(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4631423号
(P4631423)
(45)発行日　平成23年2月16日(2011.2.16)　(24)登録日　平成22年11月26日(2010.11.26)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 15/00	(2006.01)	G06F	15/00	310E
H04L 12/22	(2006.01)	H04L	12/22	

請求項の数 8　(全 29 頁)

(21)出願番号　特願2004-359847 (P2004-359847)
(22)出願日　平成16年12月13日 (2004.12.13)
(65)公開番号　特開2006-173735 (P2006-173735A)
(43)公開日　平成18年6月29日 (2006.6.29)
審査請求日　平成18年12月13日 (2006.12.13)

(73)特許権者　000000295
沖電気工業株式会社
東京都港区西新橋三丁目１６番１１号
(74)代理人　100082050
弁理士　佐藤　幸男
(72)発明者　松村　靖子
東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内

審査官　松平　英

最終頁に続く

(54)【発明の名称】メッセージの認証方法と該認証方法を用いたメッセージ認証装置およびメッセージ認証システム

(57)【特許請求の範囲】
【請求項１】
送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行う認証方法において、
前記認証鍵にインデックス情報を対応付けた認証鍵テーブルが前記送信装置および前記受信装置間で秘密裡に保持されており、
前記送信装置において、
前記メッセージに対する前記認証子を生成すること、
生成した前記認証子、該認証子を生成するための前記認証鍵に対する前記インデックス情報および前記メッセージを前記受信装置に送信すること、
前記受信装置において、
前記送信装置からの前記メッセージ、前記認証子および前記インデックス情報を受信すること、
前記インデックス情報を認証すること、
認証したインデックス情報に基づいて保持している前記認証鍵テーブルを検索し、当該インデックス情報に対応する前記認証鍵を取得すること、
取得した前記認証鍵および受信した前記メッセージに基づいて認証用認証子を生成する

こと、
生成された認証用認証子を用いて前記メッセージの認証を行うことを含み、
前記メッセージは各パケットから成り、
前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、
前記送信装置は、
予め任意に指定したインデックス情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にあるインデックス情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成すること、
生成したインデックス情報チェーンにおいて、インデックス情報I_0を、予め前記受信装置に送付し、該受信装置で保持させること、
前記受信装置は、
前記メッセージおよび前記認証子と共に受信する前記インデックス情報I_iを受信すると、前記一方向性関数ｆを用いてｆ（I_i）を求め、該ｆ（I_i）と、保持しているインデックス情報I_{i-1}との比較照合を行なって前記インデックス情報I_iの認証を行うこと、
前記インデックス情報I_iを認証すると、保持している前記インデックス情報I_{i-1}に代えて、認証された前記インデックス情報I_iを保持することを特徴とするメッセージ認証方法。

【請求項２】
送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うメッセージ認証方法において、
前記認証鍵を生成するための鍵関数が前記送信装置および前記受信装置間で秘密裡に保持されており、
前記送信装置において、
前記認証鍵を得るための媒介径数情報を前記鍵関数に代入し、認証鍵を生成すること、
生成した認証鍵を用いて前記メッセージに対する前記認証子を生成すること、
生成した認証子と、該認証子を生成するための前記認証鍵に対する前記媒介径数情報と、前記メッセージとを前記受信装置に送信すること、
前記受信装置において、
前記送信装置からの前記メッセージ、前記認証子および前記媒介径数情報を受信すること、
前記媒介径数情報を認証すること、
認証された媒介径数情報を、保持している前記鍵関数に代入し、認証用認証鍵を生成すること、
生成した前記認証用認証鍵および受信した前記メッセージに基づいて認証用認証子を生成すること、
生成した認証用認証子を用いて前記メッセージの認証を行うことを含み、
前記メッセージは各パケットから成り、
前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、
前記送信装置は、
予め任意に指定した媒介径数情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｉはパケットの総数、$n \geqq i \geqq 1$）と示す関係にある媒介径数情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成すること、
生成した媒介径数情報チェーンにおいて、媒介径数情報I_0を、予め前記受信装置に送付し、該受信装置で保持させること、
前記受信装置は、
前記メッセージおよび前記認証子と共に受信する前記媒介径数情報I_iを受信すると、

前記一方向性関数ｆを用いてｆ（Ｉ$_{i}$）を求め、該ｆ（Ｉ$_{i}$）と、保持している媒介径数情報Ｉ$_{i-1}$との比較照合を行なって前記媒介径数情報Ｉ$_{i}$の認証を行うこと、

前記媒介径数情報Ｉ$_{n}$を認証すると、保持している前記媒介径数情報Ｉ$_{i-1}$に代えて、認証された前記媒介径数情報Ｉ$_{i}$を保持することを特徴とするメッセージ認証方法。

