

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6556495号
(P6556495)

(45) 発行日 令和1年8月7日 (2019. 8. 7)

(24) 登録日 令和1年7月19日 (2019. 7. 19)

(51) Int. Cl.		F I			
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	640E
G06F	21/44	(2013.01)	G06F	21/44	350

請求項の数 40 (全 22 頁)

(21) 出願番号	特願2015-104781 (P2015-104781)	(73) 特許権者	591251636
(22) 出願日	平成27年5月22日 (2015. 5. 22)		現代自動車株式会社
(65) 公開番号	特開2016-174345 (P2016-174345A)		HYUNDAI MOTOR COMPAN Y
(43) 公開日	平成28年9月29日 (2016. 9. 29)		大韓民国ソウル特別市瑞草区獻陵路12
審査請求日	平成30年3月30日 (2018. 3. 30)		12, Heolleung-ro, Seocho-gu, Seoul, Republic of Korea
(31) 優先権主張番号	10-2015-0036940	(74) 代理人	100107582
(32) 優先日	平成27年3月17日 (2015. 3. 17)		弁理士 関根 毅
(33) 優先権主張国・地域又は機関	韓国 (KR)	(74) 代理人	100117787
			弁理士 勝沼 宏仁
		(74) 代理人	100127465
			弁理士 堀田 幸裕

最終頁に続く

(54) 【発明の名称】 秘密情報基盤の相互認証方法及び装置

(57) 【特許請求の範囲】

【請求項 1】

外部装置と連動する車両制御器での相互認証方法において、
 前記外部装置から受信された認証要請メッセージによって乱数 S を生成して前記外部装置に伝送する第 1 のステップ；
 前記乱数 S を媒介変数とする第 1 の関数を用いて変数 i を生成する第 2 のステップ；
 前記変数 i 及び予め保存された保安キー K を媒介変数とする第 2 の関数を用いて第 1 のセッションキー K_s を生成する第 3 のステップ；
 前記外部装置から第 1 の応答キーを受信する第 4 のステップ；
 前記乱数 S、前記変数 i 及び前記第 1 のセッションキー K_s を媒介変数とする第 3 の関数を用いて第 2 の応答キーを生成する第 5 のステップ；及び
 前記第 1 の応答キーと前記第 2 の応答キーとが一致するか否かに基づいて前記外部装置を認証する第 6 のステップ；
 を含む、相互認証方法。

【請求項 2】

前記認証要請メッセージに乱数 R が含まれる場合、前記乱数 R 及び前記乱数 S を前記第 1 の関数の媒介変数として設定し、前記変数 i を生成する、請求項 1 に記載の相互認証方法。

【請求項 3】

前記変数 i は、数式：

$$i = f_1(R, S) = L_S(R) + S \bmod 16$$

によって生成され、ここで、前記 $L_S(R)$ は、前記乱数 R を前記乱数 S のビット数だけ循環前置する関数である、請求項 2 に記載の相互認証方法。

【請求項 4】

前記第 1 のセッションキー K_S は、前記乱数 S をさらに用いて生成される、請求項 1 に記載の相互認証方法。

【請求項 5】

前記第 1 のセッションキー K_S は、

前記保安キー K と前記乱数 S とのビット単位 XOR 演算を通じて生成された第 1 の値と、前記第 1 の値を前記変数 i だけ循環前置して生成された第 2 の値とのビット単位 XOR 演算を通じて生成される、請求項 4 に記載の相互認証方法。

10

【請求項 6】

前記乱数 S を前記保安キー K の ビット長と同一ビット長になるまで 反復して接続した後、ビット単位 XOR 演算を通じて前記第 1 の値を生成する、請求項 5 に記載の相互認証方法。

【請求項 7】

前記認証要請メッセージに乱数 R が含まれる場合、前記乱数 R をさらに用いて前記第 2 の応答キーを生成する、請求項 1 に記載の相互認証方法。

【請求項 8】

前記第 2 の応答キーは、数式：

20

【数 1】

$$f_3(i, K_S, R, S) = g(i+m, K_S, R, S) = [g_3(w_{i+m}(K_S), g_2(g_1(R \oplus S))))]^{i+m}$$

によって算出され、ここで、 m は、前記車両制御器に要求される保安水準によって予め設定可能な最小反復実行回数である、請求項 7 に記載の相互認証方法。

【請求項 9】

前記

【数 2】

30

$$R \oplus S$$

は、数式：

【数 3】

$$R \oplus S = 1_7 || 1_6 || 1_5 || 1_4 || 1_3 || 1_2 || 1_1 || 1_0$$

によって算出され、ここで、前記 1_j は、前記乱数 R と前記乱数 S とのビット単位 XOR 結果を 4 ビット単位で区分した値である、請求項 8 に記載の相互認証方法。

【請求項 10】

前記

40

【数 4】

$$g_1(R \oplus S)$$

は、数式：

【数 5】

$$g_1(R \oplus S) = h(1_7) || h(1_6) || h(1_5) || h(1_4) || h(1_3) || h(1_2) || h(1_1) || h(1_0)$$

によって算出され、ここで、 $h(1_j)$ は置換演算である、請求項 9 に記載の相互認証

50

方法。

【請求項 1 1】

前記 $h(1_j)$ は、数式：

$h(1_j) = \{9, 4, 10, 11, 13, 1, 8, 5, 6, 2, 0, 3, 12, 14, 15, 7\}$

によって算出される、請求項 1 0 に記載の相互認証方法。

【請求項 1 2】

前記

【数 6】

$$g_2(g_1(R \oplus S))$$

10

は、予め定義された 4 X 4 行列と 4 ビット単位の前記 $h(1_j)$ との積を通じて算出される、請求項 1 0 に記載の相互認証方法。

【請求項 1 3】

前記

【数 7】

$$g_2(g_1(R \oplus S))$$

は、数式：

【数 8】

20

$$\begin{pmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 1 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} h(l_7) & h(l_6) \\ h(l_5) & h(l_4) \\ h(l_3) & h(l_2) \\ h(l_1) & h(l_0) \end{pmatrix} = \begin{pmatrix} l'_7 & l'_6 \\ l'_5 & l'_4 \\ l'_3 & l'_2 \\ l'_1 & l'_0 \end{pmatrix}$$

によって算出される、請求項 1 2 に記載の相互認証方法。

【請求項 1 4】

前記 $h(1_j)$ が (x_3, x_2, x_1, x_0) であるとき、 $2h(1_j)$ 及び $3h(1_j)$ は、

30

それぞれ下記の数式：

【数 9】

$$2h(1_j) = (x_2, x_1, x_0 \oplus x_3, x_3)$$

【数 1 0】

$$3h(1_j) = (x_2 \oplus x_3, x_1 \oplus x_2, x_0 \oplus x_1 \oplus x_3, x_0 \oplus x_3)$$

によって算出される、請求項 1 3 に記載の相互認証方法。

【請求項 1 5】

前記 $w_{i+m}(K_S)$ は、前記第 1 のセッションキー K_S の下位 32 ビットを所定ビット数だけ循環前置させる関数である、請求項 1 3 に記載の相互認証方法。

