(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6420176号
(P6420176)
(45)発行日　平成30年11月7日(2018.11.7)　(24)登録日　平成30年10月19日(2018.10.19)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A

請求項の数 16　(全 17 頁)

(21)出願番号　特願2015-36298(P2015-36298)
(22)出願日　平成27年2月26日(2015.2.26)
(65)公開番号　特開2016-158204(P2016-158204A)
(43)公開日　平成28年9月1日(2016.9.1)
審査請求日　平成29年11月27日(2017.11.27)

(73)特許権者　302062931
ルネサスエレクトロニクス株式会社
東京都江東区豊洲三丁目２番２４号
(74)代理人　100103894
弁理士　家入　健
(74)代理人　100089071
弁理士　玉村　静世
(72)発明者　押田　大介
神奈川県川崎市中原区下沼部１７５３番地
ルネサスエレクトロニクス株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】通信システムおよび通信装置

(57)【特許請求の範囲】
【請求項１】
ネットワークで相互接続され、前記ネットワークを介してパケットを送受可能な第１装置と第２装置とを含み、
前記第１及び第２装置は、それぞれ第１及び第２パケットカウンタを備え、
前記第１及び第２パケットカウンタは、初期値として同じ乱数値が与えられ、パケットの送受信に伴ってそれぞれ更新され、
前記第１装置は、前記第２装置にメッセージを伝送するときに、前記メッセージに基づいてメッセージ認証符号を生成し、その一部を前記第１パケットカウンタのカウント値に基づいて抜き出して分割メッセージ認証符号とし、前記メッセージと前記分割メッセージ認証符号とを含むパケットを生成して、前記ネットワークを介して前記第２装置に送信し、
前記第２装置は、前記パケットを受信したとき、受信したパケットに含まれるメッセージに基づいてメッセージ認証符号を生成し、その一部を前記第２パケットカウンタのカウント値に基づいて抜き出し、受信したパケットに含まれる前記分割メッセージ認証符号と比較することによってメッセージ認証を行い、
前記第１及び第２装置は、パケットの送受信ごとに、それぞれ、自身のパケットカウンタのカウンタ値から同じ計算方法で生成される値を増分値として、自身のパケットカウンタを更新する、
通信システム。

【請求項２】
請求項１において、前記第１または第２装置のうちのいずれか一方は、前記乱数値を生成し、自身のパケットカウンタの初期値として設定するとともに暗号化して他方に伝送し、他方は暗号を復号して前記乱数値を復元して自身のパケットカウンタの初期値として設定する、
通信システム。
【請求項３】
請求項２において、前記暗号化は、共通鍵暗号方式に則る暗号化である、
通信システム。
【請求項４】
請求項３において、前記第１及び第２装置は、前記乱数値をそれぞれのパケットカウンタの前記暗号化のために送受信する前に、公開鍵暗号方式に則ったチャレンジ／レスポンス認証を実行する、
通信システム。
【請求項５】
請求項１において、前記第１及び第２装置は、それぞれ、自身のパケットカウンタのカウンタ値に、同じ不可逆圧縮関数を作用させて得られる値に基づいて、前記増分値を算出する、
通信システム。
【請求項６】
請求項１において、前記パケットを受信したとき、
前記第２装置により、受信パケットに含まれるメッセージに基づいて生成したメッセージ認証符号から、前記第２パケットカウンタのカウント値に基づいて抜き出された前記一部を、中央ビット列とし、
前記第２装置は、当該受信パケットよりｉ個（ｉは任意の整数）だけ以前に受信した受信パケットからｊ個（ｊは任意の整数）だけ以降に受信する受信パケットまでに、それぞれ対応する複数のカウント値に基づいて生成される複数のＭＡＣ値における当該カウント値に基づく位置から、当該メッセージ認証符号の複数のビット列をさらに抜き出し、
前記第２装置は、前記中央ビット列及び前記複数のビット列のそれぞれを、当該受信パケットに含まれる分割メッセージ認証符号と比較し、少なくとも１個のビット列が一致したときに、当該受信パケットを正当なパケットとして認証する、
通信システム。
【請求項７】
請求項６において、前記ｉ及び前記ｊをともに１とする、
通信システム。
【請求項８】
請求項１において、前記第１及び第２装置の少なくとも一方は、ハードウェアセキュリティモジュールを備える、
通信システム。
【請求項９】
請求項１において、前記第１及び第２装置は、それぞれ電子制御ユニットであり、前記ネットワークは車載ネットワークである、
通信システム。
【請求項１０】
第１パケットカウンタを備える他の通信装置とネットワークで接続され、前記ネットワークを介してパケットを送受可能であり、前記他の通信装置から受信したパケットのメッセージ認証を行う、通信装置であって、
前記第１パケットカウンタと対応し、前記他の通信装置との間でパケットが送受信されるのに伴って更新される、第２パケットカウンタと、ハードウェアセキュリティモジュールとを備え、