【請求項３】

送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うメッセージ認証システムにおいて、

前記認証鍵にインデックス情報を対応付けた認証鍵テーブルが前記送信装置および前記受信装置間で秘密裡に保持されており、

前記送信装置は、

前記メッセージに対する前記認証子を生成する認証子生成部と、

生成した前記認証子、該認証子を生成するための前記認証鍵に対する前記インデックス情報および前記メッセージを前記受信装置に送信する送信部とを備えており、

前記受信装置は、

前記送信装置からの前記メッセージ、前記認証子および前記インデックス情報を受信する受信部と、

前記インデックス情報を認証するインデックス情報認証部と、

認証されたインデックス情報に基づいて保持している前記認証鍵テーブルを検索し、当該インデックス情報に対応する前記認証鍵を取得する認証鍵取得部と、

取得した前記認証鍵および受信した前記メッセージに基づいて認証用認証子を生成する認証用認証子生成部と、

生成した認証用認証子を用いて前記メッセージの認証を行う照合認証部とを備え、

前記メッセージは各パケットから成り、

前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、

前記送信装置は、

予め任意に指定したインデックス情報Ｉ$_{n}$に対し一方向性関数ｆを用いてＩ$_{i-1}$＝ｆ（Ｉ$_{i}$）（但し、ｎはパケットの総数、ｎ≧ｉ≧１）と示す関係にあるインデックス情報チェーン（Ｉ$_{0}$（＝ｆ（Ｉ$_{1}$））、・・・、Ｉ$_{n}$）を生成するインデックス情報チェーン生成部と、

生成したインデックス情報チェーンにおいて、インデックス情報Ｉ$_{0}$を、予め前記受信装置に送付し、該受信装置で保持させるインデックス情報チェーン送信部とを備えており、

前記インデックス情報認証部は、

前記メッセージおよび前記認証子と共に受信する前記インデックス情報Ｉ$_{i}$を受信すると、前記一方向性関数ｆを用いてｆ（Ｉ$_{i}$）を求め、該ｆ（Ｉ$_{i}$）と、保持しているインデックス情報Ｉ$_{i-1}$との比較照合を行なって前記インデックス情報Ｉ$_{i}$の認証を行う比較判定部と、

前記インデックス情報Ｉ$_{i}$を認証すると、保持している前記インデックス情報Ｉ$_{i-1}$に代えて、認証された前記インデックス情報Ｉ$_{i}$を保持するインデックス情報保持部と、を備えることを特徴とするメッセージ認証システム。

【請求項４】

送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うメッセージ認証システムにおいて、

前記認証鍵を生成するための鍵関数が前記送信装置および前記受信装置間で秘密裡に保

持されており、
前記送信装置は、
前記認証鍵を得るための媒介径数情報を前記鍵関数に代入し、認証鍵を生成する認証鍵生成部と、
生成した認証鍵を用いて前記メッセージに対する前記認証子を生成する認証子生成部と、
生成した認証子と、該認証子を生成するための前記認証鍵に対する前記媒介径数情報と、前記メッセージとを前記受信装置に送信する送信部とを備えており、
前記受信装置は、
前記送信装置からの前記メッセージ、前記認証子および前記媒介径数情報を受信する受信部と、
前記媒介径数情報を認証する媒介径数情報認証部と、
認証された媒介径数情報を、保持している前記鍵関数に代入し、認証用認証鍵を生成する認証鍵取得部と、
生成した前記認証用認証鍵および受信した前記メッセージに基づいて認証用認証子を生成する認証用認証子生成部と、
生成した認証用認証子を用いて前記メッセージの認証を行う照合認証部とを備え、
前記メッセージは各パケットから成り、
前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、
前記送信装置は、
予め任意に指定した媒介径数情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にある媒介径数情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成する媒介径数情報チェーン生成部と、
生成した媒介径数情報チェーンにおいて、媒介径数情報I_0を、予め前記受信装置に送付し、該受信装置で保持させる媒介径数情報チェーン送信部とを備えており、
前記受信装置は、
前記メッセージおよび前記認証子と共に受信する前記媒介径数情報I_iを受信すると、前記一方向性関数ｆを用いてｆ（I_i）を求め、該ｆ（I_i）と、保持している媒介径数情報I_{i-1}との比較照合を行なって前記媒介径数情報I_iの認証を行う比較判定部と、
前記媒介径数情報I_iを認証すると、保持している前記媒介径数情報I_{i-1}に代えて、認証された前記媒介径数情報I_iを保持する媒介径数情報保持部とを備えることを特徴とするメッセージ認証システム。

