(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-50004
(P2009-50004A)
(43)公開日　平成21年3月5日(2009.3.5)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104
H04L 12/28	(2006.01)	H04L	12/28	200M	5K033
G09C 1/00	(2006.01)	G09C	1/00	640E	

審査請求 未請求　請求項の数 18　ＯＬ　（全 17 頁）

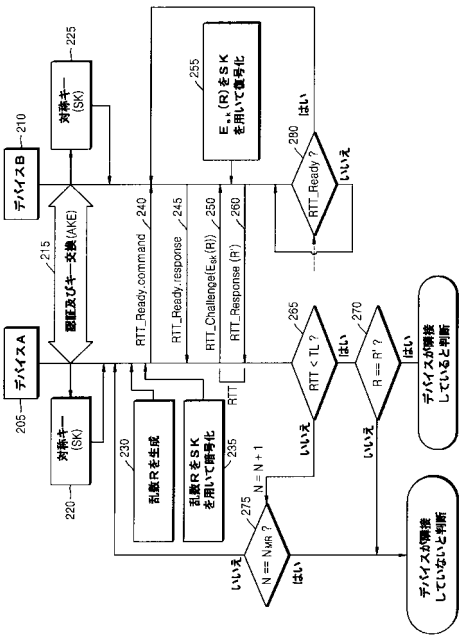
(21)出願番号　特願2008-211151 (P2008-211151)
(22)出願日　平成20年8月19日 (2008.8.19)
(31)優先権主張番号　60/956,986
(32)優先日　平成19年8月21日 (2007.8.21)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10-2007-0115504
(32)優先日　平成19年11月13日 (2007.11.13)
(33)優先権主張国　韓国 (KR)

(71)出願人　390019839
三星電子株式会社
ＳＡＭＳＵＮＧ ＥＬＥＣＴＲＯＮＩＣＳ ＣＯ．，ＬＴＤ．
大韓民国京畿道水原市靈通区梅灘洞４１６
４１６，Ｍａｅｔａｎ－ｄｏｎｇ，Ｙｅｏｎｇｔｏｎｇ－ｇｕ，Ｓｕｗｏｎ－ｓｉ，Ｇｙｅｏｎｇｇｉ－ｄｏ　４４２－７４２（ＫＲ）
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】挑戦応答基盤のＲＴＴ検査方法、装置及びその方法を記録したコンピュータで読み取り可能な記録媒体

(57)【要約】
【課題】　挑戦応答基盤のＲＴＴ検査方法、装置及びその方法を記録したコンピュータで読み取り可能な記録媒体を提供する。
【解決手段】　乱数を生成するステップと、対称キーを利用して乱数を暗号化するステップと、暗号化された乱数を含む挑戦要請メッセージをデバイスに送信するステップと、挑戦要請メッセージを受信し、かつ対称キーを利用して暗号化された乱数を復号化したデバイスから、乱数を含む挑戦応答メッセージを受信するステップと、挑戦応答メッセージが受信された時刻及び挑戦要請メッセージが送信された時刻に基づいてＲＴＴを決定するステップと、を含む挑戦応答基盤のＲＴＴ検査方法。これにより、デバイス間の効率的な隣接性検査ができる。
【選択図】　図２



【特許請求の範囲】
【請求項１】
乱数を生成するステップと、
対称キーを利用して前記乱数を暗号化するステップと、
前記暗号化された乱数を含む挑戦要請メッセージをデバイスに送信するステップと、
前記挑戦要請メッセージを受信し、かつ前記対称キーを利用して暗号化された乱数を復号化した前記デバイスから、前記乱数を含む挑戦応答メッセージを受信するステップと、
前記挑戦応答メッセージが受信された時刻及び前記挑戦要請メッセージが送信された時刻に基づいてＲＴＴ（Ｒｏｕｎｄ　Ｔｒｉｐ　Ｔｉｍｅ）を決定するステップと、を含むことを特徴とする挑戦応答基盤のＲＴＴ検査方法。
【請求項２】
前記対称キーを利用して前記乱数を暗号化するステップは、
前記対称キーを利用して乱数マスクを生成するステップと、
前記乱数及び前記乱数マスクを排他的論理和演算（ＸＯＲ）により結合するステップと、を含むことを特徴とする請求項１に記載の挑戦応答基盤のＲＴＴ検査方法。
【請求項３】
前記ＲＴＴが所定の臨界時間より短ければ、前記生成された乱数及び前記挑戦応答メッセージに含まれた乱数を比較することによって、前記デバイスを認証するステップをさらに含むことを特徴とする請求項１に記載の挑戦応答基盤のＲＴＴ検査方法。
【請求項４】
前記ＲＴＴが所定の臨界時間より長いか、または同じならば、所定の最大反復回数内で前記乱数を生成するステップないし前記ＲＴＴを決定するステップを反復的に行うことを特徴とする請求項３に記載の挑戦応答基盤のＲＴＴ検査方法。
【請求項５】
準備要請メッセージを前記デバイスに送信するステップと、
前記デバイスから準備応答メッセージを受信するステップと、をさらに含むことを特徴とする請求項１に記載の挑戦応答基盤のＲＴＴ検査方法。
【請求項６】
デバイスから、対称キーを利用して暗号化された乱数を含む挑戦要請メッセージを受信するステップと、
前記対称キーを利用して暗号化された乱数を復号化するステップと、
前記復号化された乱数を含む挑戦応答メッセージを前記デバイスに送信するステップと、を含むことを特徴とする挑戦応答基盤のＲＴＴ検査方法。
【請求項７】
前記挑戦要請メッセージを受信するステップ以前に、前記対称キーを利用して乱数マスクを生成するステップをさらに含み、
前記暗号化された乱数を復号化するステップは、前記挑戦要請メッセージに含まれた暗号化された乱数及び前記乱数マスクを、排他的論理和演算（ＸＯＲ）により結合するステップを含むことを特徴とする請求項６に記載の挑戦応答基盤のＲＴＴ検査方法。
【請求項８】
前記デバイスから準備要請メッセージを受信するステップと、
前記デバイスに準備応答メッセージを送信するステップと、をさらに含むことを特徴とする請求項６に記載の挑戦応答基盤のＲＴＴ検査方法。
【請求項９】
乱数を生成する乱数生成部と、
対称キーを利用して前記乱数を暗号化する暗号化部と、
前記暗号化された乱数を含む挑戦要請メッセージをデバイスに送信し、前記挑戦要請メッセージを受信し、かつ前記対称キーを利用して前記暗号化された乱数を復号化した前記デバイスから、前記乱数を含む挑戦応答メッセージを受信する通信部と、
前記挑戦応答メッセージが受信された時刻及び前記挑戦要請メッセージが送信した時刻