前記ハードウェアセキュリティモジュールによって生成した乱数を、前記第２パケットカウンタの初期値として設定するとともに、前記乱数を前記第１パケットカウンタの初期値とさせるために前記他の通信装置に対して暗号化して伝送し、
前記他の通信装置から受信するパケットは、前記他の通信装置が、伝送するメッセージに基づいてメッセージ認証符号を生成し、その一部を前記第１パケットカウンタのカウント値に基づいて抜き出して分割メッセージ認証符号とし、前記メッセージと前記分割メッセージ認証符号とを含んで生成したものであり、
当該通信装置は、前記他の通信装置からパケットを受信したとき、受信したパケットに含まれるメッセージに基づいてメッセージ認証符号を生成し、その一部を前記第２パケットカウンタのカウント値に基づいて抜き出し、受信したパケットに含まれる前記分割メッセージ認証符号と比較することによってメッセージ認証を行い、
当該通信装置及び前記他の通信装置は、パケットの送受信ごとに、それぞれ、自身のパケットカウンタのカウンタ値から同じ計算方法で生成される値を増分値として、自身のパケットカウンタを更新する、
通信装置。
【請求項１１】
請求項１０において、前記暗号化は、共通鍵暗号方式に則る暗号化である、
通信装置。
【請求項１２】
請求項１１において、前記通信装置は、前記乱数を前記他の通信装置に送信する前に、前記他の通信装置との間で、公開鍵暗号方式に則ったチャレンジ／レスポンス認証を実行する、
通信装置。
【請求項１３】
請求項１０において、当該通信装置及び前記他の通信装置は、それぞれ、自身のパケットカウンタのカウンタ値に、同じ不可逆圧縮関数を作用させて得られる値に基づいて、前記増分値を算出する、
通信装置。
【請求項１４】
請求項１０において、前記パケットを受信したとき、
受信パケットに含まれるメッセージに基づいて生成したメッセージ認証符号から、前記第２パケットカウンタのカウント値に基づいて抜き出された前記一部を、中央ビット列とし、
当該通信装置は、当該受信パケットよりｉ個（ｉは任意の整数）だけ以前に受信した受信パケットからｊ個（ｊは任意の整数）だけ以降に受信する受信パケットまでに、それぞれ対応する複数のカウント値に基づいて生成される複数のＭＡＣ値における当該カウント値に基づく位置から、当該メッセージ認証符号の複数のビット列をさらに抜き出し、
当該通信装置は、前記中央ビット列及び前記複数のビット列のそれぞれを、当該受信パケットに含まれる分割メッセージ認証符号と比較し、少なくとも１個のビット列が一致したときに、当該受信パケットを正当なパケットとして認証する、
通信装置。
【請求項１５】
請求項１４において、前記ｉ及び前記ｊをともに１とする、
通信装置。
【請求項１６】
請求項１０において、当該通信装置と前記通信装置は、車載ネットワークに接続される電子制御ユニットを構成する通信装置であり、当該通信装置と前記通信装置とを相互に接続する前記ネットワークは、前記車載ネットワークと同一又は異なるネットワークである、
通信装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信システムおよび通信装置に関し、特にネットワーク上の通信パケットにメッセージ認証コード（ＭＡＣ：Message Authentication Code）の一部を含む通信に好適に利用できるものである。
【背景技術】
【０００２】
自動車の制御システムを始めとして、様々な分野において、セキュリティの重要性及びニーズが高まっている。これに対応するため組み込み機器の分野においては、対象製品そのものが物理的に攻撃される機会が多いため、耐タンパ性の高い、ハードウェアセキュリティモジュール（ＨＳＭ：Hardware Security Module）にセキュリティ機能を集約する傾向がある。
【０００３】
自動車の制御システムは、例えばＣＡＮ（Controller Area Network）などの車載ネットワークに接続された複数の電子制御ユニット（ＥＣＵ：Electronic Control Unit）から構成される。このような自動車の制御システムに対する攻撃には、ＣＡＮでやり取りされるメッセージの漏洩、メッセージの改竄、偽のメッセージの配信などがあり、これを防ぐために、ＥＣＵ間の通信にはＣＡＮパケットにその正当性を証明する情報を付加する手法などが提案されている。
【０００４】
特許文献１には、ＣＡＮプロトコルを変更せずにメッセージ認証コード（ＭＡＣ）によるメッセージ認証を行う技術が開示されている。ＣＡＮに接続されている各ＥＣＵにおいてＣＡＮＩＤごとにメッセージが送信された回数をカウントする。メッセージを送信したＥＣＵはメインメッセージのデータフィールド及びＣＡＮＩＤと、ＣＡＮＩＤに対応するカウンタ値とからＭＡＣを生成して、ＭＡＣメッセージとして送信する。メインメッセージを受信したＥＣＵは、メインメッセージに含まれるデータフィールド及びＣＡＮＩＤと、ＣＡＮＩＤに対応するカウンタ値とからＭＡＣを生成して、ＭＡＣメッセージに含まれるＭＡＣとの比較を行い、メインメッセージの正当性を検証することができる。
【０００５】
非特許文献１には、上記特許文献１に記載される技術を改良した、ＣＡＮパケットの認証技術が開示されている。ＣＡＮパケットの大きさには制限があるので、算出されたＭＡＣ値の一部のビットのみをＣＡＮパケットに包含させる。送信側ＥＣＵでは、送信パケットカウンタの上位Ｌ－１－ｎビットをＭＡＣの算出に使用し、下位ｎビットを算出されたＭＡＣ値から抽出される一部のビット（Ｘｓビット）のフレーム位置を示すために使用する。即ち、送信側ＥＣＵでは、メインメッセージと、送信側と受信側とで共有される秘密の情報と、送信パケットカウンタの上位Ｌ－１－ｎビットとからＭＡＣ値を算出し、そのＭＡＣ値から送信パケットカウンタの下位ｎビットで指定されるフレーム位置のＸｓビットを抽出して、メインメッセージに付加してＣＡＮパケットを構成する。受信側ＥＣＵでは、受信パケットカウンタの送信側と同じ上位Ｌ－１－ｎビットをＭＡＣの算出に使用し、下位ｎビットを算出されたＭＡＣ値から抽出される一部のビット（Ｘｒビット）のフレーム位置を示すために使用する。即ち、受信側ＥＣＵでは、受信したＣＡＮパケット中のメインメッセージと、送信側と共有する秘密の情報と、受信パケットカウンタの上位Ｌ－１－ｎビットとからＭＡＣ値を算出し、そのＭＡＣ値から受信パケットカウンタの下位ｎビットで指定されるフレーム位置のＸｒビットを抽出する。受信したＣＡＮパケット中のＭＡＣ値Ｘｓビットと、自身が算出したＭＡＣ値のうちのＸｒビットとを比較し、一致すれば受信したＣＡＮパケットを正当なものと認証する。
【先行技術文献】
【特許文献】
【０００６】

【特許文献１】特開２０１３－９８７１９号公報
【非特許文献】
【０００７】
【非特許文献１】竹森敬祐、溝口誠一郎、川端秀明、窪田歩、「セキュアブート＋認証による車載制御システムの保護」、情報処理学会研究報告　高度交通システムとスマートコミュニティ（ITS）、2014-ITS-58、情報処理学会、２０１４年９月１２日
【発明の概要】
【発明が解決しようとする課題】
【０００８】
特許文献１及び非特許文献１について本発明者が検討した結果、以下のような新たな課題があることがわかった。
【０００９】
非特許文献１には、送信側と受信側のＥＣＵがそれぞれセキュアエレメントと呼ばれるＨＳＭを備えており、ＭＡＣの生成などを行うため、この部分の耐タンパ性は担保されているが、パケットカウンタをＨＳＭの外側に備えるため、ＥＣＵ内部でＨＳＭにデータを入出力する通信経路の秘匿性・完全性の確保が十分でないことがわかった。例えばセキュリティ機能を備えないホストプロセッサとＨＳＭとを通信路で接続してＥＣＵを構成すると、仮に、ホストプロセッサ側でソフトウェアを用いて暗号化を行い、秘匿性を確保したとしても、ホストプロセッサとＨＳＭ間の通信経路にプロービング等を行い、古い情報を流す、いわゆるリプレイアタックに対しての耐性が低いことがわかった。
【００１０】
このような課題を解決するための手段を以下に説明するが、その他の課題と新規な特徴は、本明細書の記述及び添付図面から明らかになるであろう。
【課題を解決するための手段】
【００１１】
一実施の形態によれば、下記の通りである。
【００１２】
すなわち、ネットワークで相互接続されパケットを送受する複数の装置を含む通信システムであって、パケットを送受する装置はそれぞれ通信相手に対応するパケットカウンタを備える。対応するパケットカウンタには、初期値として同じ乱数値が与えられ、パケットの送受信に伴ってそれぞれ更新される。メッセージを送信する側の装置は、前記メッセージに基づいてメッセージ認証符号（ＭＡＣ値）を生成し、その一部を自身のパケットカウンタのカウント値に基づいて抜き出して分割メッセージ認証符号（分割ＭＡＣ値）とし、前記メッセージに付加してパケットを生成してネットワークに送信する。パケットを受信した装置は、受信したパケットに含まれるメッセージに基づいてメッセージ認証符号（ＭＡＣ値）を生成し、その一部を自身のパケットカウンタのカウント値に基づいて抜き出し、受信したパケットに含まれる分割メッセージ認証符号（分割ＭＡＣ値）と比較することによってメッセージ認証を行う。
【発明の効果】
【００１３】
前記一実施の形態によって得られる効果を簡単に説明すれば下記のとおりである。
【００１４】
すなわち、パケットカウンタのカウント値を外部から観測または推定することが難しくなり、複数の装置間の通信経路（ネットワーク）の秘匿性や安全性を向上することができる。
【図面の簡単な説明】
【００１５】
【図１】図１は、通信装置の構成例及びその通信装置を含んで構成される通信システムの構成例を示すブロック図である。
【図２】図２は、通信装置が電子制御ユニット（ＥＣＵ）であり、そのＥＣＵを車載ネッ

