種制御プログラム等を記憶する。ＥＥＰＲＯＭ１５は、車両に予め登録されたＩＤコードＣ２及び第２乱数発生部２２が発生した乱数を記憶する。このＥＥＰＲＯＭ１５は、バッテリ７からの電源供給が停止されても記憶内容を保持することができる不揮発性メモリであって、その記憶内容の消去又は書き換えを部分的に行うことができるメモリである。つまり、ＥＥＰＲＯＭ１５の一部の記憶領域に書き込まれたＩＤコードＣ２の消去を伴わずに、他の領域に対して第２乱数発生部２２が発生した乱数の書き込み、消去、及び書き換えを行うことができる。

【００２３】

通信Ｉ／Ｆ回路１６は、イモビユニット２との間で通信を行い、イモビユニット２から送信されてくる乱数要求信号をＣＰＵ１１に出力するとともに、第１乱数発生部２１が発生した乱数又は演算部２３が出力する乱数をイモビユニット２に送信する。また、イモビユニット２から送信されてくるセキュリティ解除コードＣ１１もＣＰＵ１１に出力する。入力Ｉ／Ｆ回路１７は、スイッチ群３が備える各種スイッチのオン状態・オフ状態を示す信号をＣＰＵ１１に出力する。Ａ／Ｄ変換器１８は、センサ群４が備える各種センサの検出結果を示す信号をディジタル信号に変換してＣＰＵ１１に出力する。

【００２４】

出力Ｉ／Ｆ回路１９は、ＣＰＵ１１から出力される燃料噴射及び点火の制御信号を、インジェクタ５及び点火装置６に対してそれぞれ出力する。電源監視回路２０は、バッテリ７から供給される電源電圧の変化を監視し、その監視結果を示す信号をＣＰＵ１１に出力する。例えば、バッテリキャンセル後に再度電源供給が行われた場合には、電源監視回路２０は、ユーザによるエンジン始動指示がなされるまでの間、ＣＰＵ１１に対してリセッ

ト信号を出力する。このリセット信号によりＣＰＵ１１の初期化が行われるため、電源供給再開時のＣＰＵ１１の異常動作を防止することができる。ここで、リセット信号は、ユーザによってバッテリキャンセル後に最初のエンジン始動指示が行われた直後に解除される。このため、ＣＰＵ１１は、エンジン始動指示があった時点においてリセット信号が入力されているか否かに基づいて、バッテリキャンセル後に最初のエンジン始動指示が行われたことを知ることができる。

【００２５】

次に、本発明の第１実施形態による乱数発生装置及び車両制御装置で行われる処理について説明する。図２は本発明の第１実施形態による車両制御装置の処理を示すフローチャートであり、図３は本発明の第１実施形態による乱数発生装置の処理を示すフローチャートである。尚、以下の説明では、バッテリキャンセルが行われていない通常時の動作と、バッテリキャンセルが行われた時の動作とを分けて順次説明する。尚、図２のフローチャートに示す処理は、ユーザがイグニッションキーＫをキーシリンダＫＣに差し込んでイグニッションキーＫを捻ってエンジン始動指示を行い、イグニッションスイッチ（図示省略）がオンになること（イグニッションオン）により開始される。

【００２６】

［通常時の動作］

イグニッションスイッチがオンになると、その旨を示す信号がイモビユニット２から車両制御ユニット１に送信される。この信号を受信すると、車両制御ユニット１のＣＰＵ１１は、まずバッテリキャンセルからのイグニッションオンであるか否かを判断する（ステップＳ１０）。バッテリキャンセルが行われていない通常時においては、電源監視回路２０からリセット信号が出力されることはない。このため、ステップＳ１０の判断結果は「ＮＯ」となり、通常時の乱数発生処理が行われる（ステップＳ１１）。

【００２７】

通常時の乱数発生処理では、図３（ａ）に示す通り、まず第１乱数発生部２１がバックアップＲＡＭ１３に記憶されている前回発生した乱数R_{i-1}を読み出す（ステップＳ２１）。尚、変数ｉは１以上の整数である。次に、第１乱数発生部２１は、読み出した前回の乱数R_{i-1}を用いて新たな乱数R_iを演算する。具体的には、所定時間（例えば、１０ｍｓｅｃ）を計時する優先度の低いフリーランタイマを実行させて乱数値R_tを取得し、この乱数値R_tを前回の乱数R_{i-1}に加算して新たな乱数R_iを求める。（ステップＳ２２）。そして、ステップＳ２２で求めた新たな乱数R_iをバックアップＲＡＭ１３に書き込む（ステップＳ２３）。以上の処理により、通常時の乱数発生処理が終了する。