に基づいてＲＴＴを決定するＲＴＴ決定部と、を備えることを特徴とする挑戦応答基盤のＲＴＴ検査装置。
【請求項１０】
前記暗号化部は、
前記対称キーを利用して乱数マスクを生成する乱数マスク生成部と、
前記乱数及び前記乱数マスクを排他的論理和演算（ＸＯＲ）により結合する結合部と、を備えることを特徴とする請求項９に記載の挑戦応答基盤のＲＴＴ検査装置。
【請求項１１】
前記ＲＴＴ及び所定の臨界時間を比較する比較部と、
前記ＲＴＴが前記臨界時間より短ければ、前記生成された乱数及び前記挑戦応答メッセージに含まれた乱数を比較することによって前記デバイスを認証する認証部と、をさらに備えることを特徴とする請求項９に記載の挑戦応答基盤のＲＴＴ検査装置。
【請求項１２】
前記比較部は、
前記ＲＴＴが所定の臨界時間より長いか、または同じならば、所定の最大反復回数内で前記ＲＴＴ検査を反復的に行うためのフィードバック信号を提供することを特徴とする請求項１１に記載の挑戦応答基盤のＲＴＴ検査装置。
【請求項１３】
前記通信部は、
準備要請メッセージを前記デバイスに送信し、前記デバイスから準備応答メッセージを受信することを特徴とする請求項９に記載の挑戦応答基盤のＲＴＴ検査装置。
【請求項１４】
対称キーを利用して暗号化された乱数を含む挑戦要請メッセージをデバイスから受信する通信部と、
前記対称キーを利用して暗号化された乱数を復号化する復号化部と、を備え、
前記通信部は、前記復号化された乱数を含む挑戦応答メッセージを前記デバイスに送信することを特徴とする挑戦応答基盤のＲＴＴ検査装置。
【請求項１５】
前記復号化部は、
前記挑戦要請メッセージが前記通信部に受信される前に、前記対称キーを利用して乱数マスクを生成する乱数マスク生成部と、
前記挑戦要請メッセージに含まれた暗号化された乱数及び前記乱数マスクを排他的論理和演算（ＸＯＲ）により結合する結合部と、を備えることを特徴とする請求項１４に記載の挑戦応答基盤のＲＴＴ検査装置。
【請求項１６】
前記通信部は、
前記デバイスから準備要請メッセージを受信し、前記デバイスに準備応答メッセージを送信することを特徴とする請求項１４に記載の挑戦応答基盤のＲＴＴ検査装置。
【請求項１７】
乱数を生成するステップと、
対称キーを利用して前記乱数を暗号化するステップと、
前記暗号化された乱数を含む挑戦要請メッセージをデバイスに送信するステップと、
前記挑戦要請メッセージを受信し、かつ前記対称キーを利用して前記暗号化された乱数を復号化した前記デバイスから、前記乱数を含む挑戦応答メッセージを受信するステップと、
前記挑戦応答メッセージが受信された時刻及び前記挑戦要請メッセージが送信された時刻に基づいてＲＴＴを決定するステップと、を含む挑戦応答基盤のＲＴＴ検査方法を具現するためのプログラムが記録されたコンピュータで読み取り可能な記録媒体。
【請求項１８】
対称キーを利用して暗号化された乱数を含む挑戦要請メッセージをデバイスから受信す

るステップと、
前記対称キーを利用して前記暗号化された乱数を復号化するステップと、
前記復号化された乱数を含む挑戦応答メッセージを前記デバイスに送信するステップと、を含む挑戦応答基盤のＲＴＴ検査方法を具現するためのプログラムが記録されたコンピュータで読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デバイス間の隣接性検査方法に係り、より詳細には、ＲＴＴ（Ｒｏｕｎｄ Ｔｒｉｐ Ｔｉｍｅ）測定値を利用してデバイス間の隣接性を検査するための挑戦応答基盤のＲＴＴ検査方法、装置及びその方法を記録したコンピュータで読み取り可能な記録媒体に関する。
【背景技術】
【０００２】
最近、ＩＰネットワークインフラが発達するにつれて、家庭内のデバイスを連動させるためのホームネットワーク技術が注目されている。ホームネットワーク技術での争点のうち一つは、ＩＰネットワーク基盤で各デバイスが物理的に一家庭内に位置しているということをどのように判断するかの問題、すなわち、局地化（Ｌｏｃａｌｉｚａｔｉｏｎ）の問題である。これは、一家庭内にあるデバイス間でのみコンテンツを自由に共有できるようにする政策の前提になるため、非常に重要である。
【０００３】
図１は、局地化が適用される一般的なネットワーク環境を示す図である。図１を参照するに、コンテンツ提供者１１０は、正当な権限を持つコンテンツユーザーのホームネットワーク１２０内に位置したデバイスＡ　１２２にコンテンツを提供する。コンテンツユーザーは、デバイスＡ　１２２でのみならず、ホームネットワーク１２０内にあるデバイスＢ　１２４、デバイスＣ　１２６及びデバイスＤ　１２８でもコンテンツを使用できなければならない。しかし、ホームネットワーク１２０ではない外部のネットワーク１３０に位置したデバイスＥ　１３２には前記コンテンツの配布が許容されてはならない場合がある。したがって、デバイスＡ　１２２から他のデバイスへのコンテンツ伝送を制御するためには、デバイスＡ　１２２及び他のデバイス間の隣接性検査が先行されねばならない。
【０００４】
隣接性検査の技術的解決法には、ＲＴＴ検査方式及びホップカウント制限方式がある。ＲＴＴ検査は、二つのデバイス間で特定メッセージを伝送した後、再び返してもらう時間を測定して、その時間が所定時間以下であるかどうかを決定する方式である。ホップカウント制限方式は、あるメッセージがＩＰネットワークを通じて目的地デバイスに到達するまで経ることができるルーターの数を制限する方式である。
【０００５】
ＲＴＴ検査方式の例として、ＤＴＣＰ－ＩＰのＲＴＴ検査プロトコルがある。ＤＴＣＰ－ＩＰのＲＴＴ検査プロトコルは、シーケンス番号を基盤として認証コードを交換する方式を使用する。すなわち、両側のデバイスは、キー値及び０から順次に１ずつ増加するシーケンス番号を利用してＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）を生成し、該生成されたＭＡＣを互いに伝送する。ＲＴＴ検査は、ＭＡＣの伝送時間を測定する方式で行われる。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明が解決しようとする技術的課題は、デバイス間の効率的な隣接性検査を可能にする、暗号化アルゴリズムを利用した挑戦応答基盤のＲＴＴ検査方法、装置及びプログラム記録媒体を提供するところにある。
【０００７】

また、本発明が解決しようとする技術的課題は、シーケンス番号基盤の認証コード交換方式と差別化される、暗号化アルゴリズムを利用した挑戦応答基盤のＲＴＴ検査方法、装置及びプログラム記録媒体を提供するところにある。

【課題を解決するための手段】

【０００８】

前述した目的を達成するために、本発明の一実施形態による挑戦応答基盤のＲＴＴ検査方法は、乱数を生成するステップと、対称キーを利用して前記乱数を暗号化するステップと、前記暗号化された乱数を含む挑戦要請メッセージをデバイスに送信するステップと、前記挑戦要請メッセージを受信し、かつ前記対称キーを利用して暗号化された乱数を復号化した前記デバイスから、前記乱数を含む挑戦応答メッセージを受信するステップと、前記挑戦応答メッセージが受信された時刻及び前記挑戦要請メッセージが送信された時刻に基づいてＲＴＴを決定するステップと、を含むことを特徴とする。