トワーク（ＣＡＮ）で相互に接続して構成される通信システムの構成例を示すブロック図である。
【図３】図３は、通信システムが通信装置としての複数のＥＣＵをＣＡＮで相互接続して構成され、その１つの通信装置（ＥＣＵ）が、ＨＯＳＴと耐タンパ性を備えるハードウェアセキュリティモジュール（ＨＳＭ）で構成される、構成例を示すブロック図である。
【図４】図４は、実施形態１における通信フローの一例を示すフロー図である。
【図５】図５は、パケットカウンタのゆらぎを吸収するためのフローの一例を示すフロー図である。
【図６】図６は、パケットカウンタのインクリメント値を乱数にするためのフローの一例を示すフロー図である。
【図７】図７は、実施形態２における通信フローの一例を示すフロー図である。
【図８】図８は、ＨＯＳＴにも暗号機能が搭載される、ＥＣＵの構成例を示すブロック図である。
【図９】図９は、実施形態３における通信フローの一例を示すフロー図である。
【発明を実施するための形態】
【００１６】
実施の形態について詳述する。
【００１７】
〔実施形態１〕＜パケットカウンタを乱数で初期化＞
図１は、通信装置の構成例及びその通信装置を含んで構成される通信システムの構成例を示すブロック図である。通信システム１０は、ネットワーク５で相互接続され、そのネットワーク５を介してパケットを送受信する第１通信装置１＿２と第２通信装置１＿１とを含んで構成される。ネットワーク５には、他の通信装置がさらに接続されていてもよい。また、ネットワーク５は階層化されたネットワークであって、第１通信装置１＿２と第２通信装置１＿１との間に中継装置を含んで構成されても良い。また、ネットワークは有線・無線を問わず、パケットを伝送可能な何らかの通信路であればよい。
【００１８】
第１通信装置１＿２と第２通信装置１＿１は、パケットカウンタ６＿２と６＿１をそれぞれ備える。パケットカウンタ６＿２と６＿１には、初期値として同じ乱数値が与えられ、第１通信装置１＿２と第２通信装置１＿１との間のパケットの送受信に伴ってそれぞれ更新される。第１通信装置１＿２から第２通信装置１＿１へのパケットの伝送と、逆方向の第２通信装置１＿１から第１通信装置１＿２へのパケットの伝送とについてそれぞれ別のパケットカウンタが設けられていても良い。送信側がパケットを送信するときに自身のパケットカウンタを更新すると、受信側もこれに合わせてそのパケットを受信したときに自身パケットカウンタを更新するように構成し、互いのパケットカウンタが同じカウント値を保持するように制御される。このとき、１パケットの送受信に対応するパケットカウンタの増分値（インクリメント値）は、必ずしも１には限られず、パケットの送受に応じて互いのパケットカウンタに同じカウント値が保持される限り、任意の値を取り得る。
【００１９】
第１通信装置１＿２は、第２通信装置１＿１宛てに送信するメッセージと、メッセージ認証符号（ＭＡＣ値）を生成するための秘密の情報が与えられており、パケット生成部２０とＭＡＣ生成部２１と分割ＭＡＣ値生成部２２とを備える。パケット生成部２０とＭＡＣ生成部２１と分割ＭＡＣ値生成部２２とは、第１通信装置１＿２が備えるプロセッサ上でソフトウェアを実行することによって実現される機能ブロックである。ソフトウェアによって実現される代わりに、全部または一部を、専用ハードウェアによって実現しても良い。
【００２０】
第１通信装置１＿２は、第２通信装置１＿１宛てにメッセージを伝送するときに、そのメッセージと秘密の情報に基づいてＭＡＣ生成部２１においてＭＡＣ値を生成する。分割ＭＡＣ値生成部２２は、生成されたＭＡＣ値から、パケットカウンタ６＿２のカウント値

に基づいて指定される、一部分のビット位置（フレーム位置）のデータを抜き出して分割ＭＡＣ値とする。パケット生成部２０は、メッセージと分割ＭＡＣ値とを含むパケットを生成して、第２通信装置１＿１宛てにネットワーク５に送信する。

【００２１】

第２通信装置１＿１は、ＭＡＣ値を認証するための秘密の情報が与えられており、パケット分割部３０とＭＡＣ生成部３１と分割ＭＡＣ値生成部３２と比較・認証部３３とを備える。パケット分割部３０とＭＡＣ生成部３１と分割ＭＡＣ値生成部３２と比較・認証部３３とは、第２通信装置１＿１が備えるプロセッサ上でソフトウェアを実行することによって実現される機能ブロックである。ソフトウェアによって実現される代わりに、全部または一部を、専用ハードウェアによって実現しても良い。

【００２２】

第２通信装置１＿１は、第１通信装置１＿２からネットワーク５を経由してパケットを受信したとき、パケット分割部３０によってそのパケットからメッセージと分割ＭＡＣ値を抽出する。ＭＡＣ生成部３１は、受信したパケットから抽出されたメッセージと、秘密の情報と、パケットカウンタ６＿１のカウント値とから、ＭＡＣ値を生成する。分割ＭＡＣ値生成部３２は、生成されたＭＡＣ値から、パケットカウンタ６＿１のカウント値に基づいて指定される、一部分のビット位置（フレーム位置）のデータを抜き出して分割ＭＡＣ値とする。比較・認証部３３は、パケット分割部３０によって受信したパケットから抽出された分割ＭＡＣ値と、ＭＡＣ生成部３１と分割ＭＡＣ値生成部３２によって生成された分割ＭＡＣ値とを比較し、比較結果に基づいて、受信したメッセージを認証する。ここで、受信したメッセージが認証されるのは、受信したパケットから抽出された分割ＭＡＣ値と内部で生成された分割ＭＡＣ値とが完全に一致する場合には限られない。「パケットカウンタのゆらぎを吸収」に後述するように、送信側と受信側でパケットカウンタのカウント値にずれが生じている場合にも、メッセージ認証を成功と判定させることもできる。

【００２３】

パケットカウンタ６＿１と６＿２の初期値として乱数値が与えられることにより、そのカウント値を外部から観測または推定することが難しくなり、第１通信装置１＿２と第２通信装置１＿１との間の通信経路（ネットワーク５）の秘匿性や安全性を向上することができる。

【００２４】

ここで、図１には、第１通信装置１＿２がメッセージの送信側であり、第２通信装置１＿１が受信側である場合に限って説明したが、メッセージの伝送方向は逆方向でも双方向でも良い。その場合には、第１通信装置１＿２が、パケット分割部、受信したパケットから抽出されるメッセージからＭＡＣ値を生成するＭＡＣ生成部、分割ＭＡＣ値生成部、及び、比較・認証部をさらに備えてもよく、また、第２通信装置１＿１が、パケット生成部、ＭＡＣ生成部、及び、分割ＭＡＣ値生成部をさらに備えてもよい。

【００２５】

〔ＣＡＮに接続されるＥＣＵ間通信への適用〕

上述の第１及び第２通信装置をそれぞれＥＣＵとし、ネットワーク５を車載ネットワーク（ＣＡＮ）とすることによって、通信システムを構成することができる。

【００２６】

図２は、通信装置が電子制御ユニット（ＥＣＵ）であり、そのＥＣＵを車載ネットワーク（ＣＡＮ）で相互に接続して構成される通信システムの構成例を示すブロック図である。複数のＥＣＵである、ＥＣＵ－Ａ（２＿Ａ）、ＥＣＵ－Ｂ（２＿Ｂ）、及び、ＥＣＵ－Ｃ（２＿Ｃ）が、ＣＡＮ５に接続されている。ＥＣＵ－Ａ（２＿Ａ）はパケットカウンタＡＢ（６＿ＡＢ）とパケットカウンタＡＣ（６＿ＡＣ）とを備え、ＥＣＵ－Ｂ（２＿Ｂ）はパケットカウンタＢＡ（６＿ＢＡ）とパケットカウンタＢＣ（６＿ＢＣ）とを備え、ＥＣＵ－Ｃ（２＿Ｃ）はパケットカウンタＣＡ（６＿ＣＡ）とパケットカウンタＣＢ（６＿ＣＢ）とを備える。パケットカウンタＡＢ（６＿ＡＢ）とパケットカウンタＢＡ（６＿ＢＡ）とは、ＥＣＵ－Ａ（２＿Ａ）とＥＣＵ－Ｂ（２＿Ｂ）との間のパケット通信に対応し

