(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7372975号
(P7372975)

(45)発行日　令和5年11月1日(2023.11.1)

(24)登録日　令和5年10月24日(2023.10.24)

(51)国際特許分類

		FI		
H04L 12/40 (2006.01)		H04L	12/40	Z
H04L 12/28 (2006.01)		H04L	12/28	100A

請求項の数　14　（全14頁）

(21)出願番号　特願2021-534678(P2021-534678)
(86)(22)出願日　令和1年11月27日(2019.11.27)
(65)公表番号　特表2022-513496(P2022-513496A)
(43)公表日　令和4年2月8日(2022.2.8)
(86)国際出願番号　PCT/EP2019/082704
(87)国際公開番号　WO2020/126365
(87)国際公開日　令和2年6月25日(2020.6.25)
審査請求日　令和3年8月16日(2021.8.16)
(31)優先権主張番号　102018221954.0
(32)優先日　平成30年12月17日(2018.12.17)
(33)優先権主張国・地域又は機関
ドイツ(DE)
前置審査

(73)特許権者　591245473
ロベルト・ボッシュ・ゲゼルシャフト・ミト・ベシュレンクテル・ハフツング
ROBERT BOSCH GMBH
ドイツ連邦共和国 70442 シュトゥットガルト ポストファッハ 30 02 20
(74)代理人　100118902
弁理士　山本 修
(74)代理人　100196508
弁理士　松尾 淳一
(72)発明者　ポール，クリストファー
ドイツ国 40489 デュッセルドルフ，アンガームンダー・シュトラーセ 66
(72)発明者　シュトゥンプフ，フレデリック
最終頁に続く

(54)【発明の名称】　演算装置および演算装置の作動方法

(57)【特許請求の範囲】

【請求項１】

自動車の制御装置（７００）のための演算装置（１００；１００ａ）であって、前記演算装置（１００；１００ａ）は、少なくとも１つの外部ユニット（２００）からメッセージ（Ｎ）を受信する（３００）ように構成されており、前記演算装置（１００；１００ａ）は、前記受信メッセージ（Ｎ）を少なくとも一時的に記憶し（３０２）、前記受信メッセージ（Ｎ）の複数個（Ｎ’）を、伝送されたメッセージ（Ｎ）の検証（５０２）を実施するように構成された暗号モジュール（４００；４００’）に伝送する（３０４）ように構成されており、

前記演算装置（１００；１００ａ）は、前記受信メッセージがまだ前記暗号モジュール（４００；４００’）によって検証されて（５０２）いない場合、受信メッセージの処理（３０８）を実施しないように構成され、

前記暗号モジュール（４００；４００’）は、前記複数個（Ｎ’）のメッセージの検証（５０２）が全て完了したのちに、前記検証（５０２）の結果（Ｅ）を前記演算装置（１００；１００ａ）に伝達し、

前記演算装置（１００；１００ａ）は、前記暗号モジュール（４００；４００’）の前記検証（５０２）の前記結果（Ｅ）を受信し（３０６）、前記検証（５０２）の前記結果（Ｅ）に依存して前記受信メッセージ（Ｎ）の前記複数個（Ｎ’）のうちの少なくとも１つを処理する（３０８）ように構成されている、演算装置（１００；１００ａ）。

【請求項２】

前記演算装置（１００；１００ａ）は、前記受信メッセージ（Ｎ）の前記複数個（Ｎ’）を前記暗号モジュール（４００；４００’）に伝送する（３１２）前に、受信メッセージの所定の最小数を待機する（３１０）ように構成されている、請求項１に記載の演算装置（１００；１００ａ）。

【請求項３】

前記演算装置（１００；１００ａ）は、前記受信メッセージ（Ｎ）の前記複数個（Ｎ’）を所定の期間の間、前記暗号モジュール（４００；４００’）に伝送する（３２２）前に、所定の期間待機する（３２０）ように構成されている、請求項１または２に記載の演算装置（１００；１００ａ）。

【請求項４】

受信メッセージ（Ｎ）を少なくとも一時的に記憶すること（３０２）は、前記演算装置（１００；１００ａ）と前記暗号モジュール（４００；４００’）の両方からアクセス可能な記憶装置（１０４’）に前記受信メッセージ（Ｎ）を少なくとも一時的に記憶すること（３０２０）を含み、前記伝送（３０４；３１２；３２２）は、次のステップ、すなわち、前記受信メッセージ（Ｎ）が記憶されている前記記憶装置（１０４’）の記憶領域を特徴づける第１の制御情報（Ｓ１）を引き渡す（３０２２）ステップを含む、請求項１から３のいずれか一項に記載の演算装置（１００；１００ａ）。