【０００９】

前記対称キーを利用して前記乱数を暗号化するステップは、前記対称キーを利用して乱数マスクを生成するステップと、前記乱数及び前記乱数マスクを排他的論理和演算（ＸＯＲ）により結合するステップと、を含むことが望ましい。

【００１０】

前記ＲＴＴが所定の臨界時間より短ければ、前記生成された乱数及び前記挑戦応答メッセージに含まれた乱数を比較することによって、前記デバイスを認証するステップをさらに含むことが望ましい。

【００１１】

前記ＲＴＴが所定の臨界時間より長いか、または同じならば、所定の最大反復回数内で前記乱数を生成するステップないし前記ＲＴＴを決定するステップを反復的に行うことが望ましい。

【００１２】

準備要請メッセージを前記デバイスに送信するステップと、前記デバイスから準備応答メッセージを受信するステップと、をさらに含むことが望ましい。

【００１３】

また、前述した目的を達成するために、本発明の他の実施形態による挑戦応答基盤のＲＴＴ検査方法は、デバイスから、対称キーを利用して暗号化された乱数を含む挑戦要請メッセージを受信するステップと、前記対称キーを利用して暗号化された乱数を復号化するステップと、前記復号化された乱数を含む挑戦応答メッセージを前記デバイスに送信するステップと、を含むことを特徴とする。

【００１４】

前記挑戦要請メッセージを受信するステップ以前に、前記対称キーを利用して乱数マスクを生成するステップをさらに含み、前記暗号化された乱数を復号化するステップは、前記挑戦要請メッセージに含まれた暗号化された乱数及び前記乱数マスクを、排他的論理和演算（ＸＯＲ）により結合するステップを含むことが望ましい。

【００１５】

前記デバイスから準備要請メッセージを受信するステップと、前記デバイスに準備応答メッセージを送信するステップと、をさらに含むことが望ましい。

【００１６】

また、前述した目的を達成するために、本発明の一実施形態による挑戦応答基盤のＲＴＴ検査装置は、乱数を生成する乱数生成部と、対称キーを利用して前記乱数を暗号化する暗号化部と、前記暗号化された乱数を含む挑戦要請メッセージをデバイスに送信し、前記挑戦要請メッセージを受信し、かつ前記対称キーを利用して前記暗号化された乱数を復号化した前記デバイスから、前記乱数を含む挑戦応答メッセージを受信する通信部と、前記挑戦応答メッセージが受信された時刻及び前記挑戦要請メッセージが送信した時刻に基づいてＲＴＴを決定するＲＴＴ決定部と、を備えることを特徴とする。

【００１７】

また、前述した目的を達成するために、本発明の他の実施形態による挑戦応答基盤のＲＴＴ検査装置は、対称キーを利用して暗号化された乱数を含む挑戦要請メッセージをデバイスから受信する通信部と、前記対称キーを利用して暗号化された乱数を復号化する復号化部と、を備え、前記通信部は、前記復号化された乱数を含む挑戦応答メッセージを前記デバイスに送信することを特徴とする。

【００１８】

また、前述した目的を達成するために、本発明の一実施形態による挑戦応答基盤のＲＴＴ検査方法を具現するためのプログラムが記録されたコンピュータで読み取り可能な記録媒体は、乱数を生成するステップと、対称キーを利用して前記乱数を暗号化するステップと、前記暗号化された乱数を含む挑戦要請メッセージをデバイスに送信するステップと、前記挑戦要請メッセージを受信し、かつ前記対称キーを利用して前記暗号化された乱数を復号化した前記デバイスから、前記乱数を含む挑戦応答メッセージを受信するステップと、前記挑戦応答メッセージが受信された時刻及び前記挑戦要請メッセージが送信された時刻に基づいてＲＴＴを決定するステップと、を含むことを特徴とする。

【００１９】

また、前述した目的を達成するために、本発明の他の実施形態による挑戦応答基盤のＲＴＴ検査方法を具現するためのプログラムが記録されたコンピュータで読み取り可能な記録媒体は、対称キーを利用して暗号化された乱数を含む挑戦要請メッセージをデバイスから受信するステップと、前記対称キーを利用して前記暗号化された乱数を復号化するステップと、前記復号化された乱数を含む挑戦応答メッセージを前記デバイスに送信するステップと、を含むことを特徴とする。

【発明の効果】

【００２０】

本発明によれば、ＲＴＴ検査に暗号化アルゴリズムを利用した挑戦応答方式を適用することによって、デバイス間の効率的な隣接性検査が可能である。

【００２１】

また、本発明によれば、ＲＴＴ検査のために事前計算の可能な暗号化方法を使用することによって、挑戦応答メッセージの生成に必要な時間を最小化してＲＴＴ検査の信頼度を向上させる。

【発明を実施するための最良の形態】

【００２２】

以下、添付した図面を参照して本発明の望ましい実施形態を詳細に説明する。

【００２３】

図２は、本発明の第１実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するための図である。図２を参照するに、デバイスＡ　２０５及びデバイスＢ　２１０は、ＲＴＴ検査が行われる前にＡＫＥ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）のような過程を通じて対称キー（ＳＫ）２２０、２２５を共有する（ステップ２１５）。以下、本明細書では、デバイスＡ　２０５及びデバイスＢ　２１０は、ＲＴＴ検査を行うための対称キー（ＳＫ）を共有していると仮定する。対称キー（ＳＫ）を共有する方法は、本技術分野の当業者に周知であるので、具体的な説明は省略される。

【００２４】

本発明の第１実施形態による挑戦応答方式を利用したＲＴＴ検査は次のような順序によって進む。

【００２５】

ＲＴＴ検査が始まれば、ＲＴＴ検査装置はデバイスＡ　２０５及びデバイスＢ　２１０間のＲＴＴ検査回数を示すために、デバイスＡ　２０５に内蔵されたカウンタＮの値を０に設定することもある。カウンタＮの設定は、ネットワークのような伝送経路のトラフィックの可変性を考慮して、既定の最大反復回数ほど反復してＲＴＴ測定をするためのことである。数回のＲＴＴの測定結果、ＲＴＴが一度でも所定の臨界時間内に入れば、デバイスＡ　２０５及びデバイスＢ　２１０は隣接していると見なされる。