て設けられている。同様に、パケットカウンタＡＣ（６＿ＡＣ）とパケットカウンタＣＡ（６＿ＣＡ）とは、ＥＣＵ－Ａ（２＿Ａ）とＥＣＵ－Ｃ（２＿Ｃ）との間のパケット通信、パケットカウンタＢＣ（６＿ＢＣ）とパケットカウンタＣＢ（６＿ＣＢ）とは、ＥＣＵ－Ｂ（２＿Ｂ）とＥＣＵ－Ｃ（２＿Ｃ）との間のパケット通信に、それぞれ対応して設けられている。それぞれＥＣＵが１：１のパケット通信を行う場合には、そのパケット通信を行うＥＣＵどうしのパケットカウンタが、同じ乱数値によって初期化される。ブロードキャストなど１：多のパケット通信を行う場合には、その１：多のパケット通信に参加するすべてのＥＣＵどうしのパケットカウンタが、同じ乱数値によって初期化される。

【００２７】

これにより、ＣＡＮによって相互接続される電子制御ユニット（ＥＣＵ）間の通信の秘匿性や安全性を向上することができる。

【００２８】

〔ＨＯＳＴ－ＨＳＭ間通信への適用〕

上述の第１及び第２通信装置の間の通信を、ＥＣＵを構成するホストプロセッサ（ＨＯＳＴ）とハードウェアセキュリティモジュール（ＨＳＭ）との間の通信に適用することができる。「背景技術」において述べたように、自動車の制御システムを始めとする、セキュリティの重要性及びニーズが高い組み込み機器においては、対象の機器そのものが物理的に攻撃される機会が多いため、耐タンパ性の高いＨＳＭを設けて、これにセキュリティ機能を集約する傾向がある。

【００２９】

図３は、通信システムが通信装置としての複数のＥＣＵをＣＡＮで相互接続して構成され、その１つのＥＣＵが、ＨＯＳＴと耐タンパ性を備えるＨＳＭとを含んで構成される、構成例を示すブロック図である。図２と同様に、複数のＥＣＵがＣＡＮ５＿２に接続され得るが、ＥＣＵ－Ａ（２＿Ａ）とＥＣＵ－Ｂ（２＿Ｂ）のみがＣＡＮ５＿２に接続されている例が示され、ＥＣＵ－Ａ（２＿Ａ）が、ネットワーク５＿１によって相互接続される、ＨＯＳＴ４と耐タンパ性を備えるＨＳＭ３とを備えて構成される例である。

【００３０】

ＨＯＳＴ４は、ＣＰＵ１１＿２と、ＣＡＮ５＿２とのインターフェース（Ｉ／Ｆ）１２＿３と、ネットワーク５＿１とのインターフェース（Ｉ／Ｆ）１２＿２と、ＲＯＭ１５＿２と、ＲＡＭ１６＿２とが、互いにバス１７＿２に接続されて構成されている。ＨＳＭ３は、ＣＰＵ１１＿１と、ネットワーク５＿１とのインターフェース（Ｉ／Ｆ）１２＿１と、ＲＯＭ１５＿１と、ＲＡＭ１６＿１と、暗号ＩＰ（Crypt IP）１３＿１と、乱数発生回路（ＲＮＧ）１４＿１とが、互いにバス１７＿１に接続されて構成されている。暗号ＩＰ１３は、耐タンパ性を備える暗号通信に関わるデータ処理を実行する回路モジュールであり、公知の耐タンパ機能を実装することによって構成することができる。例えば、秘匿すべきパラメータを外部から観測することができないように記憶し、所定の暗号演算を実行する際に、演算時間や消費電力の変動波形にデータ依存性が現れないようにするなど、暗号通信に対する攻撃からの防御措置が講じられている。

【００３１】

ＨＯＳＴ４におけるＲＯＭ１５＿２には、ＣＰＵ１１＿２で実行されることにより、上述のパケット生成部２０、ＭＡＣ生成部２１及び分割ＭＡＣ値生成部２２として機能する、プログラムが格納されている。ＨＳＭ３におけるＲＯＭ１５＿１には、１１＿１で実行されることにより、上述のパケット分割部３０、ＭＡＣ生成部３１、分割ＭＡＣ値生成部３２及び比較・認証部３３として機能する、プログラムが格納されている。ＨＯＳＴ４とＨＳＭ３との間のネットワーク５＿１を介するパケット通信は、ＨＯＳＴ４内のＲＡＭ１６＿２に保持されるパケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）とＨＳＭ３内のＲＡＭ１６＿１に保持されるパケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）とを使って実行される。一方、ＥＣＵ－Ａ（２＿Ａ）とＥＣＵ－Ｂ（２＿Ｂ）との間のＣＡＮ５＿２を介するパケット通信は、ＥＣＵ－Ａ（２＿Ａ）のＨＳＭ３内のＲＡＭ１６＿１に保持されるパケットカウンタＡＢ（６＿３）と、ＥＣＵ－Ｂ（２＿Ｂ）が備えるパケットカウンタＢＡ（

６＿４）とを使って実行される。パケットカウンタＡＢ（６＿３）は、ＨＯＳＴ４内のＲＡＭ１６＿２に保持されてもよいが、ＨＳＭ３内のＲＡＭ１６＿１に保持される方が、耐タンパ性が高い。パケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）、パケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）及びパケットカウンタＡＢ（６＿３）は、ＨＯＳＴ４内のＲＡＭ１６＿２またはＨＳＭ３内のＲＡＭ１６＿１に保持される代わりに、専用のカウンタによって実現されてもよい。

【００３２】

ＨＯＳＴ４とＨＳＭ３との間のネットワーク５＿１を介するパケット通信に、上述の図１を引用して説明した通信を適用することにより、ＨＳＭでない一般のＨＯＳＴとＨＳＭの間の通信経路（ネットワーク）の秘匿性や安全性を向上することができる。

【００３３】

ここで、ＨＯＳＴ４とＨＳＭ３の構成として図３に示されるのは、一例に過ぎない。ネットワーク５＿１は、ＣＡＮ、ＳＰＩ（Serial Peripheral Interface）など任意の通信路で形成され得る。ＨＯＳＴ４とＨＳＭ３において、バス１７＿１、１７＿２はそれぞれ階層化されてもよい。また、ＨＯＳＴ４は、実際に用いられるアプリケーションに応じて、図示されている機能ブロック以外の機能ブロック、例えば、割り込み制御回路、ダイレクトメモリコントローラ、タイマ、その他のペリフェラルなどを適宜含んで構成されても良い。ＨＳＭ３も同様である。ＨＳＭ３としては、ＣＰＵ１１＿１が搭載される構成例を示したが、シーケンサで代用してもよい。ＨＳＭ３は耐タンパ性を備えていることが望ましいが、単に、図３に示される構成要素を備えていている半導体デバイスであれば良い。特に制限されないが、ＨＯＳＴ４とＨＳＭ３とは、それぞれ例えば、公知のＣＭＯＳ（Complementary Metal-Oxide-Semiconductor field effect transistor）ＬＳＩ（Large Scale Integrated circuit）の製造技術を用いて、シリコンなどの単一半導体基板上に形成される。このように、ＨＯＳＴ４とＨＳＭ３とがそれぞれ別の半導体チップに形成され、互いがネットワーク５＿１によって通信される場合に、ネットワーク５＿１を観測することによる攻撃に対して、パケットカウンタを乱数値によって初期化することにより、通信の秘匿性や安全性を向上することができる。一方、ＨＯＳＴ４とＨＳＭ３とが同一の半導体チップ上に混載されても良い。このとき、ネットワーク５＿１が半導体チップの外に引き出されないように構成すれば、通信の秘匿性と安全性をさらに向上することができる。