【請求項５】

前記第１の制御情報（Ｓ１）は、前記受信メッセージ（Ｎ）のポインタおよび／または個数の少なくとも１つを含む、請求項４に記載の演算装置（１００；１００ａ）。

【請求項６】

前記演算装置（１００；１００ａ）は、第２の制御情報を前記暗号モジュール（４００；４００’）に引き渡すように構成されており、前記第２の制御情報は、前記暗号モジュール（４００；４００’）がその記憶領域またはそのアドレスに前記検証（５０２）の前記結果（Ｅ）を書き込む前記記憶装置（１０４’）内の記憶領域またはアドレスを特徴づける、請求項４または５に記載の演算装置（１００；１００ａ）。

【請求項７】

前記暗号モジュール（４００；４００’）は前記演算装置（１００；１００ａ）に統合されている、および／または、前記暗号モジュール（４００；４００’）は前記演算装置（１００；１００ａ）と同じ半導体基板（６００）上に配置されている、請求項１から６のいずれか一項に記載の演算装置（１００；１００ａ）。

【請求項８】

自動車の制御装置（７００）のための演算装置（１００；１００ａ）の作動方法であって、前記演算装置（１００；１００ａ）は、少なくとも１つの外部ユニット（２００）からメッセージ（Ｎ）を受信し（３００）、前記演算装置（１００；１００ａ）は、前記受信メッセージ（Ｎ）を少なくとも一時的に記憶し（３０２）、前記受信メッセージ（Ｎ）の複数個（Ｎ’）を、伝送されたメッセージ（Ｎ’）の検証（５０２）を実施するように構成された暗号モジュール（４００；４００’）に伝送し（３０４）、

前記演算装置（１００；１００ａ）は、前記受信メッセージがまだ前記暗号モジュール（４００；４００’）によって検証されて（５０２）いない場合、受信メッセージの処理（３０８）を実施しないように構成され、

前記暗号モジュール（４００；４００’）は、前記複数個（Ｎ’）の検証（５０２）が全て完了したのちに、前記検証（５０２）の結果（Ｅ）を前記演算装置（１００；１００ａ）に送信し、

前記演算装置（１００；１００ａ）は、前記暗号モジュール（４００；４００’）の前記検証（５０２）の前記結果（Ｅ）を受信し（３０６）、前記検証（５０２）の前記結果（Ｅ）に依存して前記受信メッセージ（Ｎ）の前記複数個（Ｎ’）のうちの少なくとも１つを処理する（３０８）ように構成されている、方法。

【請求項９】

請求項１から７のいずれか一項に記載の演算装置（１００；１００ａ）用の暗号モジュ

ール（４００；４００’）であって、前記暗号モジュール（４００；４００’）は、前記演算装置（１００；１００ａ）から複数個（Ｎ’）のメッセージを受信し（５００）、前記受信メッセージの検証を実施する（５０２）ように構成されており、
前記演算装置（１００；１００ａ）は、前記受信メッセージがまだ前記暗号モジュール（４００；４００’）によって検証されて（５０２）いない場合、受信メッセージの処理（３０８）を実施しないように構成されている、暗号モジュール（４００；４００’）。
【請求項１０】
前記検証の実施（５０２）は、鍵ベースのメッセージ認証コードであるＣＭＡＣ、英語：Ｃｉｐｈｅｒ－ｂａｓｅｄ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ、を用いて行われる、請求項９に記載の暗号モジュール（４００；４００’）。
【請求項１１】
前記暗号モジュール（４００；４００’）は、前記検証（５０２）の結果（Ｅ）を前記演算装置（１００；１００ａ）に送信する（５０４）ように構成されており、前記送信（５０４）は、前記演算装置（１００；１００ａ）と前記暗号モジュール（４００；４００’）の両方がアクセス可能な記憶装置（１０４’）の所定の記憶領域に、前記結果（Ｅ）を特徴づける結果情報を書き込むことを含む、請求項９または１０に記載の暗号モジュール（４００；４００’）。
【請求項１２】
自動車のバスシステムを介して伝送されるメッセージ（Ｎ）を処理するための、請求項１から７のいずれか一項に記載の演算装置（１００；１００ａ）の使用。
【請求項１３】
自動車のバスシステムを介して伝送されるメッセージ（Ｎ）を処理するための、請求項８に記載の方法の使用。
【請求項１４】
自動車のバスシステムを介して伝送されるメッセージ（Ｎ）を処理するための、請求項９から１１のいずれか一項に記載の暗号モジュールの使用。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、演算装置、特に自動車の制御装置のための演算装置に関し、演算装置は、少なくとも１つの外部ユニットからメッセージを受信するように構成されている。
また、本開示は、そのような演算装置の作動方法に関する。
【発明の概要】
【課題を解決するための手段】
【０００２】
好ましい実施形態は、特に自動車の制御装置のための演算装置に関し、演算装置は、少なくとも１つの外部ユニット、例えばさらなる制御装置からメッセージを受信するように構成されており、演算装置は、受信メッセージを少なくとも一時的に記憶し、受信メッセージの複数個を、伝送されたメッセージの検証を実施するように構成された暗号モジュールに伝送するように構成されている。このようにして、複数の伝送メッセージの検証を効率的に行うことができる。
【０００３】
さらなる好ましい実施形態では、演算装置は、暗号モジュールの検証結果を受信し、検証結果に依存して受信メッセージの複数個のうちの少なくとも１つを処理するように構成されている。
【０００４】
さらなる好ましい実施形態では、演算装置は、受信メッセージの複数個を暗号モジュールに伝送する前に、受信メッセージの所定の最小数を待機するように構成されている。
【０００５】
さらなる好ましい実施形態では、演算装置は、受信メッセージの複数個を特に所定の期