【００２６】
次いで、デバイスＡ　２０５は乱数Ｒを生成する（ステップ２３０）。カウンタＮが増加するほど乱数Ｒは新たな値に生成される。デバイスＡ　２０５は、対称キーを利用して乱数Ｒを暗号化する（ステップ２３５）。
【００２７】
次いで、デバイスＡ　２０５及びデバイスＢ　２１０は、ＲＴＴ検査を行うための準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄ及び準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを送受信する（ステップ２４０、２４５）。変形された実施形態として、デバイスＡ　２０５とデバイスＢ　２１０との間に準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄ及び準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを送受信する過程（ステップ２４０、２４５）は省略されてもよい。これについては、図４を参照して後述する。さらに他の変形された実施形態として、デバイスＡ　２０５とデバイスＢ　２１０との間に準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄ及び準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを送受信する過程（ステップ２４０、２４５）は、乱数Ｒを生成し、かつ対称キーを利用して乱数Ｒを暗号化する過程（ステップ２３０、２３５）より先行されることもある。
【００２８】
デバイスＡ　２０５は、暗号化された乱数E_{SK}（Ｒ）を含む挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））を生成する。次いで、デバイスＡ　２０５は、デバイスＢ　２１０に挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））を送信し、同時に挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））の送信時刻を測定することによってＲＴＴ測定を始める（ステップ２５０）。
【００２９】
デバイスＢ　２１０は、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））をパージングして、暗号化された乱数E_{SK}（Ｒ）を獲得する。次いで、デバイスＢ　２１０は、対称キー（ＳＫ）を利用して暗号化された乱数E_{SK}（Ｒ）を復号化する（ステップ２５５）。デバイスＢ　２１０は、復号化された乱数Ｒ’を含む挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を生成し、該生成された挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）をデバイスＡ　２０５に伝送する（ステップ２６０）。
【００３０】
デバイスＡ　２０５は、デバイスＢ　２１０から復号化された乱数Ｒ’を含む挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を受信する。同時に、デバイスＡ　２０５は、挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）の受信時刻を測定する。デバイスＡ　２０５は、デバイスＢ　２１０に挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））を送ってから、デバイスＢ　２１０から挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を受けた時までの時間を計算することによってＲＴＴを決定する。
【００３１】
前記のような挑戦応答方式によるＲＴＴ決定によれば、デバイスＡ　２０５がデバイスＢ　２１０に乱数的な性質を含む挑戦要請メッセージを伝送すれば、デバイスＢ　２１０が受信した挑戦要請メッセージにあらかじめ約束された演算を適用して挑戦応答メッセージを導出し、これを再びＡに伝送する。すなわち、デバイスＢ　２１０は、挑戦要請メッセージを受信して初めて挑戦応答メッセージを生成できるため、挑戦応答メッセージはいつも挑戦要請メッセージ以後に生成されたものであることを確認できる。また、挑戦応答メッセージを決定するためにデバイスＡ　２０５及びデバイスＢ　２１０が事前に共有している秘密値（すなわち、対称キー）を利用した演算過程が含まれるため、挑戦応答メッセージを送るデバイスに対する認証が可能であるという長所がある。
【００３２】
次いで、デバイスＡ　２０５は、決定されたＲＴＴが事前に定義された臨界時間ＴＬ（Ｔｉｍｅ　Ｌｉｍｉｔ）より短いかどうかを決定する（ステップ２６５）。決定されたＲ

ＴＴが臨界時間ＴＬより短ければ、デバイスＡ　２０５は、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））に含まれた乱数Ｒをデバイスｂ　２１０から受信された復号化された乱数Ｒ’と比較して、デバイスＢ　２１０を認証する（ステップ２７０）。比較結果、乱数Ｒと乱数Ｒ’とが同一ならば、デバイスＡ　２０５はＲＴＴ検査が成功したと判断する。すなわち、デバイスＡ　２０５は、デバイスＢ　２１０が隣接していると判断する。一方、決定されたＲＴＴが臨界時間ＴＬより長いかか、または同じならば、デバイスＡ　２０５は、カウンタＮを１ほど増加させる。次いで、デバイスＡ　２０５は、カウンタＮが最大反復回数に到達したかどうかを判断する（ステップ２７５）。最大反復回数は、ネットワークのような伝送経路のトラフィックの可変性を考慮して事前に定義される。

【００３３】

もし、カウンタＮが最大反復回数と同じならば（または最大反復回数より大きければ）、デバイスＡ　２０５は、デバイスＢ　２１０が隣接していないと判断する。一方、カウンタＮが最大反復回数より小さければ、デバイスＡ　２０５は、ステップ２３０ないしステップ２６５を反復する。すなわち、デバイスＡ　２０５は、新たな乱数を再び生成して暗号化してデバイスＢ　２１０に伝送し、デバイスＢ　２１０は、受信された暗号化された乱数を復号化してデバイスＡ　２０５に伝達し、デバイスＡ　２０５は、暗号化された乱数の送信時間及び復号化された乱数の受信時間を利用してＲＴＴを再決定する。この時、デバイスＢ　２１０は、デバイスＡ　２０５から準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄを受信すれば（ステップ２８０）、準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを再伝送するステップを進める（ステップ２４５）。

【００３４】

図３は、本発明の第２実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するための図である。図２の実施形態が実際システムで具現される場合に、プロセッサーの演算性能が優秀でなければ、デバイスＢ　３１０は、挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を計算するための長時間を要求する。その結果、ＲＴＴ検査の信頼度が落ちる恐れがある。

【００３５】

したがって、本発明の第２実施形態は、相対的に演算性能が落ちるシステムでのさらに正確なＲＴＴ検査のために、デバイスＢ　３１０による挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅの計算に必要な時間を最小化する方法を提供する。したがって、第２実施形態は、事前計算の可能な暗号化方法を使用する方法を提供する。

【００３６】

図３を参照するに、まずＲＴＴ検査装置は、デバイスＡ　３０５及びデバイスＢ　３１０のカウンタＮを０に設定できる（図示せず）。次いで、デバイスＡ　３０５は乱数Ｒを生成し、また乱数Ｒを暗号化するための乱数マスクＲ＿Ｍａｓｋを生成する。

【００３７】

本発明の第２実施形態で使われる事前計算の可能な暗号化アルゴリズムは、ストリーム暗号（例えば、ＲＣ４）、ＣＴＲモード（例えば、ＡＥＳ－ＣＴＲ）などがある。本実施形態では、事前計算を利用して挑戦要請メッセージ及び挑戦応答メッセージを生成するための過程は、それぞれ二ステップに分けて進む。

【００３８】

デバイスＡ　３０５は、乱数Ｒを暗号化するための事前ステップとして、乱数Ｒ及び乱数マスクＲ＿Ｍａｓｋを生成する。乱数マスクＲ＿Ｍａｓｋは、暗号化アルゴリズム及びデバイス３０５、３１０間に秘密で共有される対称キーを利用して生成された乱数列を意味する。乱数Ｒは、対称キーとは関係なくランダムに生成されたものであることに対し、乱数マスクＲ＿Ｍａｓｋは、対称キーを利用して生成されたものである。

【００３９】

次いで、デバイスＡ　３０５は、前記ステップで生成された乱数マスクＲ＿Ｍａｓｋ及び乱数Ｒを排他的論理和演算（ＸＯＲ）により結合することによって、暗号文を生成する

。一般的に、乱数マスクＲ＿Ｍａｓｋを生成するためには長時間がかかるが、ＸＯＲ演算を行うには非常に短時間がかかる。

【００４０】

次いで、ＲＴＴ検査装置は、乱数Ｒ及び乱数マスクＲ＿Ｍａｓｋを排他的論理和演算により結合することによって乱数Ｒを暗号化する（ステップ３３０）。

【００４１】

次いで、デバイスＡ　３０５は、ＲＴＴ検査を行うための準備要請メッセージＲＴＴ＿Ｒｅａｄｙをデバイス Ｂ　３１０に送信する（ステップ３３５）。変形された実施形態として、デバイスＡ　２０５とデバイスＢ　２１０との間に準備要請メッセージ及び準備応答メッセージを送受信するステップ３３５及び３４５は省略されてもよい。