【００３４】

〔乱数値はＨＳＭで生成し、暗号化してＨＯＳＴに伝送〕

図３に例示されるＥＣＵ－Ａ（２＿Ａ）の動作について説明する。

【００３５】

図４は、本実施形態１における通信フローの一例を示すフロー図である。ＨＯＳＴ４とＨＳＭ３によってそれぞれ実行される処理ステップと、送受信されるデータの内容が、上から下に向かう時系列に沿って示される。

【００３６】

まず、ＨＯＳＴ４とＨＳＭ３がそれぞれ起動される（システムＯＮ）。ＨＳＭ３は、乱数Ｒ１を乱数発生回路（ＲＮＧ）１４＿１で生成し、暗号ＩＰ（Crypt IP）１３＿１によって共通鍵ＣＫを使って暗号化する。共通鍵ＣＫを使って暗号化された乱数Ｒ１を「ＣＫ（Ｒ１）」と表記する。ＨＳＭ３は、生成した乱数Ｒ１をパケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）に初期値としてセットする。ＨＳＭ３は、暗号化された乱数ＣＫ（Ｒ１）を、ネットワーク５＿１を介してＨＯＳＴ４へ送付する。ＨＯＳＴ４では、事前にＨＳＭ３と共有してある共通鍵ＣＫを用いて、暗号化された乱数ＣＫ（Ｒ１）を復号する。その段階で、ＨＯＳＴ４は、復号された乱数Ｒ１をパケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）の初期値とし、１パケット分のインクリメントを行う。即ちＨＯＳＴ４は、パケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）の値をＲ２＝Ｒ１＋１に更新する。ＨＯＳＴ４は、ＨＳＭ３に対して、署名生成、署名検証、その他暗号に関わる処理を要求する際に、リクエストメッセージ（Request msg）を生成するとともに、そのメッセージとパケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）のカウンタ値であるＲ２からＭＡＣ値を生成して、メッ

セージに付加する。ＭＡＣ値は、一般的なＣＭＡＣ（Cipher based Message Authentication Code）等の技術を用いて生成することができる。ＨＯＳＴ４は、リクエストメッセージ（Request）とＭＡＣ値を含むパケットを生成して、ＨＳＭ３に送付する。パケットを受信したＨＳＭ３では、それに含まれるＭＡＣ値からメッセージの正当性を検証（ＭＡＣ値検証）した後、メッセージの処理を実行し、その結果（Result）をＨＯＳＴ４に送付する。このとき、パケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）の値をＲ３＝Ｒ２＋１に更新する。この処理間の通信メッセージは、共通鍵ＣＫで暗号化される。ＭＡＣ値検証の際に、受信したメッセージと自身のパケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）のカウンタ値から生成されるＭＡＣ値と受信したＭＡＣ値とが相違する場合には、不正処理に移行する。不正処理には、後述の「パケットカウンタのゆらぎを吸収」する処理が含まれてもよい。これにより、メッセージのなりすましを防ぐ事が可能となり、通信の秘匿性や安全性を向上させることができる。

【００３７】

ここで、ＨＯＳＴ４とＨＳＭ３においてそれぞれ実行されるＭＡＣ値の生成は、送受信される対象のメッセージと、それぞれのパケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）とＨＳＭ－ＨＯＳＴ（６＿１）のカウント値に基づく演算処理である。ここで、ＨＯＳＴ４とＨＳＭ３がさらに秘密の情報を共有し、これをそれぞれのＭＡＣ値生成の演算に寄与させるように構成してもよい。これにより、通信の秘匿性や安全性をより向上させることができる。

【００３８】

〔パケットカウンタのゆらぎを吸収〕

上述のＭＡＣ値検証においては、パケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）とＨＳＭ－ＨＯＳＴ（６＿１）のカウント値が同期していることが前提となる。ここで、「同期」とは、必ずしも同時に同じ値を取ることを指すのではなく、ある程度の時間差を持って同じ値に更新されても良いし、さらには、互いに異なる値であっても、一定の規則に従うことによって相互に対応する値を取ってもよい。即ち、送信側でのＭＡＣ値生成に使用されたカウント値が、受信側で再現することができ、同じＭＡＣ値を生成することができればよい。

【００３９】

しかしながら、通信エラーなどに起因して、パケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）とＨＳＭ－ＨＯＳＴ（６＿１）との間で、同期が外れる場合がある。このパケットカウンタの同期はずれを、「パケットカウンタのゆらぎ」と呼ぶことにする。このようなパケットカウンタのゆらぎは、システムが正常に動作している場合にも発生し得るので、ある程度の幅までは吸収することが望ましい。一方、通信の秘匿性・安全性が優先されるシステムにおいては、ゆらぎを外部からの攻撃と判断して、即座に防御措置を講ずることが望ましい場合もある。どちらを採用するかは、システム設計におけるＨＳＭ３及びＨＯＳＴ４のセキュリティポリシーに依存する。

【００４０】

図５は、パケットカウンタのゆらぎを吸収するためのフローの一例を示すフロー図である。

【００４１】

上述のＨＳＭ３におけるＭＡＣ値検証の際に、受信したＭＡＣ値が、受信したメッセージと自身のパケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）のカウンタ値から生成されるＭＡＣ値と相違する場合（ＭＡＣの不一致検出）に、不正処理として即時に動作を停止させる場合（即時Ｓｔｏｐの場合）と、ゆらぎを吸収する処理に移行する場合（検証する場合）とのいずれかを採り得る。前者は、通信の秘匿性・安全性が優先されるシステムにおいて、ゆらぎを外部からの攻撃と判断して、即座に防御措置を講ずる場合に採用され、後者は、パケットカウンタのゆらぎを吸収する場合に採用される。

【００４２】

即時Ｓｔｏｐの場合、ＨＳＭ３からＨＯＳＴ４に対して異常を通知し、ＨＳＭ３は実行

中の処理を中断または終了する。

【００４３】

検証する場合、図５にはパケットカウンタのゆらぎを±１パケットまで許容する例が示されている。ＭＡＣの不一致検出の後、パケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）のカウンタ値のデクリメントを実施し、再びＭＡＣ検証を行う。このステップで生成されたＭＡＣ値が受信したＭＡＣ値と一致したときには、正常なメッセージであると判断して、メッセージの処理に移行する。不一致の場合には、カウンタ値のインクリメントを２回実施し、もう１度ＭＡＣ検証を行う。このステップで生成されたＭＡＣ値が受信したＭＡＣ値と一致したときには、正常なメッセージであると判断して、メッセージの処理に移行する。不一致の場合には、ＨＳＭ３からＨＯＳＴ４に対して異常を通知し、ＨＳＭ３は実行中の処理を中断または終了する。

【００４４】

ここで、デクリメント値とインクリメント値は、必ずしも１である必要はなく、後述の実施形態２に記載されるように、別の乱数値などであってもよい。また、パケットカウンタのゆらぎを±１パケットよりも広い範囲まで許容するように変更することもできる。即ち、当該受信パケットよりｉ個（ｉは任意の整数）だけ以前に受信した受信パケットからｊ個（ｊは任意の整数）だけ以降に受信する受信パケットまでに、それぞれ対応する複数のカウント値に基づいて生成される複数のＭＡＣ値と、受信したＭＡＣ値とを比較して、繰り返しＭＡＣ検証を行う。少なくとも１個のＭＡＣ値が一致したときは、正常なメッセージであると判断して、メッセージの処理に移行し、すべて不一致の場合には、ＨＳＭ３からＨＯＳＴ４に対して異常を通知し、ＨＳＭ３は実行中の処理を中断または終了する。ｉとｊの値は、システムのセキュリティポリシーに依存して任意に設定することができる。ｉとｊの値が大きければ大きいほど、リプレイアタックが容易となるため、ｉとｊの値はともに３以下であることが望ましい。また、ゆらぎの幅が小さい時には、正常なメッセージであると判断して、メッセージの処理に移行するとしても、ゆらぎの幅がある程度大きい時には、即時に停止する処理に移行する代わりに、何らかの警告を発し、別の方法でセキュリティ強化を図るなどの防御手段を採りながら、メッセージの処理に移行するなどの中庸の処理に移行することもできる。