40

【請求項 1 6】

前記

【数 1 1】

$$g_3(w_{i+m}(K_S), g_2(g_1(R \oplus S)))$$

は、前記の循環前置された 32 ビットの K_S と前記 8 個の 4 ビットブロックである

【数 1 2】

$$l'_7 || l'_6 || l'_5 || l'_4 || l'_3 || l'_2 || l'_1 || l'_0$$

50

とのビット単位XOR演算を行う関数である、請求項15に記載の相互認証方法。

【請求項17】

前記第1の応答キーと前記第2の応答キーとが一致する場合、
前記第2の応答キーを用いて第3の応答キーを生成する第7のステップ；及び
前記第3の応答キーを前記外部装置に伝送する第8のステップ；
をさらに含む、請求項1に記載の相互認証方法。

【請求項18】

前記第7のステップは、
前記第2の応答キー及び前記変数 i を媒介変数とする前記第1の関数を用いて変数 j を生成するステップ；
前記変数 j 、前記第1のセッションキー K_s 及び前記乱数 S を媒介変数とする前記第2の関数を用いて第2のセッションキー K_{s2} を生成するステップ；及び
前記変数 j 、前記第2のセッションキー K_{s2} 及び前記乱数 S を媒介変数とする前記第3の関数を用いて前記第3の応答キーを生成するステップ；
を含む、請求項17に記載の相互認証方法。

【請求項19】

前記第1の応答キーと前記第2の応答キーとが一致しない場合、乱数である第3の応答キーを前記外部装置に伝送するステップをさらに含む、請求項1に記載の相互認証方法。

【請求項20】

車両制御器と連動する外部装置での相互認証方法において、
前記車両制御器に認証要請メッセージを伝送する第1のステップ；
前記車両制御器から乱数 S を受信する第2のステップ；
前記乱数 S を媒介変数とする第1の関数を用いて変数 i を生成する第3のステップ；
前記変数 i 及び予め保存された保安キー K を媒介変数とする第2の関数を用いて第1のセッションキー K_s を生成する第4のステップ；
前記乱数 S 、前記変数 i 、前記第1のセッションキー K_s を媒介変数とする第3の関数を用いて第1の応答キーを生成する第5のステップ；及び
前記第1の応答キーを前記車両制御器に伝送する第6のステップ；
を含む、相互認証方法。

【請求項21】

前記認証要請メッセージに乱数 R が含まれて伝送される場合、前記乱数 R 及び前記乱数 S を前記第1の関数の媒介変数として設定し、前記変数 i を生成する、請求項20に記載の相互認証方法。

【請求項22】

前記変数 i は、数式：
$$i = f_1(R, S) = L_s(R) + S \bmod 16$$

によって生成され、ここで、前記 $L_s(R)$ は、前記乱数 R を前記乱数 S のビット数だけ循環前置する関数である、請求項21に記載の相互認証方法。

【請求項23】

前記乱数 S を前記第2の関数の媒介変数としてさらに用いて前記第1のセッションキー K_s を生成する、請求項20に記載の相互認証方法。

【請求項24】

前記第1のセッションキー K_s は、
前記保安キー K と前記乱数 S とのビット単位XOR演算を通じて生成された第1の値と、前記第1の値を前記変数 i だけ循環前置して生成された第2の値とのビット単位XOR演算を通じて生成される、請求項23に記載の相互認証方法。

【請求項25】

前記乱数 S を前記保安キー K のビット長と同一ビット長になるまで反復して接続した後、ビット単位XOR演算を通じて前記第1の値を生成する、請求項24に記載の相互認証方法。

【請求項 26】

前記認証要請メッセージに乱数 R が含まれる場合、前記乱数 R をさらに用いて前記第 1 の応答キーを生成する、請求項 20 に記載の相互認証方法。

【請求項 27】

前記第 1 の応答キーは、数式：

【数 13】

$$f_3(i, K_S, R, S) = g(i+m, K_S, R, S) = [g_3(w_{i+m}(K_S), g_2(g_1(R \oplus S)))^{i+m}]$$

10

によって算出され、ここで、m は、前記車両制御器に要求される保安水準によって予め設定可能な値である、請求項 26 に記載の相互認証方法。

【請求項 28】

前記

【数 14】

$$R \oplus S$$

は、数式：

【数 15】

$$R \oplus S = 1_7 || 1_6 || 1_5 || 1_4 || 1_3 || 1_2 || 1_1 || 1_0$$

20

によって算出され、ここで、前記 1_j は、前記乱数 R と前記乱数 S とのビット単位 XOR 結果を 4 ビット単位で区分した値である、請求項 27 に記載の相互認証方法。

【請求項 29】

前記

【数 16】

$$g_1(R \oplus S)$$

は、数式：

【数 17】

$$g_1(R \oplus S) = h(1_7) || h(1_6) || h(1_5) || h(1_4) || h(1_3) || h(1_2) || h(1_1) || h(1_0)$$

30

によって算出され、ここで、 $h(1_j)$ は置換演算である、請求項 28 に記載の相互認証方法。

【請求項 30】

前記 $h(1_j)$ は、数式：

$$h(1_j) = \{9, 4, 10, 11, 13, 1, 8, 5, 6, 2, 0, 3, 12, 14, 15, 7\}$$

40

によって算出される、請求項 29 に記載の相互認証方法。

【請求項 31】

前記

【数 18】

$$g_2(g_1(R \oplus S))$$

は、予め定義された 4 X 4 行列と 4 ビット単位の前記 $h(1_j)$ との積を通じて算出される、請求項 29 に記載の相互認証方法。

【請求項 32】

前記

50

【数 1 9】

$$g_2(g_1(R \oplus S))$$

は、数式：

【数 2 0】

$$\begin{pmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 1 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} h(l_7) & h(l_6) \\ h(l_5) & h(l_4) \\ h(l_3) & h(l_2) \\ h(l_1) & h(l_0) \end{pmatrix} = \begin{pmatrix} l'_7 & l'_6 \\ l'_5 & l'_4 \\ l'_3 & l'_2 \\ l'_1 & l'_0 \end{pmatrix} \quad 10$$

によって算出される、請求項 3 1 に記載の相互認証方法。

【請求項 3 3】

前記 $h(l_j)$ が (x_3, x_2, x_1, x_0) であるとき、 $2h(l_j)$ 及び $3h(l_j)$ は、

それぞれ下記の数式：

【数 2 1】

$$2h(l_j) = (x_2, x_1, x_0 \oplus x_3, x_3)$$

【数 2 2】

$$3h(l_j) = (x_2 \oplus x_3, x_1 \oplus x_2, x_0 \oplus x_1 \oplus x_3, x_0 \oplus x_3)$$

によって算出される、請求項 3 2 に記載の相互認証方法。

【請求項 3 4】

前記 $w_{i+m}(K_S)$ は、前記第 1 のセッションキー K_S の下位 32 ビットを所定ビット数だけ循環前置させる関数である、請求項 3 2 に記載の相互認証方法。