【００４２】

デバイスＢ　３１０は、暗号化された乱数E_{SK}（Ｒ）を復号化するための事前ステップとして乱数マスクＲ＿Ｍａｓｋを生成する（ステップ３４０）。ただし、本発明の第２実施形態の重要な特徴として、デバイスＢ　３１０は、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））を受信する前に乱数マスクＲ＿Ｍａｓｋを生成せねばならない。例えば、デバイスＢ　３１０は、デバイスＡ　３０５から準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄを受信（ステップ３３５）した後、対称キーを利用して乱数マスクＲ＿Ｍａｓｋを生成できる。

【００４３】

乱数マスクＲ＿Ｍａｓｋを生成した後、デバイスＢ　３１０は、デバイスＡ　３０５に準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを伝送する。変形された実施形態として、デバイスＢ　３１０は、デバイスＡ　３０５に準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを伝送した後に乱数マスクＲ＿Ｍａｓｋを生成してもよく、準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄを受信する前に乱数マスクＲ＿Ｍａｓｋを生成してもよい。

【００４４】

デバイスＡ　３０５は、暗号化された乱数E_{SK}（Ｒ）を含む挑戦要請メッセージを生成してデバイスＢ　３１０に送信して、送信時刻を測定する。

【００４５】

デバイスＢ　３１０は、暗号化された乱数E_{SK}（Ｒ）を含む挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））を受信した後、乱数マスクＲ＿Ｍａｓｋ及び暗号化された乱数E_{SK}（Ｒ）を排他的論理和演算（ＸＯＲ）により結合することによって、復号化された乱数Ｒ’を生成する（ステップ３５５）。次いで、デバイスＢ　３１０は、復号化された乱数Ｒ’を含む挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を生成してデバイスＡ　３０５に送信する（ステップ３６０）。

【００４６】

デバイスＡ　３０５は、デバイスＢ　３１０から復号化された乱数Ｒ’を含む挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を受信し、受信時間を測定する。デバイスＡ　３０５は、デバイスＢ　３１０に挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅを送った後から挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅを受けるまでの時間を計算することによって、ＲＴＴを決定できる。

【００４７】

前述したところによれば、デバイスＢ　３１０が挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））を受信した後、挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を送信するまでの時間を最小化できる。

【００４８】

以下、ステップ３６５ないしステップ３８０は、図２のステップ２６５ないしステップ２８０と類似して動作するので、追加的な説明は省略する。

【００４９】

図４は、本発明の第３実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するた

めの図である。本発明の第３実施形態は、図３の事前計算を利用したＲＴＴ検査システムでＲＴＴ＿Ｒｅａｄｙを省略したものである。

【００５０】

デバイスＢ　４１０の演算性能がデバイスＡ　４０５と比較して同等であるか、または優越な場合、デバイスＡ　４０５が挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅを生成する間に乱数マスクＲ＿Ｍａｓｋを生成することができるため、準備要請メッセージ及び準備応答メッセージの送受信過程を省略できる。

【００５１】

したがって、デバイスＢ　４１０は、デバイスＡ　４０５から準備要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅを受信する前に乱数マスクＲ＿Ｍａｓｋを生成し、デバイスＡ　４０５から受信された暗号化された乱数E_{SK}（Ｒ）を、乱数マスクＲ＿Ｍａｓｋと排他的論理和演算により結合して挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅを生成できる。

【００５２】

残りのステップは、図２及び図３で説明したものと類似して動作するので、追加的な説明は省略される。

【００５３】

図５は、本発明の第４実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するための図である。

【００５４】

図２ないし図４では、デバイスＡは、乱数Ｒを暗号化して挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅとして伝送し、デバイスＢは、暗号化された乱数E_{SK}（Ｒ）を復号化したＲ’を、挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅとして伝送する。

【００５５】

しかし、図５を参照するに、第４実施形態では、デバイスＡは、暗号化されていない乱数Ｒを含む挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（Ｒ）をデバイスＢに伝送し、デバイスＢは、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（Ｒ）に含まれた乱数Ｒを暗号化して、挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（E_{SK}（Ｒ’））に伝送する。

【００５６】

デバイスＡは、最大反復回数内で挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（Ｒ）の送信時刻及びＲＴＴ＿Ｒｅｓｐｏｎｓｅ（E_{SK}（Ｒ’））の受信時刻を測定して、ＲＴＴを決定できる。また、デバイスＡは、受信された挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（E_{SK}（Ｒ’））に含まれた暗号化された乱数E_{SK}（Ｒ’）を復号化し、デバイスＢに伝送された乱数Ｒと比較して隣接性如何を判断できる。

【００５７】

図６は、本発明の一実施形態による挑戦応答基盤のＲＴＴ検査装置を示した機能ブロック図である。本発明の一実施形態による挑戦応答基盤のＲＴＴ検査装置は、デバイスＡ　６１０に備えられるか（以下、‘第１ＲＴＴ検査装置’という）、またはデバイスＢ　６６０に備えられうる（以下、‘第２ＲＴＴ検査装置’という）。

【００５８】

まず、第１ＲＴＴ検査装置は、乱数生成部６１５、暗号化部６２０、通信部６３５、ＲＴＴ決定部６４０、及び隣接性判断部６４５を備える。

【００５９】

乱数生成部６１５は、ＲＴＴ検査が始まれば、乱数を生成する。

【００６０】

暗号化部６２０は、デバイスＢ　６６０と共有する対称キーを利用して、乱数生成部６１５で生成された乱数を暗号化する。暗号化部６２０は、例えば、対称キーを利用して乱数マスクＲ＿Ｍａｓｋを生成する乱数マスク生成部６３０、及び乱数マスクＲ＿Ｍａｓｋを乱数Ｒと排他的論理和演算（ＸＯＲ）により結合する結合部６２５を備えることができ

る。乱数マスクR＿Ｍａｓｋの生成については前述したので、追加的な説明は省略される。

【００６１】

通信部６３５は、暗号化された乱数E_{SK}（R）を含む挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（R））をデバイスＢ　６６０に送信し、デバイスＢ　６６０から、対称キーを利用して復号化された乱数Ｒ’を含む挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）を受信する。また、通信部６３５は、準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄをデバイスＢ　６６０に送信し、デバイスＢ　６６０から準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを受信することもできる。

【００６２】

ＲＴＴ決定部６４０は、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））の送信時刻及び挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）の受信時刻を測定して、ＲＴＴを決定する。

【００６３】

隣接性判断部６４５は、ＲＴＴ及び所定の臨界時間を比較する比較部６５０及び認証部６５５を備えることができる。ここで、臨界時間は、デバイスＡ　６１０及びデバイスＢ　６６０を隣接していると判断できる時間であって、事前に定義される値を持つ。デバイスＡ　６１０のユーザーは、状況により多様な値で前記臨界時間を設定できる。