【００２８】

通常の乱数発生処理が終了すると、ＣＰＵ１１はイモビユニット２から送信される乱数の送信要求信号を受信する（ステップＳ１２）。尚、この乱数の送信要求信号は、イグニッションオンがされた後に所定時間（例えば、数秒）が経過するまでの間、イモビユニット２が車両制御ユニット１に対して定期的に送信する。ＣＰＵ１１は、イモビユニット２からの乱数の送信要求信号を受信すると、その返信としてステップＳ１１で求めた新たな乱数R_iをイモビユニット２へ送信する（ステップＳ１３）。

【００２９】

車両制御ユニット１からの乱数R_iを受信すると、イモビユニット２は乱数R_iを暗号化装置ＥＤに受け渡し、読取装置Ｒで読み取られたイグニッションキーＫのＩＤコードＣ１を乱数R_iを用いて暗号化させる。これにより、セキュリティ解除コードＣ１１が生成される。生成されたセキュリティ解除コードＣ１１は、イモビユニット２から車両制御ユニット１に送信され、ＣＰＵ１１で受信される（ステップＳ１４）。ここで、セキュリティ解除コードＣ１１は乱数R_iを用いて暗号化されるため、第三者によるＩＤコードＣ１の盗用が防止される。

【００３０】

セキュリティ解除コードＣ１１を受信すると、ＣＰＵ１１の暗号化部２４は、ＥＥＰＲＯＭ１５からＩＤコードＣ２を読み出し、ステップＳ１１で求められた乱数R_iを用いて

ＩＤコードＣ２を暗号化する。これにより、照合コードＣ１２が生成される（ステップＳ１５）。以上の処理が終了すると、ＣＰＵ１１は、ステップＳ１４で受信したセキュリティ解除コードＣ１１と、ステップＳ１５で生成された照合コードＣ１２とを照合し、両者が一致するか否かの判断を行う（ステップＳ１６）。

【００３１】

この照合の結果、セキュリティ解除コードＣ１１と照合コードＣ１２とが不一致であると判断した場合（判断結果が「ＮＯ」の場合）には、ＣＰＵ１１は点火・燃料噴射を禁止する。即ち、ＣＰＵ１１は、インジェクタ５及び点火装置６に対する制御信号を出力しない（ステップＳ１７）。これに対し、セキュリティ解除コードＣ１１と照合コードＣ１２とが一致すると判断した場合（判断結果が「ＹＥＳ」の場合）には、ＣＰＵ１１は、点火・燃料噴射を許可する。即ち、ＣＰＵ１１は、燃料噴射及び点火の制御信号をインジェクタ５及び点火装置６に対してそれぞれ出力して、エンジンを始動させる（ステップＳ１８）。このようにして、エンジンの始動制御が行われる。

【００３２】

［バッテリキャンセル時の動作］

バッテリキャンセルが行われた後でバッテリ７からの電源供給が再開されると、電源監視回路２０からＣＰＵ１１に対してリセット信号が継続して出力される。この状態で、イグニッションスイッチがオンになると、その旨を示す信号がイモビユニット２から車両制御ユニット１に送信される。この信号を受信すると、車両制御ユニット１のＣＰＵ１１は、まずバッテリキャンセルからのイグニッションオンであるか否かを判断する（ステップＳ１０）。

【００３３】

ここで、イグニッションスイッチがオンになった時点においては、電源監視回路２０からのリセット信号が出力されているため、ＣＰＵ１１がバッテリキャンセルからのイグニッションオンであると判断してステップＳ１０の判断結果が「ＹＥＳ」となり、バッテリキャンセル時の乱数発生処理が行われる（ステップＳ１９）。このステップＳ１９の処理は、バッテリ７からの電源供給が開始（再開）されてから、最初の乱数を発生させる処理である。尚、イグニッションスイッチがオンになった直後に電源監視回路２０からのリセット信号は解除される。