間の間、暗号モジュールに伝送する前に、所定の期間待機するように構成されている。
【０００６】
さらなる好ましい実施形態では、受信メッセージを少なくとも一時的に記憶することは、演算装置と暗号モジュールの両方からアクセス可能な記憶装置に受信メッセージを少なくとも一時的に記憶することを含み、伝送は、受信メッセージが記憶されている記憶装置の記憶領域を特徴づける第１の制御情報を引き渡すステップを含む。
【０００７】
さらなる好ましい実施形態では、第１の制御情報は、受信メッセージのポインタおよび／または個数の少なくとも１つを含む。
【０００８】
さらなる好ましい実施形態では、演算装置は、第２の制御情報を暗号モジュールに引き渡すように構成されており、第２の制御情報は、暗号モジュールがその記憶領域またはそのアドレスに検証結果を書き込むべき記憶装置内の記憶領域またはアドレスを特徴づける。
【０００９】
さらなる好ましい実施形態では、演算装置は、受信メッセージがまだ暗号モジュールによって検証されていない場合、受信メッセージの処理を実施しないように構成されている。これにより、暗号モジュールで検証されたメッセージのみが処理されることが確実になる。
【００１０】
さらなる好ましい実施形態では、暗号モジュールは演算装置に統合されている、および／または、暗号モジュールは演算装置と同じ半導体基板上に配置され、これにより、特に小さい組立構成が実現される。
【００１１】
さらなる好ましい実施形態では、演算装置は、外部ユニットからの受信メッセージＮの代替または補足として、一般的に他のソースからデータまたはメッセージ（例えば、演算装置自体によって形成されたデータまたはメッセージも）を受信または特定し、任意選択的に、それらを、暗号法を使用して処理し、または処理させ（特に暗号モジュールによって）処理させ、例えば、それらに暗号署名を提供する、または提供させるように構成される。このために、さらなる好ましい実施形態では、演算装置は、（他のソースから得られたおよび／または自分で形成した）メッセージを、好ましくは上記の複数のメッセージを暗号モジュールに伝送することができ、さらなる好ましい実施形態では、暗号モジュールは、これらのメッセージに（例えば、上述の検証の代わりに）暗号署名を提供し、好ましくは、まず、上記の複数のメッセージの全てに署名を提供し、さらなる好ましい実施形態では、次に、署名を有するメッセージを演算装置に伝送し、演算装置はさらなる好ましい実施形態では、次に、署名されたメッセージを、例えば、さらなる演算装置または制御装置に伝送する。
【００１２】
さらなる好ましい実施形態は、演算装置、特に自動車の制御装置の作動方法であって、演算装置は、少なくとも１つの外部ユニットからメッセージを受信し、演算装置は、受信メッセージを少なくとも一時的に記憶し、受信メッセージの複数個を、伝送されたメッセージの検証を実施するように構成された暗号モジュールに伝送する方法に関する。
【００１３】
さらなる好ましい実施形態は、演算装置用の暗号モジュール、特に実施形態にかかる演算装置用の暗号モジュールに関し、暗号モジュールは、演算装置から複数のメッセージを受信し、受信メッセージの検証を実施するように構成されている。
【００１４】
さらなる好ましい実施形態では、検証の実施は、鍵ベースのメッセージ認証コードであるＣＭＡＣ（英語：Ｃｉｐｈｅｒ－ｂａｓｅｄ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を用いて行われる。これにより、特に効率的な検証が可能になる。ＣＭＡＣ法の例示的な構成に関連するインターネット出版物は、例えば、ｈｔｐｓ：／／ｄ