【００４５】

ここでは、パケットカウンタのゆらぎを吸収する構成及び方法について、パケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）とＨＯＳＴ－ＨＳＭ（６＿２）の初期値を乱数に設定する、本実施形態１の一変形例として説明したが、パケットカウンタの初期値は、必ずしも乱数である必要はない。パケットカウンタが従来技術と同様に、１または０に初期化される場合にも、同じ構成及び方法を適用することができ、同様の効果を得ることができる。またここでは、ＥＣＵ２を構成するＨＯＳＴ４とＨＳＭ３との間の通信を例にとって説明したが、任意の通信装置間の通信にも同様に適用することができる。例えば、ＣＡＮで接続されるＥＣＵ間の通信に適用することもできる。

【００４６】

〔実施形態２〕＜パケットカウンタのインクリメント値も乱数＞

実施形態１について図４を引用して説明した例では、パケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）とＨＯＳＴ－ＨＳＭ（６＿２）のインクリメント値を１とする単純な増加であるため、攻撃者が次のカウンタ値を類推しやすくなる可能性がある。そのため、インクリメントする値をランダム（乱数）にする事で、攻撃者が次のカウンタ値を類推する事を困難にする事が有効である。

【００４７】

図６は、パケットカウンタのインクリメント値を乱数にするためのフローの一例を示すフロー図である。

パケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）とＨＯＳＴ－ＨＳＭ（６＿２）の初期値となる乱数Ｒ１（初期カウンター）を、例えばＳＨＡ２５６などの不可逆圧縮関数を用いて圧縮する。その際に得られた固定値の最後の１桁を抽出し、インクリメントする数値Ｓ１

とする。このＳ１を乱数Ｒ１に加算して得られるＲ２（＝Ｒ１＋Ｓ１）を次のカウンタ値とする。さらに次のカウンタ値の生成は、このＲ２から例えばＳＨＡ２５６などの不可逆圧縮関数を用いて生成したＳ２を用いてインクリメントする。このような方式を用いる事により、カウンタの増加数の類推が困難となる。

【００４８】

図７は、実施形態２における通信フローの一例を示すフロー図である。図４と同様に、ＨＯＳＴ４とＨＳＭ３によってそれぞれ実行される処理ステップと、送受信されるデータの内容が、上から下に向かう時系列に沿って示される。

【００４９】

まず、ＨＯＳＴ４とＨＳＭ３がそれぞれ起動される（システムＯＮ）。ＨＳＭ３は、乱数Ｒ１を乱数発生回路（ＲＮＧ）１４＿１で生成し、暗号ＩＰ（Crypt IP）１３＿１によって共通鍵ＣＫを使って暗号化する。ＨＳＭ３は、生成した乱数Ｒ１をパケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）に初期値としてセットする。ＨＳＭ３は、暗号化された乱数ＣＫ（Ｒ１）を、ネットワーク５＿１を介してＨＯＳＴ４へ送付する。ＨＯＳＴ４では、受信した、暗号化された乱数ＣＫ（Ｒ１）を、共通鍵ＣＫを用いて復号する。その段階で、ＨＯＳＴ４はパケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）の初期値とし、１パケット分のインクリメントを行う。即ちＨＯＳＴ４は、パケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）の値をＲ２＝Ｒ１＋Ｓ１に更新する。ＨＯＳＴ４は、ＨＳＭ３に対してリクエストメッセージ（Request msg）を生成するとともに、そのメッセージとパケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）のカウンタ値であるＲ２からＭＡＣ値を生成して、メッセージに付加する。ＨＯＳＴ４は、リクエストメッセージ（Request）とＭＡＣ値を含むパケットを生成して、ＨＳＭ３に送付する。パケットを受信したＨＳＭ３では、それに含まれるＭＡＣ値からメッセージの正当性を検証（ＭＡＣ値検証）した後、メッセージの処理を実行し、その結果（Result）をＨＯＳＴ４に送付する。このとき、パケットカウンタＨＳＭ－ＨＯＳＴ（６＿１）の値をＲ３＝Ｒ２＋Ｓ２に更新する。この処理間の通信メッセージは、共通鍵ＣＫで暗号化される。

【００５０】

図４に示されるフローとの違いは、インクリメント値が図５を引用して上述したように、乱数とされている点である。これより、次のパケットに対応する、パケットカウンタＨＯＳＴ－ＨＳＭ（６＿２）とＨＳＭ－ＨＯＳＴ（６＿１）をカウント値の類推が困難となり、通信の秘匿性や安全性をさらに向上させることができる。

【００５１】

本実施形態２では、ＥＣＵ２を構成するＨＯＳＴ４とＨＳＭ３との間の通信を例にとって説明したが、任意の通信装置間の通信にも同様に適用することができる。例えば、ＣＡＮで接続されるＥＣＵ間の通信に適用することもできる。

【００５２】

〔実施形態３〕＜ＨＯＳＴにも暗号機能を搭載＞

以上の実施形態１及び２における、図３に例示される構成例に基づいた説明では、ＨＯＳＴ４とＨＳＭ３との間の通信は、あらかじめ共有していた共通鍵ＣＫを用いて暗号化する方式を示した。これに対して、ＨＯＳＴ４に暗号機能が搭載されている場合、或いは、ＨＯＳＴ４のＣＰＵ１１＿２にて暗号の計算処理が可能な場合には、公開鍵暗号方式を用いて双方を認証した後に、共通鍵ＣＫの交換を行う事が可能である。

【００５３】

図８は、ＨＯＳＴ４にも暗号機能が搭載される、ＥＣＵ２の構成例を示すブロック図である。ＥＣＵ２は、図３に示されるＥＣＵ－Ａ（２＿Ａ）に対応する。ＨＯＳＴ４は、図３に示されるＥＣＵ－Ａ（２＿Ａ）に搭載されるＨＯＳＴ４と同様に、互いにバス１７＿２に接続される、ＣＰＵ１１＿２と、ＣＡＮ５＿２とのインターフェース（Ｉ／Ｆ）１２＿３と、ネットワーク５＿１とのインターフェース（Ｉ／Ｆ）１２＿２と、ＲＯＭ１５＿２と、ＲＡＭ１６＿２とを備え、さらに暗号ＩＰ（Crypt IP）１３＿２を備える点で異なる。暗号ＩＰ１３＿２は、図３に示される暗号ＩＰ１３＿１と同様に、耐タンパ性を備え

る暗号通信に関わるデータ処理を実行する回路モジュールである。ネットワーク５＿１及びＨＳＭ３は、図３に示されるＥＣＵ－Ａ（２＿Ａ）に搭載される、ネットワーク５＿１及びＨＳＭ３と同様である。ＨＯＳＴ４に暗号ＩＰ１３＿２が追加されている点以外は、実施形態１での説明がそのまま適用できるので、重複した説明は控える。

【００５４】

ＥＣＵ２の動作について説明する。

【００５５】

図９は、本実施形態３における通信フローの一例を示すフロー図である。ＨＯＳＴ４とＨＳＭ３によってそれぞれ実行される処理ステップと、送受信されるデータの内容が、図４、７と同様に、上から下に向かう時系列に沿って示される。