【請求項 3 5】

前記

【数 2 3】

$$\underline{g_3(w_{i+m}(K_S), g_2(g_1(R \oplus S)))} \quad 30$$

は、前記の循環前置された 32 ビットの K_S と前記 8 個の 4 ビットブロックである

【数 2 4】

$$l'_7 || l'_6 || l'_5 || l'_4 || l'_3 || l'_2 || l'_1 || l'_0$$

とのビット単位 XOR 演算を行う関数である、請求項 3 4 に記載の相互認証方法。

【請求項 3 6】

前記車両制御器から第 3 の応答キーを受信する第 7 のステップ；

前記第 1 の応答キーを用いて第 4 の応答キーを生成する第 8 のステップ；及び

前記第 3 の応答キーと前記第 4 の応答キーとが一致するか否か基づいて前記車両制御器を認証する第 9 のステップ；

をさらに含む、請求項 2 0 に記載の相互認証方法。

【請求項 3 7】

前記第 8 のステップは、

前記第 1 の応答キー及び前記変数 i を媒介変数とする前記第 1 の関数を用いて変数 j を生成するステップ；

前記変数 j 及び前記第 1 のセッションキー K_S を媒介変数とする前記第 2 の関数を用いて第 2 のセッションキー K_{S2} を生成するステップ；及び

前記変数 j 、前記セッションキー K_{S2} 前記及び乱数 S を媒介変数とする第 3 の関数を用いて前記第 4 の応答キーを生成するステップ；

を含む、請求項 3 6 に記載の相互認証方法。

【請求項 3 8】

請求項 1 から 3 7 のいずれか一つの方法を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 3 9】

外部装置と相互認証を行う相互認証装置において、

前記外部装置との通信を行う通信部；

前記外部装置から受信された認証要請メッセージによって乱数 S を生成する乱数生成部；

前記乱数 S を媒介変数とする第 1 の関数を用いて変数 i を生成する反復回数生成部；

前記変数 i 及び予め保存された保安キー K を媒介変数とする第 2 の関数を用いて第 1 のセッションキー K_s を生成するセッションキー生成部；

前記外部装置から第 1 の応答キーが受信されると、前記乱数 S、前記変数 i 及び前記第 1 のセッションキー K_s を媒介変数とする第 3 の関数を用いて第 2 の応答キーを生成する応答キー生成部；及び

前記第 1 の応答キーと前記第 2 の応答キーとが一致するか否かに基づいて前記外部装置を認証する認証部；

を含む、相互認証装置。

【請求項 4 0】

車両制御器と相互認証を行う相互認証装置において、

前記車両制御器に認証要請メッセージを伝送し、前記車両制御器から乱数 S を受信する通信部；

前記乱数 S を媒介変数とする第 1 の関数を用いて変数 i を生成する反復回数生成部；

前記変数 i 及び予め保存された保安キー K を媒介変数とする第 2 の関数を用いて第 1 のセッションキー K_s を生成するセッションキー生成部；

前記変数 i、前記第 1 のセッションキー K_s 及び前記乱数 S を媒介変数とする第 3 の関数を用いて第 1 の応答キーを生成する応答キー生成部；及び

前記車両制御器に伝送された前記第 1 の応答キーと前記前記車両制御器から受信された第 3 の応答キーとが一致するか否かを確認し、前記車両制御器を認証する認証部；

を含む、相互認証装置。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、車両での相互認証方法及び装置に関し、より詳細には、秘密情報に基づいて車両制御器と外部装置との間の相互認証を可能にする秘密情報基盤の相互認証方法及び装置に関する。

【背景技術】

【0 0 0 2】

最近、市販されている車両には、運転手の便宜及び安全を向上させるための各種の電子制御装置が搭載されており、これら電子制御装置間の相互通信のための車両内の通信ネットワークが基本的に搭載されている。

【0 0 0 3】

車両内の電子制御器の個数が持続的に増加し、多様な外部機器との連動が可能になることによって、車両の保安を維持することは安全運行のために非常に重要な 이슈である。

【0 0 0 4】

したがって、車両制御器に対する診断及び車両制御器内部のデータアップデートを行うためには、外部診断装置に対する認証手順が要求される。

【0 0 0 5】

従来、車両制御器と診断器との間の認証手順は、診断器の認証要請に応じて車両制御器

10

20

30

40

50

がシード (Seed) 値を診断器に伝送すると、診断器が受信されたシード値を用いてキー (Key) 値を生成する。このとき、生成されたキー値は電子制御器に伝送され、電子制御器は、診断器から受信されたキー値と、予め定義されたアルゴリズムによって内部に生成されたキー値とが一致するか否かに基づいて診断器の接近を許容する。

【0006】

しかし、従来のシードキー (Seed Key) アルゴリズムは、シード値を受け取り、キーを生成するアルゴリズム自体を秘密に維持することによって保安を達成する方式であるので、該当のシードキーアルゴリズムが公開または分析される場合、保安に致命的であるという問題があった。

【発明の概要】

10

【発明が解決しようとする課題】

【0007】

本発明は、上述した従来技術の問題を解決するためになされたものであって、本発明の目的は、保安情報に基づいた相互認証方法及び装置を提供することにある。

【0008】

本発明の他の目的は、シード値に対して独立的な事前に共有された秘密キーに基づいて相互認証を行うことが可能な保安情報に基づいた相互認証方法及び装置を提供することにある。

【0009】

本発明で達成しようとする技術的課題は、上述した技術的課題に制限されず、言及していない更に他の技術的課題は、下記の記載から、本発明の属する技術分野で通常の知識を有する者に明確に理解され得るだろう。

20

【課題を解決するための手段】

【0010】

本発明は、秘密情報基盤の相互認証方法及び装置に関する。

【0011】

本発明の一実施例に係る外部装置と連動する車両制御器での相互認証方法は、前記外部装置から受信された認証要請メッセージによって乱数 S を前記外部装置に伝送する第1のステップと、前記乱数 S を媒介変数とする第1の関数を用いて変数 i を生成する第2のステップと、前記変数 i 及び予め保存された保安キー K を媒介変数とする第2の関数を用いて第1のセッションキー K_s を生成する第3のステップと、前記外部装置から第1の応答キーを受信する第4のステップと、前記乱数 S 、前記変数 i 、前記第1のセッションキー K_s を媒介変数とする第3の関数を用いて第2の応答キーを生成する第5のステップと、前記第1の応答キーと前記第2の応答キーとが一致するか否かに基づいて前記外部装置を認証する第6のステップとを含んで構成することができる。

30

【0012】

本発明の他の一実施例に係る車両制御器と連動する外部装置での相互認証方法は、前記車両制御器に認証要請メッセージを伝送する第1のステップと、前記車両制御器から乱数 S を受信する第2のステップと、前記乱数 S を媒介変数とする第1の関数を用いて変数 i を生成する第3のステップと、前記変数 i 及び予め保存された保安キー K を媒介変数とする第2の関数を用いて第1のセッションキー K_s を生成する第4のステップと、前記乱数 S 、前記変数 i 、前記第1のセッションキー K_s を媒介変数とする第3の関数を用いて第1の応答キーを生成する第5のステップと、前記第1の応答キーを前記車両制御器に伝送する第6のステップとを含んで構成することができる。

40

【0013】

本発明の更に他の一実施例に係る外部装置と相互認証を行う相互認証装置は、前記外部装置との通信を行う通信部と、前記外部装置から受信された認証要請メッセージによって乱数 S を生成する乱数生成部と、前記乱数 S を媒介変数とする第1の関数を用いて変数 i を生成する反復回数生成部と、前記変数 i 及び予め保存された保安キー K を媒介変数とする第2の関数を用いて第1のセッションキー K_s を生成するセッションキー生成部と、前