ｏｉ．ｏｒｇ／ｔ０．８０２８％２Ｆｎｉｓｔ．ｓｐ．８００－３８ｂで取得可能である。
【００１５】
さらなる好ましい実施形態では、暗号モジュールは、検証結果を演算装置に送信するように構成されており、送信は、特に、演算装置と暗号モジュールの両方がアクセス可能な記憶装置の所定の記憶領域に、結果を特徴づける結果情報を書き込むことを含むことができる。
【００１６】
さらなる好ましい実施形態は、メッセージ、特に車両、特に自動車のバスシステムを介して伝送されるメッセージを処理するための、実施形態にかかる演算装置の使用、および／または実施形態にかかる方法の使用、および／または実施形態にかかる暗号モジュールの使用に関する。
【００１７】
本発明のさらなる特徴、使用範囲、および利点は、図面の図に示された本発明の実施例の以下の説明からわかる。ここで、記載または図示された全ての特徴は、請求項におけるそれらの要約もしくはそれらの引用関係に関わらず、および、説明もしくは図面におけるそれらの記載もしくは表現に関わらず、それ自体または任意の組み合わせで本発明の主題を構成する。
【図面の簡単な説明】
【００１８】
【図１】好ましい実施形態にかかる演算装置の簡略化したブロック図を模式的に示した図。
【図２】さらなる好ましい実施形態にかかる方法の簡略化したフロー図を模式的に示した図。
【図３】さらなる好ましい実施形態にかかる方法の簡略化したフロー図を模式的に示した図。
【図４】さらなる好ましい実施形態にかかる方法の簡略化したフロー図を模式的に示した図。
【図５】図５Ａは、さらなる好ましい実施形態にかかる方法の簡略化したフロー図を模式的に示した図。図５Ｂは、さらなる好ましい実施形態にかかる方法の簡略化したフロー図を模式的に示した図。
【図６】さらなる好ましい実施形態にかかる演算装置の簡略化したブロック図を模式的に示した図。
【図７】さらなる好ましい実施形態にかかる演算装置の簡略化したブロック図を模式的に示した図。
【図８】さらなる好ましい実施形態にかかる半導体基板の簡略化したブロック図を模式的に示した図。
【図９】さらなる好ましい実施形態にかかる制御装置の簡略化したブロック図を模式的に示した図。
【発明を実施するための形態】
【００１９】
図１は、好ましい実施形態にかかる演算装置１００の簡略化したブロック図を模式的に示す。演算装置１００は、例えば制御装置などの少なくとも１つの外部ユニット２００からメッセージＮ（または一般的に任意のデータ）を受信し、受信メッセージＮを少なくとも一時的に記憶し、受信メッセージＮの複数個Ｎ’を暗号モジュール４００に伝送するように構成されており、この暗号モジュール４００は、伝送されたメッセージＮ’の検証を実施するように構成されている。このようにして、伝送された複数のメッセージＮ’の効率的な検証を行うことができ、メッセージの複数個Ｎ’は、例えば、個々のメッセージを繰り返し伝送するのとは対照的に、例えば、関連したデータブロックとして、特にリソース効率の高い方法で、演算装置１００によって暗号モジュール４００に伝送することができる。
【００２０】
図２は、さらなる好ましい実施形態にかかる方法の簡略化したフロー図を模式的に示す

。ステップ３００では、装置１００（図１）は、外部ユニット２００から（または、図示しない複数の異なるユニットから）メッセージＮ（または、一般的に任意のデータ）を受信する。ステップ３０２では、演算装置１００は、受信メッセージＮを少なくとも一時的に記憶する。ステップ３０４において、演算装置１００は、検査のために受信メッセージの複数個Ｎ’を暗号モジュール４００に伝送する。

【００２１】

さらなる好ましい実施形態では、演算装置１００は、図２の任意選択的なステップ３０６を参照すると、暗号モジュール４００から検証結果Ｅ（図１）を受信し、図２の任意選択的なステップ３０８を参照すると、検証結果Ｅに依存して、受信メッセージＮの複数個のうちの少なくとも１つを処理するように構成されている。

【００２２】

さらなる好ましい実施形態では、演算装置１００は、ステップ３０４の伝送後、特にステップ３０６にかかる結果Ｅを受信する前に、他のタスクを実施してもよく、これにより、暗号モジュール４００が以前に決定された検査対象メッセージを検証するために場合によって必要となる期間は、演算装置１００によって別の方法で使用されてもよい。例えば、暗号モジュール４００によって以前に通信された結果、または関連する受信メッセージは、時間帯に演算装置１００によって処理されてもよい。