【請求項５】
送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うメッセージ認証装置において、
前記認証鍵にインデックス情報を対応付けた認証鍵テーブルが前記送信装置および前記受信装置間で秘密裡に保持されており、
前記送信装置において、
前記メッセージに対する前記認証子が生成され、
生成された前記認証子、該認証子を生成するための前記認証鍵に対する前記インデックス情報および前記メッセージが前記受信装置に送信されており、
前記送信装置からの前記メッセージ、前記認証子および前記インデックス情報を受信する受信部と、
前記インデックス情報を認証するインデックス情報認証部と、
認証されたインデックス情報に基づいて保持している前記認証鍵テーブルを検索し、当該インデックス情報に対応する前記認証鍵を取得する認証鍵取得部と、
取得した前記認証鍵および受信した前記メッセージに基づいて認証用認証子を生成する

認証用認証子生成部と、
生成した認証用認証子を用いて前記メッセージの認証を行う照合認証部とを備え、
前記メッセージは各パケットから成り、
前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、
前記送信装置では、
予め任意に指定したインデックス情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にあるインデックス情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成し、
生成したインデックス情報チェーンにおいて、インデックス情報I_0を、予め前記受信装置に送付し、該受信装置で保持させ、
前記インデックス情報認証部は、
前記メッセージおよび前記認証子と共に受信する前記インデックス情報I_iを受信すると、前記一方向性関数ｆを用いてｆ（I_i）を求め、該ｆ（I_i）と、保持しているインデックス情報I_{i-1}との比較照合を行なって前記インデックス情報I_iの認証を行う比較判定部と、
前記インデックス情報I_iを認証すると、保持している前記インデックス情報I_{i-1}に代えて、認証された前記インデックス情報I_iを保持するインデックス情報保持部と、
を備えることを特徴とするメッセージ認証装置。

【請求項６】
送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うメッセージ認証装置において、
前記認証鍵を生成するための鍵関数が前記送信装置および前記受信装置間で秘密裡に保持されており、
前記送信装置において、
前記認証鍵を得るための媒介径数情報が前記鍵関数に代入されて認証鍵が生成され、
生成された認証鍵を用いて前記メッセージに対する前記認証子が生成され、
生成された認証子と、該認証子を生成するための前記認証鍵に対する前記媒介径数情報と、前記メッセージとが前記受信装置に送信されており、
前記送信装置からの前記メッセージ、前記認証子および前記媒介径数情報を受信する受信部と、
前記媒介径数情報を認証する媒介径数情報認証部と、
認証された媒介径数情報を、保持している前記鍵関数に代入し、認証用認証鍵を生成する認証鍵取得部と、
生成した前記認証用認証鍵および受信した前記メッセージに基づいて認証用認証子を生成する認証用認証子生成部と、
生成した認証用認証子を用いて前記メッセージの認証を行う照合認証部とを備え、
前記メッセージは各パケットから成り、
前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、
前記送信装置では、
予め任意に指定した媒介径数情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にある媒介径数情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成し、
生成した媒介径数情報チェーンにおいて、媒介径数情報I_0を、予め前記受信装置に送付し、該受信装置で保持させ、
前記媒介径数情報認証部は、
前記メッセージおよび前記認証子と共に受信する前記媒介径数情報I_iを受信すると、前記一方向性関数ｆを用いてｆ（I_i）を求め、該ｆ（I_i）と、保持している媒介径数

情報I_{i-1}との比較照合を行なって前記媒介径数情報I_iの認証を行う比較判定部と、
前記媒介径数情報I_iを認証すると、保持している前記媒介径数情報I_{i-1}に代えて、認証された前記媒介径数情報I_iを保持する媒介径数情報保持部とを備えることを特徴とするメッセージ認証装置。

【請求項７】

送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うためのメッセージ認証送信装置において、
前記認証鍵にインデックス情報を対応付けた認証鍵テーブルが前記送信装置および前記受信装置間で秘密裡に保持されており、
前記メッセージに対する前記認証子を生成する認証子生成部と、
生成した前記認証子、該認証子を生成するための前記認証鍵に対する前記インデックス情報および前記メッセージを前記受信装置に送信する送信部とを備え、
前記メッセージは各パケットから成り、
前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、
予め任意に指定したインデックス情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にあるインデックス情報チェーン（I_0（＝ｆ（I_1））、・・・、I_n）を生成するインデックスチェーン情報生成部と、
生成したインデックス情報チェーンにおいて、インデックス情報I_0を、予め前記受信装置に送付し、該受信装置で保持させるインデックス情報チェーン送信部とを備えることを特徴とするメッセージ認証送信装置。