【００６４】

認証部６５５は、ＲＴＴが臨界時間より短ければ、生成された乱数Ｒと挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）に含まれた乱数Ｒ’とを比較することによって、デバイスＢ　６６０を認証する。

【００６５】

比較部６５０は、ＲＴＴが所定の臨界時間より長いか、または同じならば、所定の最大反復回数内でＲＴＴ検査を反復的に行うためのフィードバック信号を生成して、乱数生成部６１５、乱数マスク生成部６３０などに提供できる（図示せず）。

【００６６】

また、第２ＲＴＴ検査装置は、通信部６６５及び復号化部６７０を備える。

【００６７】

通信部６６５は、対称キーを利用して暗号化された乱数E_{SK}（Ｒ）を含む挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））を、デバイスＡ　６１０から受信する。通信部６６５は、復号化された乱数Ｒ’を含む挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）をデバイスＡ　６１０に送信する。また、通信部６６５は、デバイスＡ　６１０から準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄを受信し、デバイスＡ　６１０に準備応答メッセージＲＴＴ。Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを送信できる。

【００６８】

復号化部６７０は、対称キーを利用して暗号化された乱数E_{SK}（Ｒ）を復号化して、乱数Ｒ’を生成する。望ましくは、復号化部６７０は、乱数マスク生成部６７５及び結合部６８０を備えることができる。

【００６９】

乱数マスク生成部６７５は、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））が通信部６６５に受信される前に、対称キーを利用して乱数マスクＲ＿Ｍａｓｋを生成する。

【００７０】

結合部６８０は、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））に含まれた暗号化された乱数E_{SK}（Ｒ）及び乱数マスクＲ＿Ｍａｓｋを、排他的論理和演算（ＸＯＲ）により結合して通信部６６５に出力する。

【００７１】

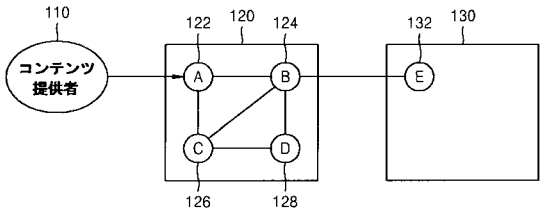
図７は、本発明の一実施形態による挑戦応答基盤のＲＴＴ検査方法を示したフローチャ

ートである。図７を参照するに、ステップ７０５では、カウンタＮが０に設定される。
【００７２】
ステップ７１０では、乱数Ｒが生成される。
【００７３】
ステップ７１５では、乱数Ｒは、所定のデバイスと共有する対称キー（ＳＫ）を利用して暗号化される。乱数を暗号化するステップは、対称キーを利用して乱数マスクＲ＿Ｍａｓｋを生成するステップ、及び生成された乱数Ｒと乱数マスクＲ＿Ｍａｓｋとを排他的論理和演算により結合するステップを含むことができる。
【００７４】
ステップ７２０では、暗号化された乱数E_{SK}（Ｒ）を含む挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））が所定のデバイスに送信され、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））の送信時刻が測定される。
【００７５】
ステップ７２５では、所定のデバイスから復号化された乱数Ｒ’を含む挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）が受信され、挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）の受信時刻が測定される。
【００７６】
ステップ７３０では、挑戦応答メッセージＲＴＴ＿Ｒｅｓｐｏｎｓｅ（Ｒ’）の受信時刻、及び挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））の送信時刻を利用してＲＴＴが決定される。
【００７７】
ステップ７３５では、ＲＴＴが所定の臨界時間と比較される。比較結果、ＲＴＴが所定の臨界時間より短ければ、生成された乱数Ｒと挑戦応答メッセージに含まれた乱数Ｒ’とを比較することによって、所定のデバイスを認証できる（ステップ７４０）。生成された乱数Ｒ及び挑戦応答メッセージに含まれた乱数Ｒ’が同一ならば、所定のデバイスは隣接していると判断される（ステップ７４５）。一方、生成された乱数Ｒ及び挑戦応答メッセージに含まれた乱数Ｒ’が同一でなければ、ＲＴＴ検査は失敗したと判断される（ステップ７５０）。
【００７８】
ステップ７３５の比較結果、ＲＴＴが所定の臨界時間より長いか、または同じならば、ステップ７５５でカウンタＮを１ほど増加させる。ステップ７６０では、カウンタＮが所定の最大反復回数より多いか、または同じでなければ（すなわち、最大反復回数内で）、ステップ７１０からプロセスを再び反復的に行える。一方、カウンタＮが所定の最大反復回数より多いか、または同じならば、デバイスは隣接していないと判断される（ステップ７６５）。
【００７９】
また、本発明の一実施形態による挑戦応答基盤のＲＴＴ検査方法の準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄを所定のデバイスに送信し、所定のデバイスから準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを受信するステップをさらに含むことができる（図示せず）。
【００８０】
図８は、本発明の他の実施形態による挑戦応答基盤のＲＴＴ検査方法を示したフローチャートである。
【００８１】
ステップ８１０では、挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））が受信される前に、対称キーを利用して乱数マスクが生成される。
【００８２】
ステップ８２０では、対称キーを利用して暗号化された乱数E_{SK}（Ｒ）を含む挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））が、所定のデバイスから受信される。