【００３４】

バッテリキャンセル時の乱数発生処理では、図３（ｂ）に示す通り、まず第２乱数発生部２２がＥＥＰＲＯＭ１５に記憶されている前回値X_{i-1}を読み出す（ステップＳ３１）。尚、変数ｉは１以上の整数である。次に、第２乱数発生部２２は、読み出した前回値X_{i-1}を用いて線形合同法により新たな乱数X_iを演算する。具体的には、前述した（１）式を用いて、前回値X_{i-1}に所定の定数Ａを乗算した上で所定の定数Ｂを加算して得られる値に対して所定の定数Ｍを用いた剰余演算（mod）を行うことにより新たな乱数X_iを演算する（ステップＳ３２）。そして、ステップＳ３２で求めた新たな乱数X_iをＥＥＰＲＯＭ１５に書き込む（ステップＳ３３）。このように、第２乱数発生部２２は、バッテリキャンセルからのイグニッションオンの場合にのみ新たな乱数を発生し、且つ発生した乱数をＥＥＰＲＯＭ１５に書き込む。

【００３５】

以上の処理と並行して、第１乱数発生部２１は、所定時間（例えば、１０ｍｓｅｃ）を計時する優先度の低いフリーランタイマを実行させて乱数値R_tを取得する。そして、演算部２３は、ステップＳ３２において第２乱数発生部２２で求められた新たな乱数X_iと、第１乱数発生部２１が取得した乱数値R_tとを演算して新たな乱数R_iを生成する。具体的には、乱数X_iと乱数値R_tとを加算して新たな乱数R_iを生成する（ステップＳ３４）。以上の処理により、バッテリキャンセル時の乱数発生処理が終了する。

【００３６】

バッテリキャンセル時の乱数発生処理が終了すると、ＣＰＵ１１がイモビユニット２から送信される乱数の送信要求信号を受信し（ステップＳ１２）、その返信としてステップ

Ｓ１９で求めた新たな乱数$Ｒ_{i}$をイモビユニット２へ送信する（ステップＳ１３）。そして、イモビユニット２において、イグニッションキーＫから読み取られたＩＤコードＣ１が新たな乱数$Ｒ_{i}$を用いて暗号されてセキュリティ解除コードＣ１１が生成され、このセキュリティ解除コードＣ１１が車両制御ユニット１に送信されてＣＰＵ１１で受信される（ステップＳ１４）。

【００３７】

次に、ＣＰＵ１１の暗号化部２４は、ＥＥＰＲＯＭ１５からＩＤコードＣ２を読み出し、ステップＳ１９で求められた乱数$Ｒ_{i}$を用いてＩＤコードＣ２を暗号化する。これにより、照合コードＣ１２が生成される（ステップＳ１５）。そして、ステップＳ１４で受信したセキュリティ解除コードＣ１１と、ステップＳ１５で生成された照合コードＣ１２とが照合され（ステップＳ１６）、両者が不一致である場合には点火・燃料噴射が禁止され（ステップＳ１７）、両者が一致する場合には点火・燃料噴射が許可される（ステップＳ１８）。このようにして、エンジンの始動制御が行われる。

【００３８】

以上説明した通り、本発明の第１実施形態による乱数発生装置は、バッテリキャンセル後にバッテリ７からの電源供給が再開されてから最初の乱数を発生させる場合に、第１乱数発生部２１で乱数値$Ｒ_{t}$を取得するとともに第２乱数発生部２２で新たな乱数$Ｘ_{i}$を発生させ、演算部２３において乱数値$Ｒ_{t}$に対して乱数$Ｘ_{i}$を用いた所定の演算（加算）を行っているため、セキュリティ性を向上させることができる。また、ＥＥＰＲＯＭ１５に対する書き込みは、バッテリキャンセルからのイグニッションオンの場合にのみ行っているため、ＥＥＰＲＯＭ１５に対する書き換え回数を極めて低減することができる。本発明の第１実施形態による車両制御装置は、以上の乱数発生装置を備えるため、車両盗難防止効果を高めることができる。

【００３９】

〔第２実施形態〕

図４は、本発明の第２実施形態による乱数発生装置及び車両制御装置の要部構成を示すブロック図である。尚、図４においては、図１に示したイモビユニット２、スイッチ群３、センサ群４、インジェクタ５、点火装置６、及びバッテリ７の図示は省略している。前述した第１実施形態では、ＣＰＵ１１がＲＯＭ１４に記憶された制御プログラムを実行することにより、ＣＰＵ１１に第１乱数発生部２１、第２乱数発生部２２、演算部２３、及び暗号化部２４が実現されていたが、本実施形態ではこれらに加えて第３乱数発生部２５がＣＰＵ１１に実現される点が第１実施形態とは異なる。