【００２３】

図３は、暗号モジュール４００によるメッセージの処理を説明する、さらなる好ましい実施形態にかかる方法の簡略化したフロー図を模式的に示す。ステップ５００では、暗号モジュール４００は、ステップ３０４で演算装置１００から暗号モジュール４００に伝送された、メッセージの複数個Ｎ’を受信する。ステップ５０２では、暗号モジュール４００は、演算装置１００からの受信メッセージの検証を実施する。さらなる好ましい実施形態では、図３のステップ５０２による検証の実施は、鍵ベースのメッセージ認証コードであるＣＭＡＣを用いて行われる。例えば、該当する検証対象メッセージに対して、暗号モジュール４００がアクセスできるＣＭＡＣ参照値を提供してもよい。検証するステップ５０２について、暗号モジュール４００は、有利には、ＣＭＡＣ法を用いて、検証対象受信メッセージに依存して現在のＣＭＡＣ値を形成し、それをＣＭＡＣ参照値と比較することができる。比較が、比較された値がお互いに同じであることを示す場合、暗号モジュール４００は、検証メッセージが真であると推測し、検証の対応する結果Ｅを提供することができる。比較された値がお互いに一致しない場合、現在受信されて検証されたメッセージは正常ではなく、例えば不正操作されている（および／または意図せずに破損している）と推測することができる。

【００２４】

さらなる好ましい実施形態では、検証５０２のための１つまたは複数の参照値、特に暗号モジュール４００による検証対象のメッセージのための１つまたは複数のＣＭＡＣ参照値が、演算装置１００によって暗号モジュール４００に提供されてもよい。例えば、演算装置１００は、参照値またはＣＭＡＣ参照値を、検証対象メッセージの複数個Ｎ’とともに、暗号モジュール４００に伝送してもよい。

【００２５】

さらなる好ましい実施形態では、このために、例えば以下のようなデータ形式を使用することができる。検査対象のメッセージ（「平文」）にインデックス値が割り当てられ、このインデックス値により、検査対象メッセージの複数個Ｎ’の中でメッセージを一意に識別することができる。任意選択的に、検査対象メッセージに（ＣＭＡＣ）参照値が割り当てられる。さらに任意選択的に、検証対象のメッセージには、検証対象のメッセージに関連する特定の暗号鍵を特徴づける鍵情報（「鍵ＩＤ」）が割り当てられる。したがって、さらなる好ましい実施形態では、上記に例示したデータ形式のデータセットは、次の要素、すなわち、ａ）インデックス値、ｂ）メッセージコンテンツ（「平文」）、ｃ）（ＣＭＡＣ）参照値、ｄ）鍵情報（「鍵ＩＤ」）のうち、少なくとも１つの要素を含んでもよい。さらなる好ましい実施形態では、伝送するステップ３０４（図２）において、さらなる

好ましい実施形態にかかる検証対象メッセージに加えて、例示的に記載されたデータ形式の前述の要素ａ）、ｃ）、ｄ）のうちの１つまたは複数個を暗号モジュール４００へ伝送してもよく、再び有利には、メッセージの複数個Ｍ’またはメッセージの前述の複数個Ｍ’に相当する、対応する前述のデータセットの複数個を暗号モジュール４００に伝送してもよい。

【００２６】

図３にかかるステップ５０４において、暗号モジュール４００は、検査５０２（図３）の結果Ｅ（図１）を演算装置１００に送信し、ここで演算装置１００は、結果Ｅに依存して任意選択的なステップ３０６および／または３０８を用いて、図２を参照して既に上述した方法を継続することができる。

【００２７】

さらなる好ましい実施形態では、演算装置１００から暗号モジュール４００へのメッセージの複数個Ｎ’の伝送３０２（図２）によって、暗号モジュール４００が演算装置１００とさらに通信することなく（または、演算装置１００との通信のためにメッセージの複数個Ｎ’の検査を中断することなく）、例えば検査対象の個々のさらなるメッセージを再ロードするために、複数の伝送されたメッセージを一度に検査できるという点で、さらなる利点がもたらされる。むしろ、メッセージの複数個Ｎ’は、まず、図３にかかるステップ５０２を参照して説明した方法で、暗号モジュール４００内で検証され、上記複数個Ｎ’の検証が完了した後に初めて、結果Ｅを演算装置１００に伝達することができる。

【００２８】

さらなる好ましい実施形態では、図４の簡略化されたフロー図を参照すると、演算装置１００は、受信メッセージの複数個Ｎ’（図１）が暗号モジュール４００に伝送される前に、ステップ３１０を参照すると、所定の最小数の受信メッセージを待機するように構成されている。これにより、複数の受信メッセージは、有利には、演算装置１００によって束ねられ、１つの伝送プロセスで暗号モジュール４００に伝送することができる。

【００２９】

さらなる好ましい実施形態では、図５Ａの簡略化されたフロー図を参照して、演算装置１００は、ステップ３２２を参照すると、特に所定の期間中に受信したメッセージの複数個Ｎ’が暗号モジュール４００に伝送される前に、ステップ３２０を参照すると、所定の期間待機するように構成されている。これにより、有利には、演算装置１００で少なくとも１つのさらなるユニット２００から受信した複数のメッセージＮを、これを検証の目的で複数個Ｎ’の形で暗号モジュール４００に伝送する前に、束ねることができる。