【００５６】

まず、ＨＯＳＴ４とＨＳＭ３がそれぞれ起動される（システムＯＮ）。ＨＯＳＴ４は、暗号ＩＰ１３＿２によって公開鍵Ｐｐと秘密鍵Ｐｓを生成し、生成した公開鍵ＰｐをＨＳＭ３に送付する。ＨＳＭ３は、乱数発生回路（ＲＮＧ）１４＿１によって乱数ＲＣを生成し、暗号ＩＰ１３＿１によって受信した公開鍵Ｐｐを使って暗号化する。公開鍵Ｐｐを使って暗号化された乱数ＲＣを、「Ｐｐ（ＲＣ）」と表記する。ＨＳＭ３は、暗号化された乱数Ｐｐ（ＲＣ）を、チャレンジデータとしてＨＯＳＴ４に送付する。ＨＯＳＴ４は、受信したチャレンジデータを、暗号ＩＰ１３＿２によって秘密鍵Ｐｓを用いて復号し、レスポンスデータを生成し、ＨＳＭ３に送付する。ＨＳＭ３では期待値比較を行って受信したレスポンスデータを検証し、ＨＯＳＴ４が真正な通信装置であることを確認する。

【００５７】

その後、ＨＳＭ３は、乱数Ｒ１を乱数発生回路（ＲＮＧ）１４＿１で生成し、暗号ＩＰ１３＿１によって共通鍵ＣＫを使って暗号化する。以降のフローは、図７を引用して説明した実施形態２のフローと同様であるので、説明を省略する。以降のフローを、図４を引用して説明した実施形態１のフローと同様とすることもできる。

【００５８】

これにより、パケットカウンタの初期値とされる乱数値を不正に取得しようとする攻撃に対する耐性が向上し、ＨＳＭ３とＨＯＳＴ４との間の通信経路（ネットワーク）の秘匿性や安全性を向上することができる。

【００５９】

本実施形態３では、ＥＣＵ２を構成するＨＯＳＴ４とＨＳＭ３との間の通信を例にとって説明したが、任意の通信装置間の通信にも同様に適用することができる。例えば、ＣＡＮで接続されるＥＣＵ間の通信に適用することもできる。

【００６０】

上述のチャレンジで利用された乱数ＲＣをＨＯＳＴ４とＨＳＭ３間の共通鍵ＣＫとして用いる事により、鍵交換シーケンスを省略する事ができるが、別途、共通鍵ＣＫを交換するシーケンスを追加しても良い。

【００６１】

以上本発明者によってなされた発明を実施形態に基づいて具体的に説明したが、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

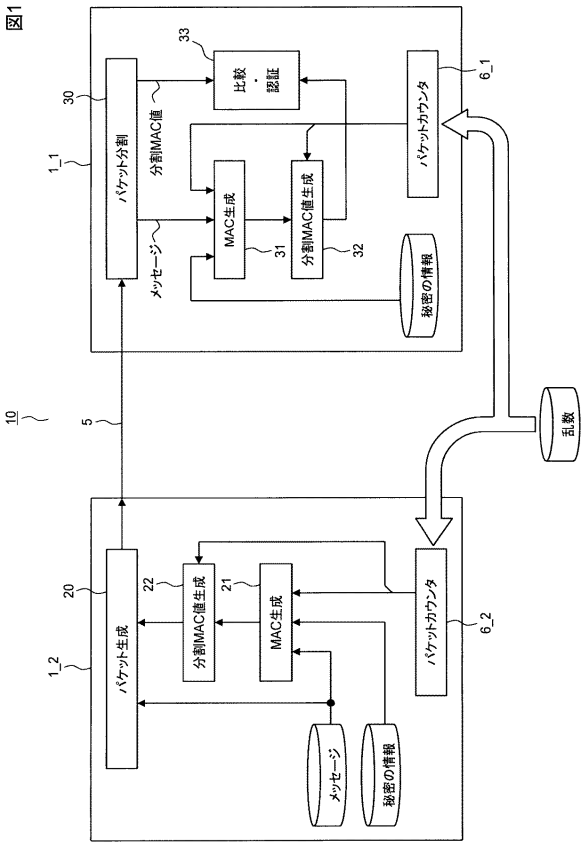
【符号の説明】

【００６２】

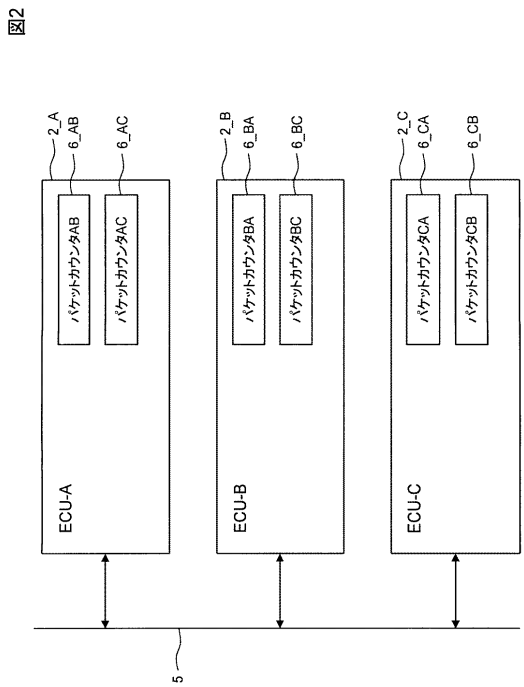
１　通信装置
２　電子制御ユニット（ＥＣＵ：Electronic Control Unit）
３　ハードウェアセキュリティモジュール（ＨＳＭ：Hardware Security Module）
４　ホスト（ＨＯＳＴ）
５　ネットワーク
６　パケットカウンタ
１０　通信システム

１１　ＣＰＵ（Central Processing Unit）
１２　インターフェース（Ｉ／Ｆ）
１３　暗号ＩＰ（Crypt IP）
１４　乱数発生回路（ＲＮＧ：Random Number Generator）
１５　ＲＯＭ（Read Only Memory）
１６　ＲＡＭ（Random Access Memory）
１７　バス
２０　パケット生成部
２１　ＭＡＣ生成部
２２　分割ＭＡＣ生成部
３０　パケット分割部
３１　ＭＡＣ生成部
３２　分割ＭＡＣ生成部
３３　比較・認証部