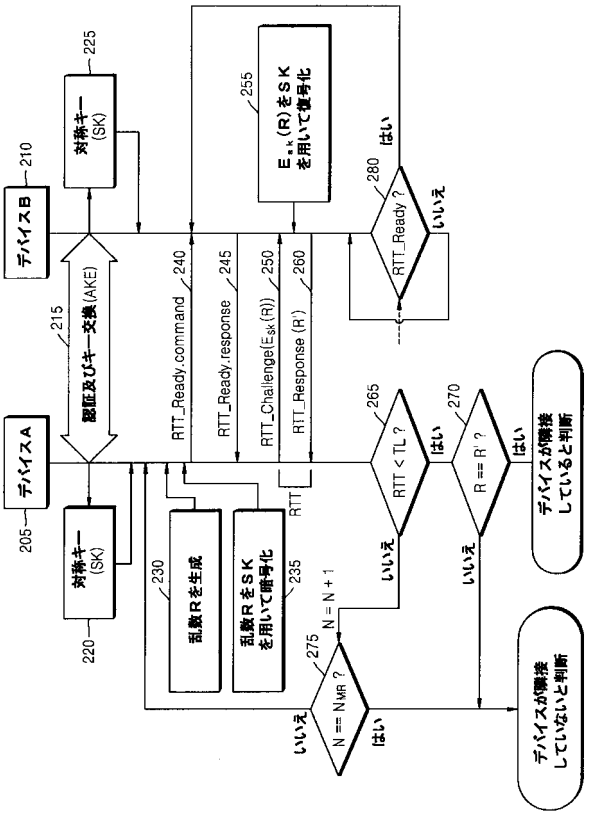
【００８３】
ステップ８３０では、対称キーを利用して暗号化された乱数E_{SK}（Ｒ）が復号化されて、復号化された乱数Ｒ’が生成される。挑戦要請メッセージＲＴＴ＿Ｃｈａｌｌｅｎｇｅ（E_{SK}（Ｒ））に含まれた暗号化された乱数E_{SK}（Ｒ）及び乱数マスクＲ＿Ｍａｓｋは、排他的論理和演算（ＸＯＲ）により結合されうる。
【００８４】
ステップ８４０では、復号化された乱数Ｒ’を含む挑戦応答メッセージは前記デバイスに送信される。
【００８５】
また、本発明の他の実施形態による挑戦応答基盤のＲＴＴ検査方法は、デバイスから準備要請メッセージＲＴＴ＿Ｒｅａｄｙ．ｃｏｍｍａｎｄを受信するステップ、及び所定のデバイスに準備応答メッセージＲＴＴ＿Ｒｅａｄｙ．ｒｅｓｐｏｎｓｅを送信するステップを含むこともできる。
【００８６】
また、本発明による挑戦応答基盤のＲＴＴ検査方法を行うためのプログラムは、コンピュータで読み取り可能な記録媒体にコンピュータで読み取り可能なコードとして具現することができる。コンピュータで読み取り可能な記録媒体は、コンピュータシステムによって読み取られるデータが保存されるあらゆる種類の保存装置を含む。コンピュータで読み取り可能な記録媒体の例には、ＲＯＭ、ＲＡＭ、ＣＤ－ＲＯＭ、磁気テープ、フロッピー（登録商標）ディスク、光データ保存装置などがある。また、コンピュータで読み取り可能な記録媒体は、ネットワークに連結されたコンピュータシステムに分散されて、分散方式でコンピュータで読み取り可能なコードとして保存されて実行されうる。
【００８７】
これまで本発明についてその望ましい実施形態を中心に説明した。当業者ならば、本発明が本発明の本質的な特性から逸脱しない範囲内で変形された形態で具現されるということを理解できるであろう。したがって、開示された実施形態は限定的な観点ではなく説明的な観点で考慮されねばならない。本発明の範囲は、前述した説明ではなく特許請求の範囲に現れており、それと同等な範囲内にあるあらゆる差異点は本発明に含まれていると解釈されねばならない。
【産業上の利用可能性】
【００８８】
本発明は、デバイス関連の技術分野に好適に用いられる。
【図面の簡単な説明】
【００８９】
【図１】局地化が適用される一般的なネットワーク環境を示す図である。
【図２】本発明の第１実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するための図である。
【図３】本発明の第２実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するための図である。
【図４】本発明の第３実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するための図である。
【図５】本発明の第４実施形態による挑戦応答基盤のＲＴＴ検査システムを説明するための図である。
【図６】本発明の一実施形態による挑戦応答基盤のＲＴＴ検査装置を示した機能ブロック図である。
【図７】本発明の一実施形態による挑戦応答基盤のＲＴＴ検査方法を示したフローチャートである。
【図８】本発明の他の実施形態による挑戦応答基盤のＲＴＴ検査方法を示したフローチャートである。
【符号の説明】

【００９０】
２０５　デバイスＡ
２１０　デバイスＢ
２１５　ＡＫＥ
２２０、２２５　対称キー（ＳＫ）

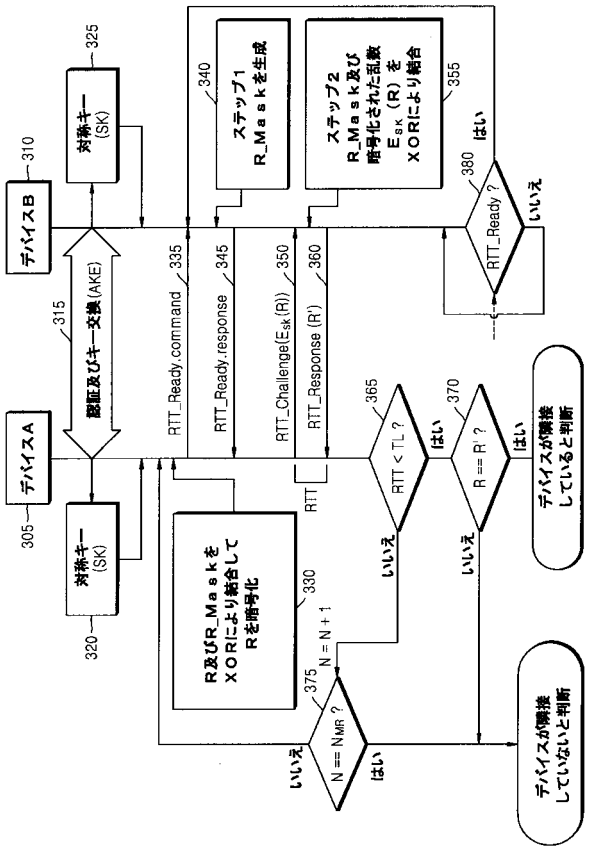
【図１】



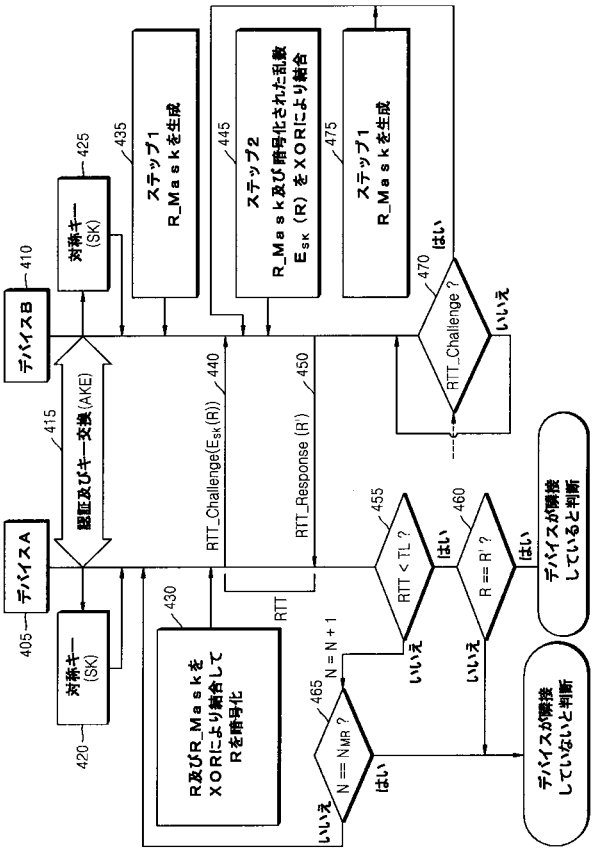
【図２】



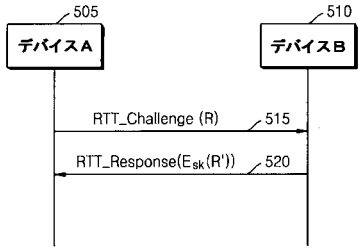
【図３】


デバイスB
310
対称キー (SK)
325
ステップ1 R_Maskを生成
340
ステップ2 R_Mask及び暗号化された乱数 E_{SK} (R) をXORにより結合
355
はい
380
RTT_Ready ?
いいえ
315
認証及びキー交換 (AKE)
RTT_Ready.command
335
RTT_Ready.response
345
RTT_Challenge(E_{SK}(R))
350
RTT_Response (R')
360
デバイスA
305
対称キー (SK)
320
R及びR_MaskをXORにより結合してRを暗号化
330
RTT
365
RTT < TL ?
はい
いいえ
370
R == R' ?
はい
いいえ
N = N + 1
375
$N == N_{MR}$?
いいえ
はい
デバイスが隣接していると判断
デバイスが隣接していないと判断