【００３０】

さらなる好ましい実施形態では、図５Ｂにかかる簡略化されたフロー図を参照すると、演算装置１００による受信メッセージを少なくとも一時的に記憶することは、演算装置１００と暗号モジュール４００の両方がアクセス可能な記憶装置に受信メッセージを少なくとも一時的に記憶すること３０２０を含み、伝送３０２２は、受信メッセージが記憶されている記憶装置の記憶領域を特徴づける第１の制御情報Ｓ１（図１）を引き渡すステップを含む。例えば、第１の制御情報Ｓ１は、記憶装置の対応する記憶領域への少なくとも１つのポインタを含んでいてもよい。

【００３１】

さらなる好ましい実施形態では、検証対象のメッセージの複数Ｍ’を伝送することに加えて、さらに、それぞれのメッセージに対応付けられた１つまたは複数の要素、ａ）インデックス値、ｃ）（ＣＭＡＣ）参照値、ｄ）鍵情報（「鍵ＩＤ」）を、この方法で暗号モジュール４００に効率的に伝送することもできる。

【００３２】

図６は、さらなる好ましい実施形態にかかる簡略化したブロック図を模式的に示す。例えば、図１の演算装置１００は、図６にかかる構成１００ａを有していてもよい。構成１００ａは、少なくとも１つの演算ユニット１０２と、コンピュータプログラムＰＲＧを少なくとも一時的に記憶するために演算装置１０２に対応付けられた少なくとも１つの記憶

装置１０４とを有し、コンピュータプログラムＰＲＧは、特に演算装置１００または構成１００ａの作動を制御するために、特に実施形態にかかる方法を実施するために構成されている。

【００３３】

さらなる好ましい実施形態では、演算ユニット１０２は、次の要素、すなわち、マイクロプロセッサ、マイクロコントローラ、デジタルシグナルプロセッサ（ＤＳＰ）、プログラマブルロジック装置（例えば、ＦＰＧＡ、フィールドプログラマブルゲートアレイ）、ＡＳＩＣ（特定用途向け集積回路）、ハードウェア回路の要素のうちの少なくとも１つを有する。また、これらの組み合わせは、さらなる好ましい実施形態でも考えられる。

【００３４】

さらなる好ましい実施形態では、記憶装置１０４は、次の要素、すなわち、揮発性メモリ１０４ａ、特にワーキングメモリ（ＲＡＭ）、不揮発性メモリ１０４ｂ、特にフラッシュＥＥＰＲＯＭ、の要素のうちの少なくとも１つを有する。好ましくは、コンピュータプログラムＰＲＧは、不揮発性メモリ１０４ｂに格納されている。

【００３５】

また、さらなる好ましい実施形態では、演算装置１００、１００ａおよび暗号モジュール４００の両方によってアクセス可能な、既に上述した記憶装置１０４’が設けられている。同様に、既に記載したように、さらなる好ましい実施形態では、演算装置１００、１００ａによって受信されたメッセージＮは、記憶装置１０４’に少なくとも一時的に記憶されてもよい。さらなる好ましい実施形態では、受信対象メッセージのための少なくとも１つの受信バッファが、このために定義されてもよい。

【００３６】

さらなる好ましい実施形態では、記憶装置１０４’はまた、記憶装置１０４の一部を形成するか、またはこれに統合されていてもよい。このようにして、演算装置１００から暗号モジュール４００へ、メッセージＮを特に効率的に伝送することができる。例えば、さらなる好ましい実施形態では、演算装置１００から第１の制御情報Ｓ１を暗号モジュール４００に伝送することは、暗号モジュール４００が記憶装置１０４’から検証対象のメッセージを読み出す、またはロードするのに十分であり得る。

【００３７】

さらなる好ましい実施形態では、第１の制御情報Ｓ１は、少なくとも１つのポインタ（例えば、検証対象メッセージＮを含む記憶装置１０４’の記憶領域へのポインタ）および／または受信メッセージの個数を含む。

【００３８】

さらなる好ましい実施形態では、演算装置１００、１００ａは、第２の制御情報Ｓ２（図１）を暗号モジュール４００に伝送するように構成されており、第２の制御情報Ｓ２は、その記憶領域またはそのアドレスに暗号モジュール４００が検証５０２（図３）の結果Ｅ（図１）を書き込むべき記憶装置１０４’内の記憶領域またはアドレスを特徴づける。

【００３９】

さらなる好ましい実施形態では、演算装置１００、１００ａは、受信メッセージが暗号モジュール４００によってまだ検証されていない場合、受信メッセージＮの処理を実施しないように構成されている。これにより、暗号モジュール４００によって検証されたメッセージのみが処理されることが確実になる。