50

記外部装置から第1の応答キーが受信されると、前記乱数S、前記変数i及び前記第1のセッションキー K_s を媒介変数とする第3の関数を用いて第2の応答キーを生成する応答キー生成部と、前記第1の応答キーと前記第2の応答キーとが一致するか否かに基づいて前記外部装置を認証する認証部とを含むことができる。

【0014】

本発明の更に他の一実施例に係る車両制御器と相互認証を行う相互認証装置は、前記車両制御器に認証要請メッセージを送信し、前記車両制御器から乱数Sを受信する通信部と、前記乱数Sを媒介変数とする第1の関数を用いて変数iを生成する反復回数生成部と、前記変数i及び予め保存された保安キーKを媒介変数とする第2の関数を用いて第1のセッションキー K_s を生成するセッションキー生成部と、前記変数i、前記第1のセッションキー K_s 及び前記乱数Sを媒介変数とする第3の関数を用いて第1の応答キーを生成する応答キー生成部と、前記車両制御器に伝送された前記第1の応答キーと、前記前記車両制御器から受信された第3の応答キーとが一致するか否かを確認し、前記車両制御器を認証する認証部とを含むことができる。

10

【0015】

本発明の更に他の一実施例は、前記相互認証方法を実行させるためのプログラムを記録したコンピューター読み取り可能な記録媒体を提供することができる。

【0016】

前記本発明の各様態は、本発明の好ましい各実施例の一部に過ぎず、本願発明の技術的特徴が反映された多様な実施例は、当該技術分野で通常の知識を有する者によって後述する本発明の詳細な説明に基づいて導出されて理解され得る。

20

【発明の効果】

【0017】

本発明に係る方法及び装置に対する効果について説明すると、次の通りである。

【0018】

第一に、本発明は、保安情報に基づいた相互認証方法及び装置を提供するという長所を有する。

【0019】

第二に、本発明は、シード値に対して独立的な事前に共有された秘密キーに基づいて相互認証を行うことが可能な保安情報に基づいた相互認証方法及び装置を提供するという長所を有する。

30

【0020】

第三に、本発明は、シード値によって反復回数iが動的に変更され、秘密キー値に対する保安水準及び演算の複雑度が動的に変更され得るという長所を有する。

【0021】

第四に、本発明は、多様な長さの秘密キーを提供することによって、保安水準を制御できるという長所を有する。

【図面の簡単な説明】

【0022】

【図1】本発明の一実施例に係る秘密情報に基づいた相互認証システム構成図である。

40

【図2】本発明の一実施例に係る相互認証方法を説明するためのフローチャートである。

【図3】本発明の一実施例に係るセッションキー生成方法を説明するための図である。

【図4】本発明の他の一実施例に係るセッションキー生成方法を説明するための図である。

。

【図5】本発明の一実施例に係る応答キー生成手順を説明するための図である。

【図6】本発明の一実施例に係る車両制御器での相互認証方法を説明するためのフローチャートである。

【図7】本発明の一実施例に係る外部装置での相互認証方法を説明するためのフローチャートである。

【発明を実施するための形態】

50

【0023】

以下、本発明の各実施例が適用される装置及び多様な方法について図面を参照してより詳細に説明する。以下の説明で使用する構成要素に対する接尾辞「モジュール」及び「部」は、明細書作成の容易さのみが考慮されて付与または混用されるものであって、それ自体で互いに区別される意味または役割を有するものではない。

【0024】

以上で、本発明の実施例を構成する全ての構成要素が一つに結合されたり、一つに結合されて動作すると説明されたとして、本発明が必ずしもこのような実施例に限定されることはない。すなわち、本発明の目的範囲内であれば、その全ての構成要素が一つ以上に選択的に結合されて動作することもできる。また、その全ての構成要素がそれぞれ一つの独立的なハードウェアで具現化され得るが、各構成要素のその一部または全部が選択的に組み合わせられ、一つまたは複数のハードウェアで組み合わせられた一部または全部の機能を行うプログラムモジュールを有するコンピュータプログラムとして具現されることも可能である。そのコンピュータプログラムを構成する各コード及び各コードセグメントは、本発明の技術分野の当業者によって容易に推測可能であろう。このようなコンピュータプログラムは、コンピュータ読み取り可能な保存媒体 (Computer Readable Media) に保存され、コンピュータによって読み取られて実行されることによって、本発明の実施例を具現することができる。コンピュータプログラムの保存媒体としては、磁気記録媒体、光記録媒体、キャリアウェーブ媒体などを含ませることができる。

【0025】

また、以上で記載した「含む」、「構成する」または「有する」などの用語は、特別に反対の記載がない限り、該当の構成要素が内在し得ることを意味するので、他の構成要素を除外するのではなく、他の構成要素をさらに含み得ると解釈しなければならない。技術的または科学的な用語を含む全ての用語は、異なる意味に定義されない限り、本発明の属する技術分野で通常の知識を有する者によって一般的に理解されるものと同じ意味を有する。事前に定義された用語のように一般的に使用される各用語は、関連技術の文脈上の意味と一致するものと解釈しなければならない。本発明で明らかに定義しない限り、理想的または過度に形式的な意味に解釈しない。

【0026】

また、本発明の構成要素を説明するにおいて、第1、第2、A、B、(a)、(b)などの用語を使用することができる。このような用語は、その構成要素を他の構成要素と区別するためのものに過ぎず、その用語によって該当の構成要素の本質や順番または順序などが限定されることはない。いずれかの構成要素が他の構成要素に「連結」、「結合」または「接続」されると記載した場合、その構成要素は、その他の構成要素に直接連結または接続され得るが、各構成要素の間に更に他の構成要素が「連結」、「結合」または「接続」されることも可能であると理解すべきであろう。

【0027】

図1は、本発明の一実施例に係る秘密情報に基づいた相互認証システム構成図である。

【0028】

図1を参照すると、相互認証システムは、大きく、外部装置10及び車両制御器20を含んで構成することができる。

【0029】

一例において、外部装置10は、所定の接続端子または無線連結を通じて車両の状態を診断する診断器 (Tester) またはOBD (On-Board Diagnostics) であり得る。

【0030】

外部装置10と車両制御器20は、有線または無線連結を通じて信号を送受信する通信部11及び21を含むことができる。

【0031】

また、外部装置 10 と車両制御器 20 は、相互認証のための乱数生成部 12、22、反復回数生成部 13、23、セッションキー生成部 14、24、応答キー生成部 15、25、認証部 16、26、及び装置内部の全体的な動作を制御する制御部 17、27を含んで構成することができる。

【0032】

乱数生成部 12、22 は、所定の長さを有する乱数を生成する機能を行うことができる。一例として、外部装置 10 の乱数生成部 12 は、所定長さの乱数 R を生成し、生成された乱数 R が含まれた認証要請メッセージを車両制御器 20 に伝送することができる。また、車両制御器 20 の乱数生成部 22 は、認証要請メッセージが受信されると、所定長さの乱数 S を生成することができる。