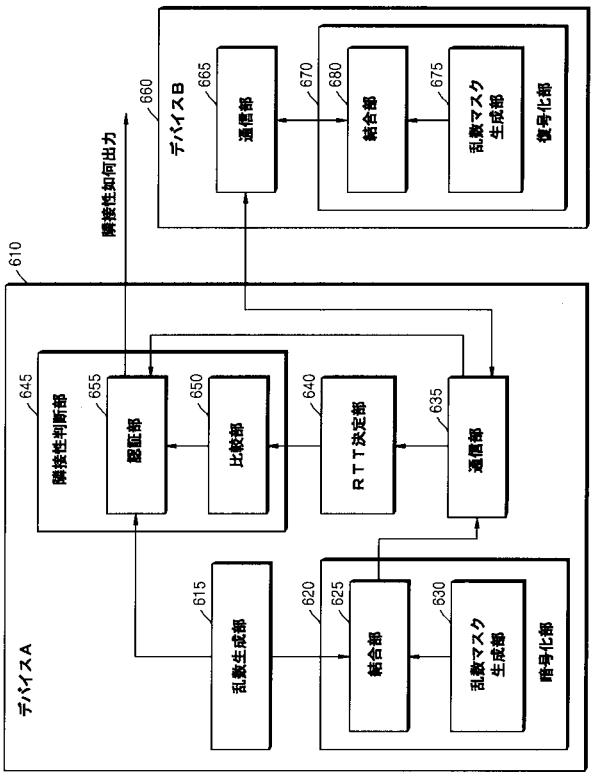
【図４】


デバイスB
410
対称キー (SK)
425
ステップ1 R_Maskを生成
435
ステップ2 R_Mask及び暗号化された乱数 E_{SK} (R) をXORにより結合
445
ステップ1 R_Maskを生成
475
はい
470
RTT_Challenge ?
いいえ
415
認証及びキー交換 (AKE)
RTT_Challenge(E_{SK}(R))
440
RTT_Response (R')
450
デバイスA
405
対称キー (SK)
420
R及びR_MaskをXORにより結合してRを暗号化
430
RTT
455
RTT < TL ?
はい
いいえ
460
R == R' ?
はい
いいえ
N = N + 1
465
$N == N_{MR}$?
いいえ
はい
デバイスが隣接していると判断
デバイスが隣接していないと判断

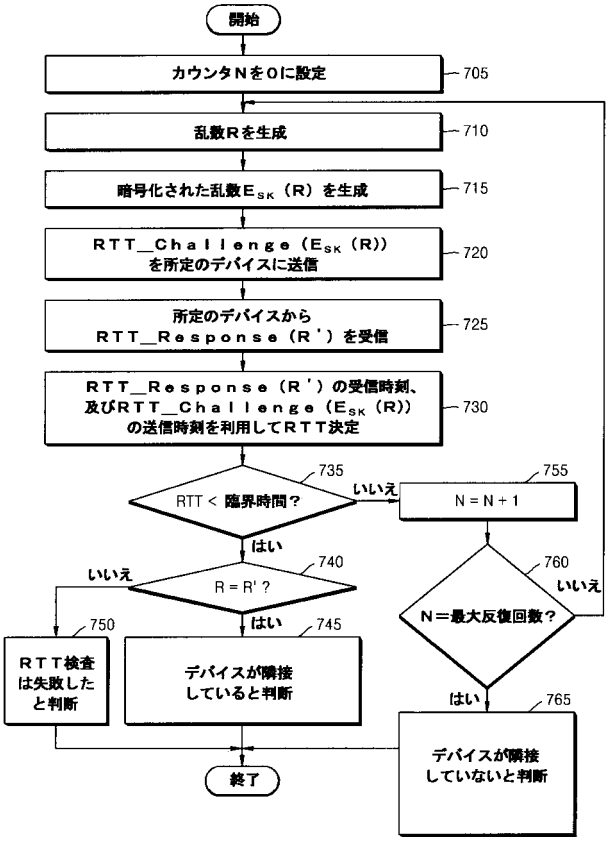
【図５】


505
デバイスA
510
デバイスB
RTT_Challenge (R)
515
RTT_Response(E_{SK}(R'))
520

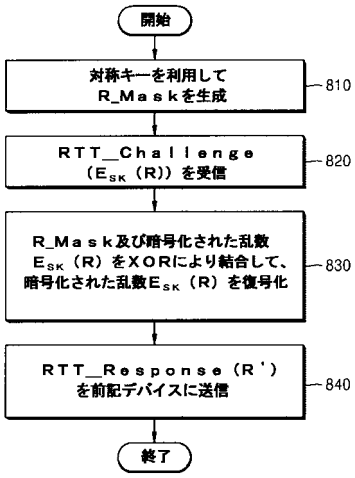
【図６】


610
隣接性如何出力
デバイスB
660
通信部
665
結合部
680
670
乱数マスク生成部
675
暗号化部
デバイスA
隣接性判断部
645
認証部
655
比較部
650
RTT決定部
640
通信部
635
乱数生成部
615
結合部
625
620
乱数マスク生成部
630
暗号化部

【図７】


開始
カウンタNを0に設定
705
乱数Rを生成
710
暗号化された乱数E_{SK}（R）を生成
715
RTT_Challenge（E_{SK}（R））を所定のデバイスに送信
720
所定のデバイスからRTT_Response（R'）を受信
725
RTT_Response（R'）の受信時刻、及びRTT_Challenge（E_{SK}（R））の送信時刻を利用してRTT決定
730
735
RTT < 臨界時間？
いいえ
755
N = N + 1
はい
740
R = R' ?
いいえ
760
N＝最大反復回数？
いいえ
750
RTT検査は失敗したと判断
はい
745
デバイスが隣接していると判断
はい
765
デバイスが隣接していないと判断
終了

【図８】


開始
対称キーを利用してR_Maskを生成
810
RTT_Challenge（E_{SK}（R））を受信
820
R_Mask及び暗号化された乱数E_{SK}（R）をXORにより結合して、暗号化された乱数E_{SK}（R）を復号化
830
RTT_Response（R'）を前記デバイスに送信
840
終了

フロントページの続き

(72)発明者　朴　志　淳
大韓民国京畿道水原市靈通区梅灘洞１７２－２６番地１０１号
(72)発明者　愼　峻　範
大韓民国京畿道水原市靈通区靈通洞　サルグゴル７團地アパート　７１７棟１０４号（番地なし）

Ｆターム(参考) 5J104 AA07 AA16 EA04 EA08 EA18 JA03 KA02 KA04 KA06 NA02
NA37 NA38 PA07
5K033 AA08 CC01 DB20 DB21 EA02 EA05