【図１】

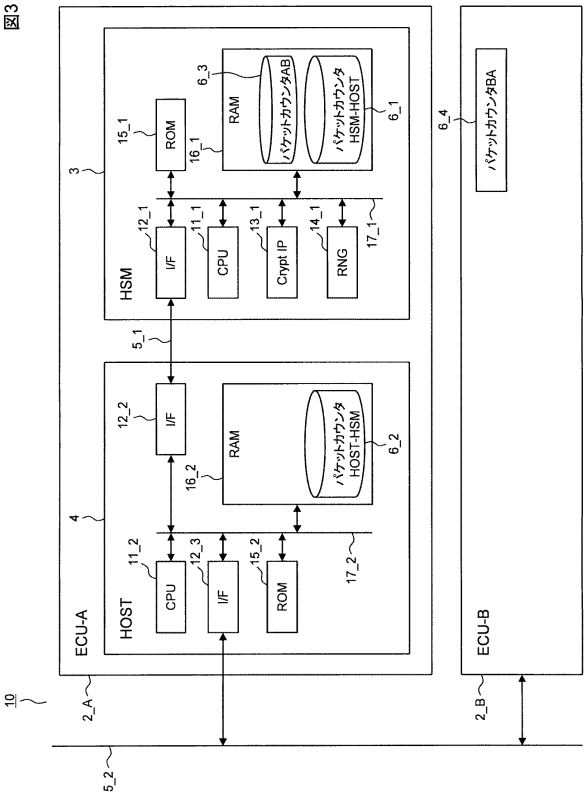


【図２】



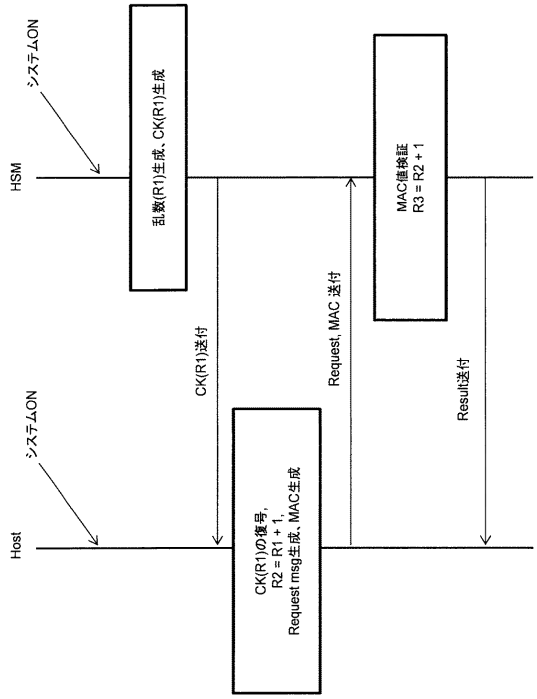
【図３】

図3



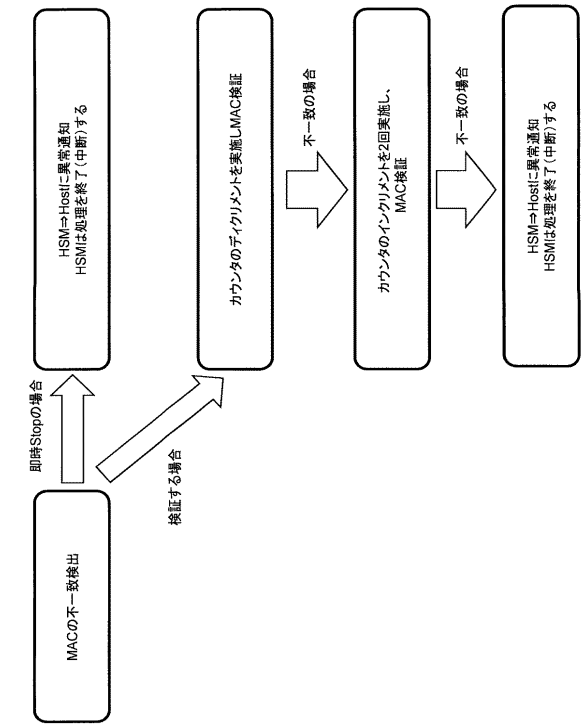
【図４】

図4



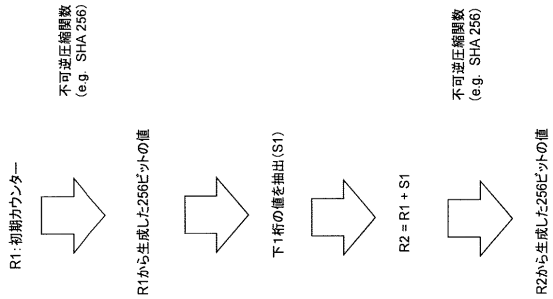
【図５】

図5



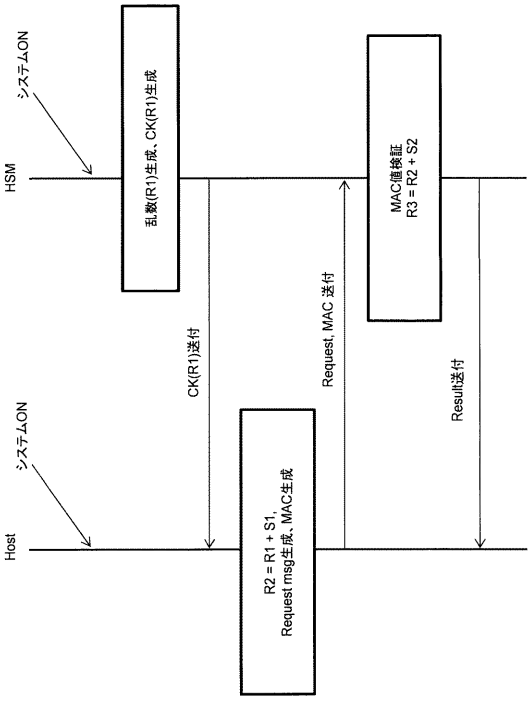
【図６】

図6



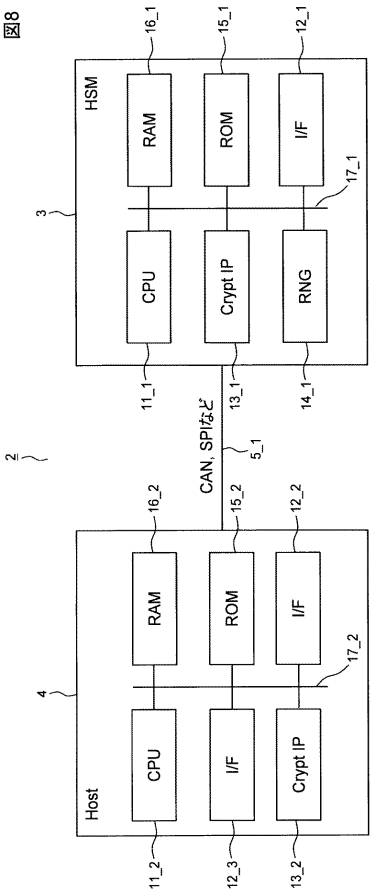
【図７】

図7



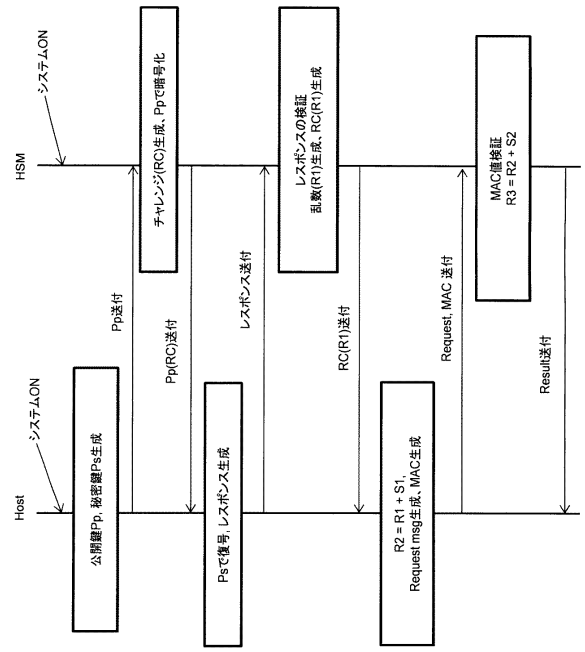
【図８】

図8



【図９】

図9



フロントページの続き

(56)参考文献 米国特許出願公開第２０１１／０２３８９８９（ＵＳ，Ａ１）
特開２０００－１０６５５３（ＪＰ，Ａ）
特表２００９－５１７９３９（ＪＰ，Ａ）
米国特許出願公開第２００９／０２２２６６６（ＵＳ，Ａ１）
竹森　敬祐　ほか，セキュアブート＋認証による車載制御システムの保護，電子情報通信学会技術研究報告，日本，電子情報通信学会，２０１４年　9月１２日，Ｖｏｌ．１１４，Ｎｏ．２２５，ｐｐ．４７－５４
D. W. Davides, W. L. Price　著／上園　忠弘　監訳，ネットワーク・セキュリティ，日本，日経マグロウヒル社，１９８５年１２月　5日，1版1刷，ｐｐ．１２６－１２９

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２