10

【0033】

反復回数生成部 13、23 は、外部装置 10 の乱数生成部 12 によって生成された乱数 R 及び車両制御器 20 の乱数生成部 22 によって生成された乱数 S のうち少なくとも一つを用いて保安水準及び認証アルゴリズムの演算複雑度を決定するパラメータ値である変数 i 以下、説明の便宜上、反復回数 i と混用して使用することにする。一を生成することができる。以下、乱数 R 及び乱数 S のうち少なくとも一つを媒介変数として変数 i を生成する関数を、説明の便宜上、第 1 の関数 (f_1) と称することにする。

【0034】

一例として、反復回数 i は、下記の数式 (1) によって算出することができる。

【0035】

$$i = f_1(R, S) = L_S(R) + S \bmod 16 \quad \text{数式 (1)}$$

20

【0036】

ここで、 $L_S(R)$ は、乱数 R を乱数 S のビット数だけ循環前置 (cyclic shift) させる関数であり得る。一例として、乱数 R のビット順序が $(x_{n-1}, x_{n-2}, \dots, x_1, x_0)_2$ である場合、関数 $L_S(R)$ は、乱数 S のビット数だけ左側に循環前置され、 $(x_{n-s-1}, \dots, x_1, x_0, x_{n-1}, x_{n-2}, \dots, x_{n-s})_2$ 値が生成されるように定義することができる。

【0037】

セッションキー生成部 14、24 は、反復回数 i 、予め共有された秘密キー K 及び乱数 S を媒介変数とする第 2 の関数 f_2 を用いて第 1 のセッションキー K_S を生成する機能を行う。また、セッションキー生成部 14、24 は、反復変数 i 、第 1 のセッションキー K_S 及び後述する第 1 の応答キー A__Tester または第 2 の応答キー A__ECU を用いて第 2 のセッションキー K_{S2} を生成することもできる。

30

【0038】

セッションキー生成手順は、後述する図 3～図 4 を通じて詳細に説明する。

【0039】

応答キー生成部 15、25 は、反復回数 i 、セッションキー、乱数 R、及び乱数 S のうち少なくとも一つを媒介変数として受け取り、応答キーを生成する機能を行うことができる。以下、説明の便宜上、応答キーの生成のために使用される関数を第 3 の関数と称することにする。

40

【0040】

一例として、車両制御器 20 の応答キー生成部 25 は、反復回数 i 、第 1 のセッションキー K_S 、乱数 R 及び乱数 S を媒介変数として受け取り、第 2 の応答キー A__ECU を生成することができる。これと同様に、外部装置 10 の応答キー生成部 15 も、反復回数 i 、第 1 のセッションキー K_S 、乱数 R 及び乱数 S を媒介変数として受け取り、第 1 の応答キー A__Tester を生成することができる。

【0041】

また、車両制御器 20 の応答キー生成部 25 は、外部装置 10 から第 1 の応答キー A__Tester が受信されると、第 1 の応答キーと第 2 の応答キーとが同一であるか否かによって第 3 の応答キー B__ECU を生成することができる。これと同様に、外部装置 10

50

の応答キー生成部15も第4の応答キーB__T e s t e rを生成することができる。

【0042】

応答キー生成部15、25での応答キー生成手順は、後述する図5を通じて詳細に説明する。

【0043】

認証部16、26は、他の装置から受信された応答キーと内部に生成された応答キーとが一致するか否かを確認し、他の装置に対する認証成功の有無を判断する機能を行うことができる。

【0044】

一例として、外部装置10の認証部16は、内部に生成された第4の応答キーB__T e s t e rと車両制御器20から受信された第3の応答キーB__E C Uとが互いに一致する場合、車両制御器20に対する認証に成功したと判断することができる。

10

【0045】

他の一例として、車両制御器20の認証部26は、外部装置10から受信された第1の応答キーA__T e s t e rと内部に生成された第2の応答キーA__E C Uとが互いに一致する場合、外部装置10の認証に成功したと判断することができる。

【0046】

したがって、本発明に係る外部装置10及び車両制御器20は、予め共有された秘密キーを用いて応答キーを生成した後、生成された応答キーを互いに交換することによって相互認証を行うことができる。

20

【0047】

図2は、本発明の一実施例に係る相互認証方法を説明するためのフローチャートである。

【0048】

図2を参照すると、外部装置10と車両制御器20には、予め共有された秘密キーKを維持することができる。一例として、秘密キーKの長さは、80ビット及び128ビットのうちいずれか一つであり得る。

【0049】

外部装置10は、乱数Rを生成し、生成された乱数Rが含まれた認証要請メッセージを車両制御器20に伝送することができる(S201~S203)。

30

【0050】

車両制御器20は、認証要請メッセージが受信されると、乱数Sを生成して外部装置10に伝送する(S205~S207)。このとき、車両制御器20は、乱数R及び乱数Sを媒介変数とする第1の関数を用いて反復回数iを算出することができる(S209)。

【0051】

続いて、車両制御器20は、反復回数i、秘密キーK及び乱数Sを第2の関数の媒介変数として入力し、第1のセッションキーK_sを生成することができる(S211)。

【0052】

外部装置10は、シード値である乱数Sが受信されると、既に生成された乱数R及び車両制御器20から受信された乱数Sを媒介変数とする第1の関数を用いて反復回数iを生成することができる(S215)。

40

【0053】

また、外部装置10は、反復回数i、秘密キーK及び乱数Sを第2の関数の媒介変数として入力し、第1のセッションキーK_sを生成することができる(S216)。

【0054】

外部装置10は、反復回数i、第1のセッションキーK_s、乱数R及び乱数Sを媒介変数とする第3の関数を用いて第1の応答キーA__T e s t e rを生成して車両制御器20に伝送することができる(S219~S221)。

【0055】

このとき、外部装置10は、生成された第1の応答キーA__T e s e t e rを用いて第

50

4の応答キーB__T e s t e rを生成することができる。より詳細に、外部装置10は、第1の応答キーA__T e s t e rと反復回数iを媒介変数とする第4の関数を用いて反復回数jを生成し、生成された反復回数j及び既に生成された第1のセッションキーK_sを媒介変数とする第5の関数を用いて第2のセッションキーK_{s2}を生成することができる。続いて、外部装置10は、変換変数j、第2のセッションキーK_{s2}、乱数R及び乱数Sを媒介変数とする第6の関数を用いて第4の応答キーB__T e s t e rを生成することができる。

【0056】

車両制御器20は、受信された第1の応答キーA__T e s e t e rと内部に生成された第2の応答キーA__E U Cとが一致するか否かを確認することができる（S223）。ここで、確認の結果、これらが一致すると、第1の応答キーA__E C Uと反復回数iを媒介変数とする第4の関数を用いて反復回数jを生成し、生成された反復回数j及び既に生成された第1のセッションキーK_sを媒介変数とする第5の関数を用いて第2のセッションキーK_{s2}を生成することができる。続いて、車両制御器20は、変換変数j、第2セッションキーK_{s2}、乱数R及び乱数Sを媒介変数とする第6の関数を用いて第3の応答キーB__E C Uを生成することができる。前記223ステップの確認の結果、これらが一致しない場合、車両制御器20は、所定の乱数生成器を用いて乱数を生成することができる。このとき、生成された乱数は、第3の応答キーB__E C Uになり得る。