【００４０】

第３乱数発生部２５は、第２乱数発生部２２が発生した乱数をＥＥＰＲＯＭ１５に書き込むのに要する時間に応じた乱数を発生する。具体的には、第３乱数発生部２５は、第１乱数発生部２１が起動するフリーランタイマと同様の優先度の低いフリーランタイマを起動しており、第２乱数発生部２２がＥＥＰＲＯＭ１５に対する書き込みを開始した時刻Ｔ１とＥＥＰＲＯＭ１５において書き込みが終了した時刻Ｔ２との差分を求めて乱数とする。ここで、ＥＥＰＲＯＭ１５の書き込みに要する時間は、ＥＥＰＲＯＭ１５の特性のばらつきや周囲の温度によって変化するため、乱数として用いるのに好都合である。

【００４１】

次に、本発明の第２実施形態による乱数発生装置及び車両制御装置で行われる処理について説明する。本実施形態の処理は、基本的には図２に示したフローチャートに従って実行される。但し、バッテリキャンセル時の処理（ステップＳ１９）が第１実施形態とは異なるため、以下ではバッテリキャンセル時の処理に着目して説明する。図５は、本発明の第２実施形態によるバッテリキャンセル時における乱数発生装置の処理を示すフローチャートである。

【００４２】

バッテリキャンセル時の乱数発生処理が開始されると、図５に示す通り、まず第２乱数発生部２２がＥＥＰＲＯＭ１５に記憶されている前回値$Ｘ_{i-1}$を読み出し（ステップＳ

４１）、読み出した前回値X_{i-1}を用いて線形合同法により新たな乱数X_iを演算する（ステップＳ４２）。次に、第２乱数発生部２２によってＥＥＰＲＯＭ１５に対する新たな乱数X_iの書き込み指示がなされると、第３乱数発生部２５がフリーランタイマの値Ｔ１を読み込む（ステップＳ４３）。そして、上記の書き込み指示に従って、ステップＳ４２で求められた新たな乱数X_iがＥＥＰＲＯＭ１５に書き込まれる（ステップＳ４４）。

【００４３】

書き込み処理が終了すると、第３乱数発生部２５がフリーランタイマの値Ｔ２を読み込み（ステップＳ４５）、ＥＥＰＲＯＭ１５の書き込み時間Ｔを算出する。つまり、ステップＳ４５で読み込んだ値Ｔ２からステップＳ４３で読み込んだ値Ｔ１を減算することにより、ＥＥＰＲＯＭ１５の書き込み時間Ｔを求める。尚、以上の処理と並行して、第１乱数発生部２１は、所定時間（例えば、１０ｍｓｅｃ）を計時する優先度の低いフリーランタイマを実行させて乱数値R_tを取得する。

【００４４】

以上の処理が終了すると、演算部２３は、ステップＳ３２において第２乱数発生部２２で求められた新たな乱数X_iと、第１乱数発生部２１が取得した乱数値R_tと、ステップＳ４６で求められたＥＥＰＲＯＭ１５の書き込み時間Ｔとを演算して新たな乱数R_iを生成する。具体的には、乱数X_i、乱数値R_t、及び書き込み時間Ｔを加算して新たな乱数R_iを生成する（ステップＳ４７）。以上の処理により、バッテリキャンセル時の乱数発生処理が終了する。

【００４５】

以上説明した通り、本発明の第２実施形態による乱数発生装置は、バッテリキャンセル後にバッテリ７からの電源供給が再開されてから最初の乱数を発生させる場合に、第１乱数発生部２１で乱数値R_tを取得するとともに第２乱数発生部２２で新たな乱数X_iを発生させ、且つＥＥＰＲＯＭ１５に対する乱数X_iの書き込み時間Ｔを求め、演算部２３において乱数値R_tに対して乱数X_i及び書き込み時間Ｔを用いた所定の演算（加算）を行っているため、第１実施形態よりもセキュリティ性を向上させることができる。また、ＥＥＰＲＯＭ１５に対する書き込みは、第１実施形態と同様に、バッテリキャンセルからのイグニッションオンの場合にのみ行っているため、ＥＥＰＲＯＭ１５に対する書き換え回数を極めて低減することができる。本発明の第２実施形態による車両制御装置は、以上の乱数発生装置を備えるため、車両盗難防止効果をより高めることができる。