【００４０】

さらなる好ましい実施形態では、図７にかかる簡略化されたブロック図を参照すると、暗号モジュール４００’が演算装置１００ａに統合されている。

【００４１】

さらなる好ましい実施形態では、図８にかかる簡略化されたブロック図を参照すると、暗号モジュール４００は演算装置１００と同じ半導体基板６００上に配置されており、これにより、特に小さい組立構成が実現される。

【００４２】

さらなる好ましい実施形態では、暗号モジュール４００、４００’は、検査５０２（図３）の結果Ｅを演算装置１００、１００ａに送信するように構成され、送信は、特に、演算装置１００、１００ａと暗号モジュール４００、４００’の両方がアクセス可能な記憶装置１０４’（図６）の所定の記憶領域に、結果Ｅを特徴づける結果情報を書き込むことを含む。さらなる好ましい実施形態では、複数のＭ’の異なるメッセージに対応付けられた結果Ｅの異なる結果値は、それぞれの結果値と対応する検証されたメッセージとの一義的な対応付けを可能にするために、例えば、既に上述したインデックス値によって補完されてもよい。

【００４３】

さらなる好ましい実施形態は、メッセージＮ（または一般的に任意のデータ）、特に車両、特に自動車のバスシステムを介して伝送されるメッセージを処理するための、実施形態にかかる演算装置１００、１００ａの使用、および／または実施形態にかかる方法の使用、および／または実施形態にかかる暗号モジュール４００、４００’の使用に関する。

【００４４】

さらなる好ましい実施形態では、図９にかかる概略ブロック図を参照すると、演算装置１００は、特に自動車用の制御装置７００の構成要素であり、任意選択的に、暗号モジュール４００も同様に制御装置７００の一部を形成することができる。

【００４５】

さらなる好ましい実施形態では、演算装置１００が、外部ユニット２００から受信するメッセージＮの代替的にまたは補完的に、一般的に他のソース（例えば、演算装置１００自身によっても形成される）からデータまたはメッセージを受信または特定し、これらを任意に、暗号化方法を用いて処理し、例えば、これらに暗号化署名を付与する。このために、演算装置１００は、図２を参照して上述したプロセスに匹敵するさらなる好ましい実施形態において、上述の（例えば、自己形成された）メッセージを暗号モジュール４００に伝送することができ、好ましくは再び上述のメッセージの複数個を伝送し、暗号モジュール４００は、図３を参照して上述した検証５０２の代わりに、これらのメッセージに暗号署名を付与し、好ましくは、最初に上述のメッセージの複数の全てに署名を付与し、その後、署名を付与されたメッセージを演算装置１００に伝送し、演算装置１００は、さらなる好ましい実施形態では、その後、署名されたメッセージを、例えばさらなる演算装置または制御装置に伝送することが可能である。さらなる好ましい実施形態では、図６を参照して上述した記憶装置１０４’は、署名のこの生成または追加、および演算装置１００と暗号モジュール４００との間の対応するデータ交換に使用されてもよく、両方の装置１００、４００によってアクセスされてもよい。換言すると、さらなる好ましい実施形態では、暗号モジュール４００による署名生成のために、演算装置１００との対応するデータ交換が、ポインタベースの方法で実施されることが可能であり、この場合、演算装置１００は、共用可能な記憶装置１０４’の応答する記憶領域への対応するポインタを暗号モジュール４００と交換し、この記憶領域は、例えば、署名を付与されるべきメッセージおよび／または署名を付与されたメッセージを含む。

【００４６】

実施形態にかかる原理は、演算装置１００、１００ａによるメッセージＮの特に効率的な処理を可能にする。これは、演算装置１００、１００ａにおける外部ユニット２００から受信されるメッセージの処理と、演算装置１００で形成または署名されるべきメッセージの処理の両方に該当する。メッセージの複数個Ｎ’の暗号モジュール４００への伝送および／または暗号モジュール４００によるメッセージの複数個Ｎ’の処理により、演算装置１００、１００ａの特に演算リソースが節約され、検査対象メッセージが演算装置によって個別に処理されるか、または暗号モジュール４００に伝送可能である従来のシステムで発生する通信オーバーヘッドが回避される。

【００４７】

また、実施形態にかかる原理を適用することで、特にセキュリティクリティカルな情報に関して、演算装置１００、１００ａから暗号モジュール４００への伝送動作を最小限に

できる、これによりセキュリティをさらに高めることができる。

【００４８】

さらなる好ましい実施形態では、メッセージの複数個Ｎ’は、待機される受信メッセージの所定の最小数（図４のステップ３１０を参照）および／または図５Ａのステップ３２０にかかる所定の期間と同様に、設定化またはパラメータ化することができる。これにより、本実施形態にかかる原理は、特にそれぞれの制御装置の通信負荷（時間あたりに処理すべきメッセージ数）および／または演算リソースおよび／または記憶リソースを考慮して、例えば制御装置などの異なる対象システムに効率的に適合させることができる。さらに、本実施形態にかかる原理は、演算装置１００、１００ａによるメッセージＮの処理の設定可能性に関して柔軟性が高い。