【0057】

車両制御器20は、第3の応答キーB__E C Uを外部装置10に伝送することができる（S225）。

【0058】

外部装置10は、受信された第3の応答キーB__E C Uと既に生成された第4の応答キーB__T e s t e r値とが一致するか否かを確認することができる（S227）。ここで、確認の結果、これらが一致すると、外部装置10は、車両制御器20の認証に成功したと判断することができる。その一方、前記227ステップの確認の結果、これらが一致しないと、外部装置10は、車両制御器20の認証に失敗したと判断することができる。

【0059】

図3は、本発明の一実施例に係るセッションキー生成方法を説明するための図である。

【0060】

より詳細に、図3は、外部装置10で予め割り当てられた秘密キーK（301）の長さが80ビットである場合、第1のセッションキーK_sを生成する方法に関する。

【0061】

図3を参照すると、外部装置10は、車両制御器20から受信されたシード値である乱数S（302）を秘密キーK（301）の長さだけ反復して接続した後、XOR演算（303）を通じて80ビットの長さを有するK'（304）を生成することができる。

【0062】

一例として、図面番号310に示したように、2個の乱数S（302）と乱数S（302）の下位16ビットが接続され、80ビットの長さを有するビットシーケンスが生成され得る。このとき、外部装置10は、生成されたビットシーケンスと秘密キーK（301）とのビット単位XOR演算を通じてK'（304）を生成することができる。

【0063】

続いて、図面番号320に示したように、外部装置10は、生成されたK'（304）を反復回数iだけ左側または右側に循環前置させた後、循環前置されたK'（L_i（K'））とK'（304）とのビット単位XOR演算を通じて第1のセッションキーK_sを生成することができる。

【0064】

図4は、本発明の他の一実施例に係るセッションキー生成方法を説明するための図である。

【0065】

より詳細に、図4は、外部装置10で予め割り当てられた秘密キーK(401)の長さが128ビットである場合、第1のセッションキー K_s を生成する方法に関する。

【0066】

図4を参照すると、外部装置10は、車両制御器20から受信されたシード値である乱数S(402)を秘密キーK(401)の長さだけ反復して接続した後、XOR演算(403)を通じて128ビットの長さを有する K' (404)を生成することができる。

【0067】

一例として、図面番号410に示したように、乱数S(402)が32ビットの長さを有する場合、4個の乱数S(402)を接続し、128ビットの長さを有するビットシーケンスが生成され得る。このとき、外部装置10は、生成されたビットシーケンスと秘密キーK(401)とのビット単位XOR演算を通じて K' (404)を生成することができる。

10

【0068】

続いて、図面番号420に示したように、外部装置10は、生成された K' (404)を反復回数 i だけ左側または右側に循環前置させた後、循環前置された $K'(L_i(K'))$ と K' (404)とのビット単位XOR演算を通じて第1のセッションキー K_s を生成することができる。

【0069】

以上では、外部装置10での第1のセッションキー K_s を生成する手順を説明しているが、本発明に係る第2のセッションキー K_{s2} も、前記の図3～図4に開示した方法で生成され得ることに注意すべきである。

20

【0070】

図5は、本発明の一実施例に係る応答キー生成手順を説明するための図である。

【0071】

より詳細に、図5は、外部装置10での第1の応答キーA__Tester生成手順を説明するための図である。

【0072】

図5を参照すると、外部装置10は、下記の数式5-1のように、内部に生成された乱数Rと車両制御器20から受信された乱数Sとのビット単位XOR演算を通じて4ビット単位の l_i を生成することができる。ここで、 i は、0～7の値を有することができる。

30

【0073】

<数式5-1>

【数1】

$$R \oplus S = l_7 || l_6 || l_5 || l_4 || l_3 || l_2 || l_1 || l_0$$

【0074】

続いて、外部装置10は、下記の数式5-2のように、集合 $h(l_i)$ を参照して l_i に対する置換演算を行うことができる。

【0075】

<数式5-2>

【数2】

$$g_1(R \oplus S) = h(l_7) || h(l_6) || h(l_5) || h(l_4) || h(l_3) || h(l_2)$$

$$|| h(l_1) || h(l_0)$$

【0076】

ここで、 $h(l_i) = \{9, 4, 10, 11, 13, 1, 8, 5, 6, 2, 0, 3, 1$

50

2, 14, 15, 17}

【0077】

その後、外部装置10は、前記置換演算結果である $h(l_7) || h(l_6) || h(l_5) || h(l_4) || h(l_3) || h(l_2) || h(l_1) || h(l_0)$ を、下記の数式5-3のように、所定の4X4行列と掛けて

【数3】

$$l'_7 || l'_6 || l'_5 || l'_4 || l'_3 || l'_2 || l'_1 || l'_0$$

を生成することができる。

10

【0078】

<数式5-3>

【数4】

$$\begin{pmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 1 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} h(l_7) & h(l_6) \\ h(l_5) & h(l_4) \\ h(l_3) & h(l_2) \\ h(l_1) & h(l_0) \end{pmatrix} = \begin{pmatrix} l'_7 & l'_6 \\ l'_5 & l'_4 \\ l'_3 & l'_2 \\ l'_1 & l'_0 \end{pmatrix}$$

20

【0079】

一例として、前記数式5-3を参照すると、

l'_7 は、

【数5】

$$h(l_7) \oplus h(l_5) \oplus 2h(l_3) \oplus 3h(l_1)$$

と算出することができる。

30

【0080】

ここで、2進数として表記したxが(x3, x2, x1, x0)である場合、2xと3xは、それぞれ

【数6】

$$(x_2, x_1, x_0 \oplus x_3, x_3).$$

及び

【数7】

$$(x_2 \oplus x_3, x_1 \oplus x_2, x_0 \oplus x_1 \oplus x_3, x_0 \oplus x_3)$$

40

と定義することができる。

【0081】

最後に、外部装置10は、下記の数式5-4のように、第1の応答キーA_Testerを生成することができる。

【0082】

<数式5-4>

【数 8】

$$\begin{aligned} A_Tester &= [g_3(w_{i+4}(K_S), /_7//_6//_5//_4//_3//_2//_1//_0)]^{i+4} \\ &= [w_{i+4}(K_S) \oplus /_7//_6//_5//_4//_3//_2//_1//_0]^{i+4} \end{aligned}$$

によって算出することができ、 $w_j(K_S) = L_{37j \bmod (\text{secret key size})}(K_S) \bmod 2^{32}$ と定義することができる。ここで、 K_S は、前記の図3または図4で算出された第1のセッションキー K_S の値であり、 j は、反復回数 i に4—ここで、4は、 g_3 関数の最小反復実行回数である。—を足した値であり得る。また、 $w_j(K_S)$ は、第1のセッションキー K_S の下位32ビットを37ビットだけ左側に循環前置させる関数であり得る。

10

【0083】

以上の実施例では、応答キーを生成するための g_3 関数の最小反復実行回数が4であると定義されているが、これは一つの実施例に過ぎず、本発明の他の一実施例は、ECUの種類及び該当のECUに対して要求される保安等級によって最小反復実行回数が差等的に指定され得ることに注意すべきである。一例として、要求される保安等級が高いECUの最小反復実行回数は、相対的に保安等級が低いECUより高く設定され得る。