【００４６】

以上、本発明の実施形態による乱数発生装置及び車両制御装置について説明したが、本発明は上述した実施形態に制限されることなく、本発明の範囲内で自由に変更が可能である。例えば、上記実施形態における第１乱数発生部２１は、優先度の低いフリーランタイマを利用して得られた乱数値とバックアップＲＡＭ１３に記憶された過去の乱数とから新たな乱数を発生させるものであった。しかしながら、第１乱数発生部２１は、各種の合同法（線形合同法、混合合同法、累積合同法、加法合同法）や平方採中法を用いて乱数（疑似乱数）を発生させるものであっても良い。

【００４７】

また、第２乱数発生部２２は、ＥＥＰＲＯＭ１５に記憶された過去の乱数を基に新たな乱数を発生させるものであった。しかしながら、第２乱数発生部２２は、ＥＥＰＲＯＭ１５の過去の乱数を用いずに、第１乱数発生部２１のフリーランタイマの計時結果から乱数を発生させるものであっても良い。また、上記実施形態においては、第２乱数発生部２２が線形合同法を用いて乱数を発生する場合を例に挙げて説明したが、乱数発生法としては、線形合同法以外に、各種の合同法（混合合同法、累積合同法、加法合同法）や平方採中法を用いることも可能である。

【００４８】

また、第２乱数発生部２２が発生する乱数が第１乱数発生部２１が発生する乱数と異なっていれば、第２乱数発生部２２で使用される乱数発生法は、第１乱数発生部２１で使用される乱数発生法と同じであって良い。例えば、第１乱数発生部２１と第２乱数発生部２

２との双方で線形合同法を用いても良い。第１乱数発生部２１と第２乱数発生部２２との双方で線形合同法を用いる場合には、前述した（１）式中の定数Ａ，Ｂ，Ｍを第１乱数発生部２１及び第２乱数発生部２２の各々で異ならせれば良い。これにより、第１乱数発生部２１が発生する乱数と第２乱数発生部２２が発生する乱数とを異ならせることができる。

【００４９】

更に、上記実施形態では、車両制御ユニット１がエンジンの始動制御を行うものである場合を例に挙げてて説明したが、本発明の車両制御ユニットは、エンジンの始動制御以外に、錠の開閉制御、その他の車両に関する各種制御を行うものである場合にも適用が可能である。また、上記実施形態では、キーシリンダＫＣに差し込まれたイグニッションキーＫからＩＤコードＣ１を読み取る場合を例に挙げたが、キーに登録されたＩＤコードを電波にて飛ばす形態の場合にも適用が可能である。かかる形態の場合には、キーとの間で電波にて通信を行う通信装置をイモビユニットに設け、車両制御ユニット１からイモビユニット２に送信される乱数を電波にてキーに送信し、キーで作成されて電波にて返信されるセキュリティ解除コードをイモビユニットが受信して車両制御ユニット１に送信するようにすればよい。

【００５０】

また更に、上記実施形態では、ＣＰＵ１１がＲＯＭ１４に記憶された制御プログラムを実行することにより、ＣＰＵ１１には第１乱数発生部２１、第２乱数発生部２２、演算部２３、暗号化部２４、第３乱数発生部２５を実現する場合を例に挙げて説明した。しかしながら、これら各部は電子回路によりハードウェア的に構成されていても良い。