【図面】

【図１】

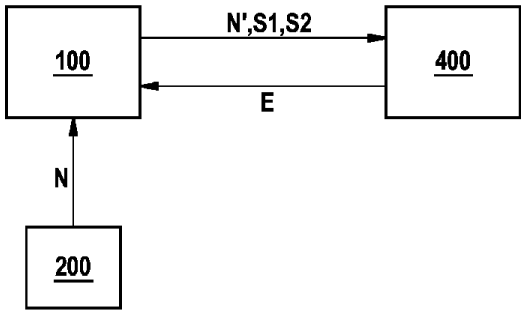

Fig. 1

【図２】

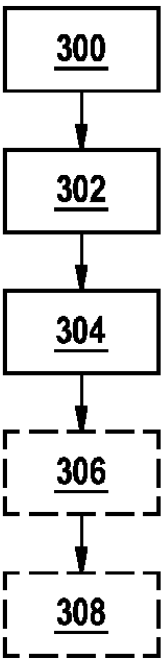

Fig. 2

【図３】

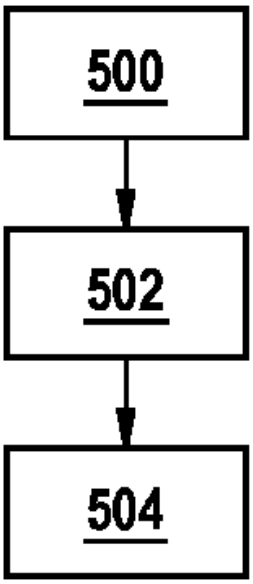

Fig. 3

【図４】

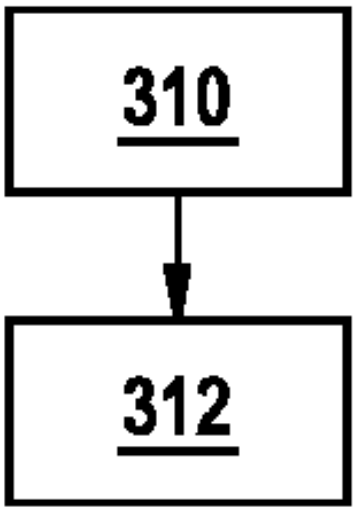

Fig. 4

【図５ａ】

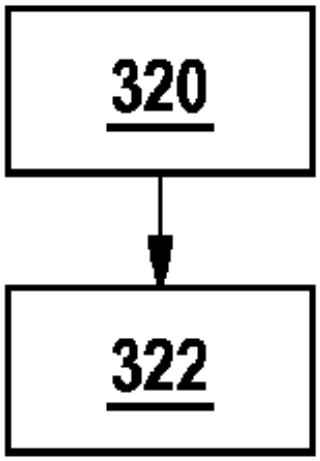

Fig. 5a

【図５ｂ】

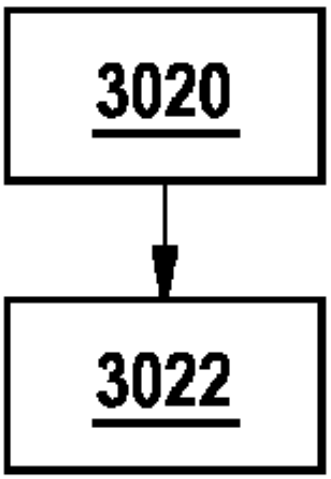

Fig. 5b

【図６】

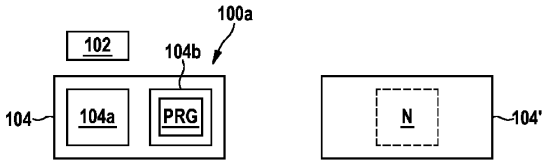

Fig. 6

【図７】

Fig. 7

【図８】

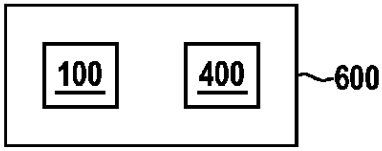

Fig. 8

【図９】

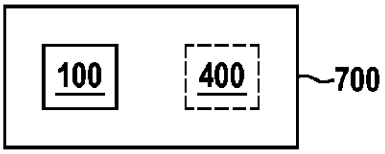

Fig. 9

フロントページの続き

ドイツ国 ７１２２９ レーオンベルク，エッシェンベーク ２１

審査官 野元 久道

(56)参考文献 特開２０１８－１３３７４３（ＪＰ，Ａ）
特表２０１８－５１１２４８（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／４０
Ｈ０４Ｌ １２／２８