20

【0084】

以上の図3～図5では、外部装置10でのセッションキー生成手順及び応答キー生成手順について説明したが、車両制御器20でのセッションキー生成手順及び応答キー生成手順も、それと同一または類似する方法で生成することができる。

【0085】

図6は、本発明の一実施例に係る車両制御器での相互認証方法を説明するためのフローチャートである。

【0086】

図6を参照すると、車両制御器20は、外部装置10から認証要請メッセージが受信されると、乱数 S を生成して外部装置10に伝送することができる(S601)。

【0087】

30

ここで、認証要請メッセージには、外部装置10によって生成された乱数 R を含ませることができる。

【0088】

車両制御器20は、乱数 S を媒介変数とする第1の関数を用いて反復回数である変数 i を生成し、生成された変数 i 及び予め保存された保安キー K を媒介変数とする第2の関数を用いて第1のセッションキー K_S を生成することができる(S603～S605)。

【0089】

車両制御器20は、外部装置10から第1の応答キー A_Tester が受信されると、乱数 S 、変数 i 及び第1のセッションキー K_S を媒介変数とする第3の関数を用いて第2の応答キー A_ECU を生成することができる(S607～S609)。認証要請メッセージに乱数 R が含まれる場合、車両制御器20は、乱数 S 、変数 i 及び第1のセッションキー K_S のみならず、乱数 R をさらに用いて第1の応答キー A_Tester を生成することも可能であることに注意すべきである。

40

【0090】

続いて、車両制御器20は、第1の応答キー A_Tester と第2の応答キー A_ECU とが一致するか否かを確認することができる(S611)。

【0091】

前記確認の結果、これらが一致すると、車両制御器20は、第2の応答キー A_ECU 及び変数 i を媒介変数とする第4の関数を用いて変数 j を生成し、前記605ステップで生成された第1のセッションキー K_S 及び変数 j を媒介変数とする第5の関数を用いて第

50

2のセッションキー K_{S_2} を生成することができる(S615)。

【0092】

ここで、第4の関数は、第2の応答キー A_ECU を変数 i だけ左側に循環前置させる関数であって、第1の関数に対応し得る。

【0093】

また、第5の関数は、変数 j 、セッションキー K_S 及び乱数 S を媒介変数として前記の図3または図4に示したセッションキー生成手順を行う関数であって、前記605ステップの第2の関数に対応し得る。

【0094】

車両制御器20は、乱数 S 、変数 j 、第2のセッションキー K_{S_2} を媒介変数とする第6の関数を用いて第3の応答キー B_ECU を生成した後、生成された第3の応答キー B_ECU を外部装置10に伝送することができる(S617~S619)。認証要請メッセージに乱数 R が含まれる場合、車両制御器20は、乱数 R をさらに用いて第3の応答キー B_ECU を生成することも可能であることに注意すべきである。

【0095】

ここで、第6の関数は、前記図5に示した応答キー生成手順を行う関数であって、前記609ステップの第3の関数に対応し得る。

【0096】

前記の611ステップの確認の結果、これらが一致しないと、車両制御器20は、所定の乱数生成器を通じて乱数を生成し、生成された乱数を第3の応答キー B_ECU として設定して外部装置10に伝送することができる(S618~S619)。この場合、外部装置10では、内部に生成された第4の応答キー B_Tester と車両制御器20から受信された第3の応答キー B_ECU とが互いに異なることを確認し、車両制御器20の認証に失敗したと判断することができる。

【0097】

図7は、本発明の一実施例に係る外部装置での相互認証方法を説明するためのフローチャートである。

【0098】

図7を参照すると、外部装置10は、認証要請メッセージを車両制御器20に伝送することができる(S701)。ここで、認証要請メッセージには、外部装置10によって生成された乱数 R が含まれて伝送され得る。

【0099】

外部装置10は、車両制御器20から乱数 S が受信されると、乱数 S を媒介変数とする第1の関数を用いて反復回数である変数 i を生成することができる(S703~S705)。

【0100】

外部装置10は、生成された変数 i 、予め保存された保安キー K 及び乱数 S を媒介変数とする第2の関数を用いて第1のセッションキー K_S を生成することができる(S707)。

【0101】

続いて、外部装置10は、乱数 S 、変数 i 及び第1のセッションキー K_S を媒介変数とする第3の関数を用いて第3の応答キー A_Tester を生成した後、生成された第3の応答キー A_Tester を車両制御器200に伝送することができる(S709)。認証要請メッセージに乱数 R が含まれる場合、外部装置10は、乱数 R をさらに用いて第1の応答キー A_Tester を生成することも可能であることに注意すべきである。

【0102】

外部装置10は、第1の応答キー A_Tester 及び変数 i を媒介変数とする第4の関数を用いて変数 j を生成し、前記変数 j 及び第1のセッションキー K_S を媒介変数とする第5の関数を用いて第2のセッションキー K_{S_2} を生成することができる(S711)。

。

10

20

30

40

50

【0103】

ここで、第4の関数は、第1の応答キーA__T e s t e rを変数iだけ左側に循環前置させる関数であり得る。また、第5の関数は、前記707ステップの第2の関数と同様に、変数j、第1のセッションキーK_s及び乱数Sを媒介変数として前記の図3または図4に示したセッションキー生成手順を行う関数であり得る。

【0104】

外部装置10は、乱数S、変数j、第2のセッションキーK_{s2}を媒介変数とする第6の関数を用いて第4の応答キーB__T e s t e rを生成することができる(S713)。ここで、第6の関数は、前記図5に示した応答キー生成手順を行う関数であって、前記709ステップの第3の関数に対応し得る。

10

【0105】

外部装置10は、車両制御器20から第3の応答キーB__E C Uが受信されると、既に生成された第4の応答キーB__T e s t e rと第3の応答キーB__E C Uとが一致するかどうかを確認することができる(S714～S715)。

【0106】

確認の結果、第4の応答キーB__T e s t e rと第3の応答キーB__E C Uとが一致すると、外部装置10は、車両制御器20の認証に成功したと判断することができる(S717)。その一方、確認の結果、第4の応答キーB__T e s t e rと第3の応答キーB__E C Uとが一致しないと、外部装置10は、車両制御器20の認証に失敗したと判断することができる(S719)。

20

【0107】

本発明が本発明の精神及び必須的特徴から逸脱しない範囲で他の特定の形態に具体化され得ることは、当業者にとって自明である。

【0108】

したがって、前記の詳細な説明は、全ての面で制限的に解釈してはならず、例示的なものとして考慮しなければならない。本発明の範囲は、添付の請求項の合理的解釈によって決定しなければならない。本発明の均等の範囲内での全ての変更は本発明の範囲に含まれる。