【図面の簡単な説明】

【００５１】

【図１】本発明の第１実施形態による乱数発生装置及び車両制御装置の要部構成を示すブロック図である。

【図２】本発明の第１実施形態による車両制御装置の処理を示すフローチャートである。

【図３】本発明の第１実施形態による乱数発生装置の処理を示すフローチャートである。

【図４】本発明の第２実施形態による乱数発生装置及び車両制御装置の要部構成を示すブロック図である。

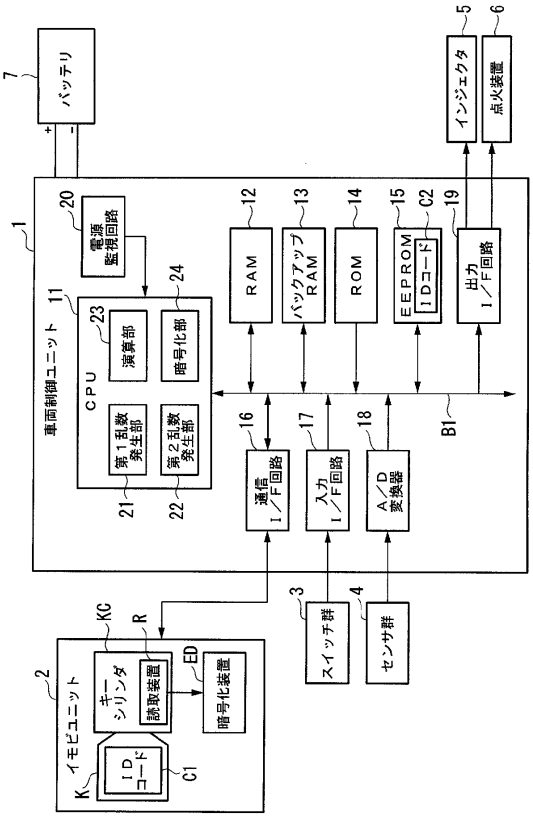
【図５】本発明の第２実施形態によるバッテリキャンセル時における乱数発生装置の処理を示すフローチャートである。

【符号の説明】

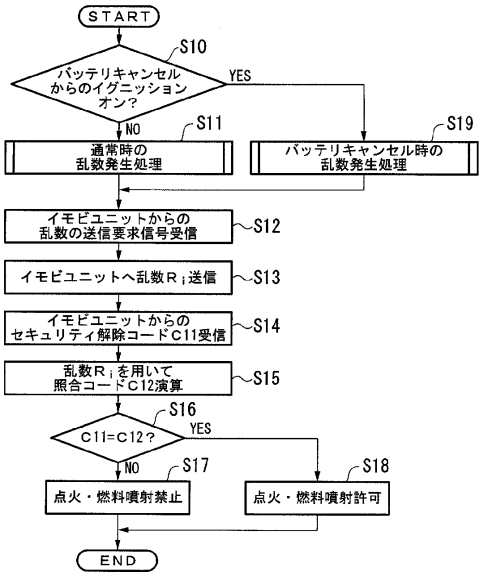
【００５２】

１　車両制御装置
１３　バックアップＲＡＭ
１５　ＥＥＰＲＯＭ
２１　第１乱数発生部
２２　第２乱数発生部
２３　演算部
２５　第３乱数発生部
Ｃ１，Ｃ２　ＩＤコード
Ｋ　イグニッションキー

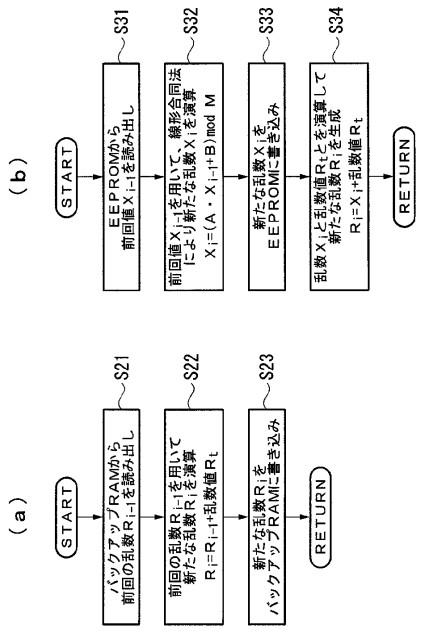
【図１】


バッテリ
車両制御ユニット
CPU
第１乱数発生部
第２乱数発生部
演算部
暗号化部
RAM
バックアップRAM
ROM
EEPROM
IDコード
出力I／F回路
通信I／F回路
入力I／F回路
A／D変換器
電源監視回路
インジェクタ
点火装置
スイッチ群
センサ群
イモビユニット
キーシリンダ
読取装置
暗号化装置
IDコード