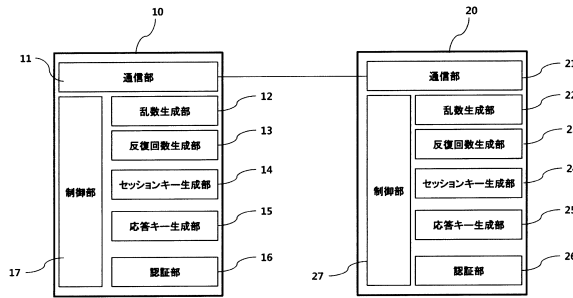
【符号の説明】

【0109】

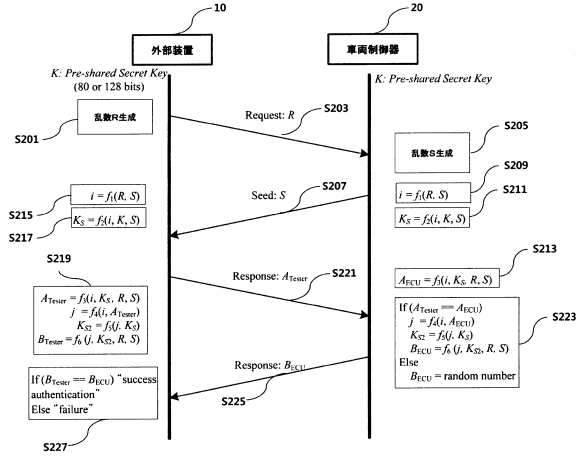
30

- 10 外部装置
- 20 車両制御器
- 12、22 乱数生成部
- 13、23 反復回数生成部
- 14、24 セッションキー生成部
- 15、25 応答キー生成部
- 16、26 認証部

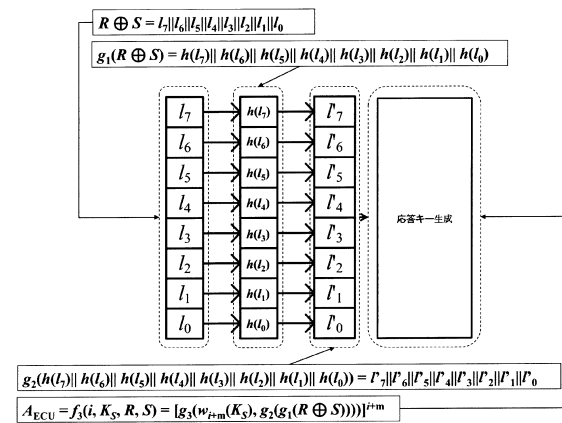
【図 1】



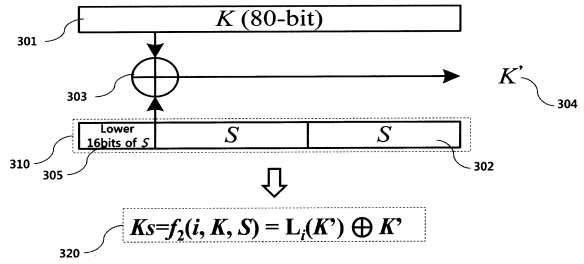
【図 2】



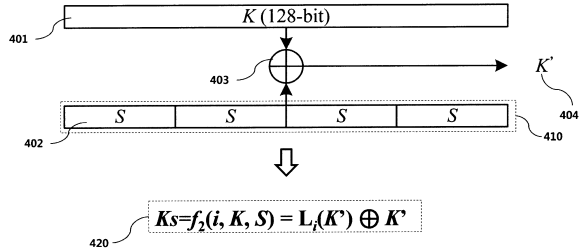
【図 5】



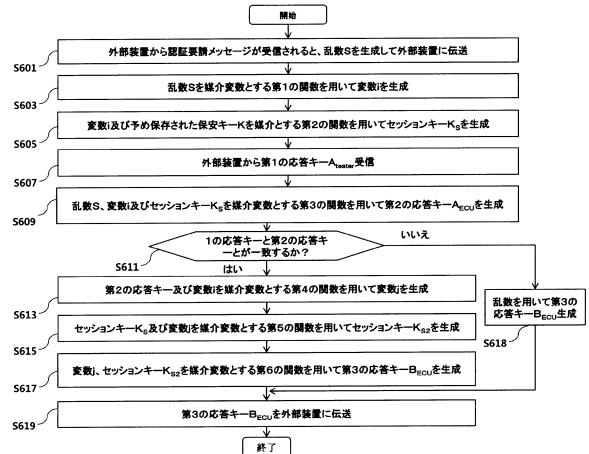
【図 3】



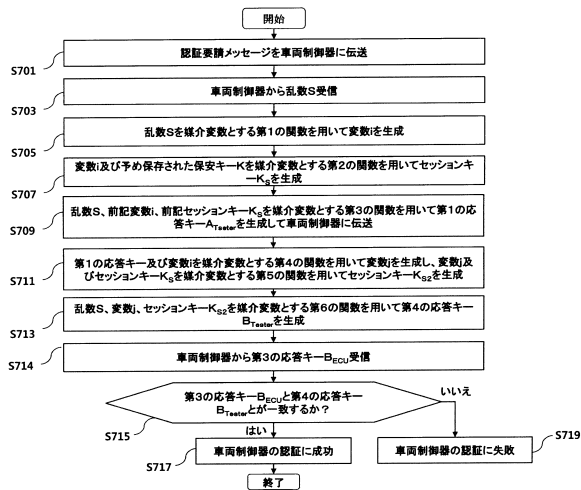
【図 4】



【図 6】



【図 7】



フロントページの続き

(74)代理人 100124372

弁理士 山ノ井 傑

(73)特許権者 500518050

起亜自動車株式会社

KIA MOTORS CORPORATION

大韓民国ソウル特別市瑞草区獻陵路12

12, Heolleung-ro, Seocho-gu, Seoul, Republic
of Korea

(73)特許権者 515140130

インダストリーアカデミック、コーオペレーション、ファウンダーション、チョスン、ユニバー
シティー

INDUSTRY-ACADEMIC COOPERATION FOUNDATION, CH
OSUN UNIVERSITY

大韓民国クァンジュ、トング、ピルムンデロ、309

(73)特許権者 513246872

ソウル大学校産学協力団

SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION

大韓民国 ソウル 08826 クァナクグ クァナクロー 1

(74)代理人 100117787

弁理士 勝沼 宏仁

(74)代理人 100127465

弁理士 堀田 幸裕

(74)代理人 100124372

弁理士 山ノ井 傑

(72)発明者 アン、ヒョン、ス

大韓民国ソウル特別市、ソンパング、オリンピッククロー、35-ギル、104、27-407

(72)発明者 チョン、ホ、ジン

大韓民国ソウル特別市、クムチョング、シフンデロ、165、210-904

(72)発明者 ウ、ジュン、ヤン

大韓民国ソウル特別市、ソチョグ、サピョンデロ、240、501-101

(72)発明者 キム、ホ、ヨン

大韓民国ソウル特別市、ヨンドゥンポグ、ククジェクムユンロー、109、エイ-802

(72)発明者 イ、カン、ソク

大韓民国キョンギード、コヤンシ、イルサンソグ、テファ、2-ロ、68、204-1004

(72)発明者 ユン、ジョン、ユン

大韓民国キョンギード、ヨンインシ、スジグ、ヒョナムロー、3、105-1004

(72)発明者 ノ、ジョン、ソン

大韓民国ソウル特別市、カンナムグ、クァンピョンロー、10-ギル、15、109-406

(72)発明者 キム、ヤン、シク

大韓民国クァンジュ、ソグ、プナム、2-ロ、36、105-903

審査官 赤穂 州一郎

(56)参考文献 国際公開第2013/014778 (WO, A1)

特開2009-284086 (JP, A)

特開2012-104049 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L	9/32
G06F	21/44
G09C	1/00