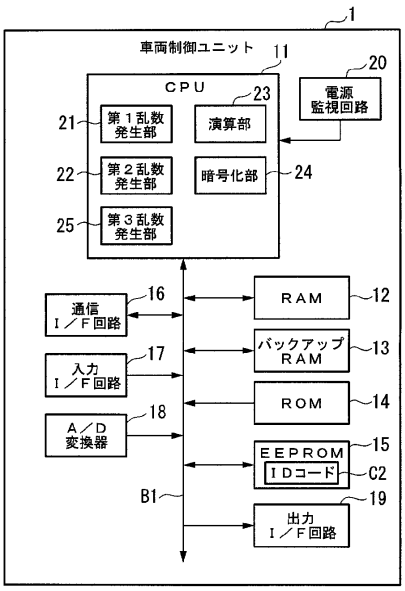
【図２】


START
バッテリキャンセルからのイグニッションオン？
YES
NO
通常時の乱数発生処理
バッテリキャンセル時の乱数発生処理
イモビユニットからの乱数の送信要求信号受信
イモビユニットへ乱数Riを送信
イモビユニットからのセキュリティ解除コードC11受信
乱数Riを用いて照合コードC12演算
C11=C12？
点火・燃料噴射禁止
点火・燃料噴射許可
END

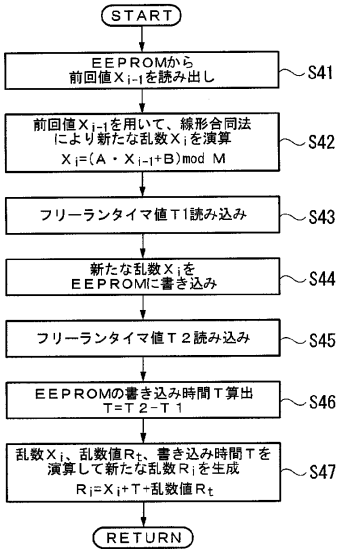
【図３】


（a）
START
バックアップRAMから前回の乱数Ri-1を読み出し
前回の乱数Ri-1を用いて新たな乱数Riを演算
Ri=Ri-1+乱数値Rt
新たな乱数Riをバックアップ RAMに書き込み
RETURN
（b）
START
EEPROMから前回値Xi-1を読み出し
前回値Xi-1を用いて、線形合同法により新たな乱数Xiを演算
Xi=(A・Xi-1+B)mod M
新たな乱数XiをEEPROMに書き込み
乱数Xiと乱数値Rtとを演算して新たな乱数Riを生成
Ri=Xi+乱数値Rt
RETURN

【図４】


車両制御ユニット
CPU
第１乱数発生部
第２乱数発生部
第３乱数発生部
演算部
暗号化部
電源監視回路
通信I／F回路
入力I／F回路
A／D変換器
RAM
バックアップRAM
ROM
EEPROM
IDコード
出力I／F回路
B1

【図５】


START
EEPROMから
前回値X_{i-1}を読み出し
S41
前回値X_{i-1}を用いて、線形合同法
により新たな乱数X_iを演算
$X_i=(A\cdot X_{i-1}+B) \bmod M$
S42
フリーランタイマ値Ｔ1読み込み
S43
新たな乱数X_iを
EEPROMに書き込み
S44
フリーランタイマ値Ｔ２読み込み
S45
EEPROMの書き込み時間Ｔ算出
T=Ｔ２−Ｔ１
S46
乱数X_i、乱数値R_t、書き込み時間Ｔを
演算して新たな乱数R_iを生成
$R_i=X_i+T+$乱数値R_t
S47
RETURN

フロントページの続き

(74)代理人 100107836
弁理士 西 和哉
(74)代理人 100108453
弁理士 村山 靖彦
(72)発明者 鈴木 暁
栃木県塩谷郡高根沢町宝積寺字サギノヤ東２０２１番地８ 株式会社ケーヒン栃木開発センター内
(72)発明者 柴 允与
栃木県塩谷郡高根沢町宝積寺字サギノヤ東２０２１番地８ 株式会社ケーヒン栃木開発センター内
(72)発明者 清野 幸平
埼玉県和光市中央１丁目４番１号 株式会社本田技術研究所内

審査官 田中 友章

(56)参考文献 特開２０００－１８１６８６（ＪＰ，Ａ）
特開２００２－２６８９４６（ＪＰ，Ａ）
特開２００６－０２４１４０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ 7／５８
Ｂ６０Ｒ ２５／０４
Ｇ０９Ｃ 1／００
Ｈ０３Ｋ 3／８４