【請求項８】

送信装置から受信装置に送られたメッセージを認証すべく、前記送信装置において認証鍵を用いて前記メッセージに対する認証子を生成し、生成した認証子およびメッセージを前記受信装置に送信した後、前記受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うメッセージ認証送信装置において、
前記認証鍵を生成するための鍵関数が前記送信装置および前記受信装置間で秘密裡に保持されており、
前記認証鍵を得るための媒介径数情報が前記鍵関数に代入し、認証鍵を生成する認証鍵生成部と、
生成した認証鍵を用いて前記メッセージに対する前記認証子を生成する認証子生成部と、
生成した認証子と、該認証子を生成するための前記認証鍵に対する前記媒介径数情報と、前記メッセージとを前記受信装置に送信する送信部とを備え、
前記メッセージは各パケットから成り、
前記受信装置で前記送信装置から順次送信される前記各パケットを順次認証すべく、
予め任意に指定した媒介径数情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にある媒介径数情報チェーン（I_0（＝ｆ（I_1））、・・・、I_n）を生成する媒介径数情報チェーン生成部と、
生成した媒介径数情報チェーンにおいて、媒介径数情報I_0を、予め前記受信装置に送付し、該受信装置で保持させ媒介径数情報チェーン送信部とを備えることを特徴とするメッセージ認証送信装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はメッセージの認証方法であって、特にパケット化されたメッセージの認証方法

と、該認証方法を用いた認証装置および認証システムに関するものである。

【背景技術】

【０００２】

送信元から受信先に送られるパケット化されたメッセージを認証する方法がμＴＥＳＬＡとして非特許文献１に開示されている。

【０００３】

非特許文献１に開示されているμＴＥＳＬＡを図を用いて説明する。μＴＥＳＬＡを説明するための概念図が図７に示されている。図７には、パケットの認証に必要な情報を生成して送信する送信元が図中上段に、送信元からのパケットを受信して認証を行う受信先が図中下段に示されており、処理順序の番号が丸囲い文字で示されている。

【０００４】

送信元において、先ず乱数などから任意の値をK_nとして指定し、それをパラメータとして一方向性関数ｆ（ｘ）に入力する。ところで一方向性関数は、要約関数又はメッセージダイジェスト（圧縮）関数と称される関数であり、具体的にはＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ５）やＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）などである。このような一方向性関数を用いて、式１に示す演算を行う。

$$K_{n-1} = f(K_n) \qquad \text{（式１）}$$

【０００５】

式１による演算結果をパラメータとして一方向性関数ｆに逐次入力する。すなわち、式１による演算結果を入力パラメータとして、式１に入力することを繰返す。これにより、一方向鍵チェーンと称される数値列、K_0（＝ｆ（K_1））、K_2（＝ｆ（K_3））、・・・K_nが生成される（図７の１）。

送信元で生成した一方向鍵チェーンにおいて認証鍵K_0は、予め秘密裡に受信先に送られ、該受信先で保持管理される（図７の２）。

【０００６】

ところで、各認証鍵は各パケットに対応付けられており、例えばパケットP_nに対し認証鍵K_n＝（ｆ（K_n））が対応付けられている。尚、パケットP_nおよび認証鍵K_nの関係は、所定の送信間隔に基づいている。

【０００７】

すなわち、各パケットは所定の時間間隔で送信元から受信先に送信されており、各送信間隔には、各パケットに対応する各認証鍵が対応付けられている。つまり、図７において、例えば期間１には認証鍵K_1が対応しており、期間２には認証鍵K_2が対応しており、期間３には認証鍵K_3が対応している。

【０００８】

このように割当てられた認証鍵を用いてパケットを認証するための認証子が生成される。認証子の生成は、例えばＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）関数を用いて生成されており、具体的には、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）暗号などの共通鍵ブロック暗号を用いたＣＢＣ－ＭＡＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ－ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）などが認証子の生成に用いられている。

【０００９】

尚、認証子をＭＡＣ（・）と称して以降の説明を行う。例えば認証鍵K_1を用いたパケットP_1に対する認証子をＭＡＣ（K_1・P_1）と称し、以降の説明を行う。

【００１０】

このように送信元で生成された認証子ＭＡＣ（K_n・P_n）およびパケットP_nは、送信元から受信先に送信される。

受信先は、送信元からの認証子ＭＡＣ（K_n・P_n）およびパケットP_nを、ある時間の遅延ｄをもって受信する。この遅延ｄは、通信トラフィックの輻輳状況や、通信設備などの通信環境などによって異なる。

【００１１】

その後受信先は、認証に必要な認証鍵が公開されるまで、受信した認証子およびパケットを保持し続ける。受信先は、公開された認証鍵を取得すると、当該認証鍵の検証を行う。認証鍵の検証は、例えば取得した認証鍵が認証鍵K_iであるとき、該認証鍵K_iを一方向性関数ｆに入力し、その演算結果を用いて、式２に示すように、以前に公開されて保持管理している認証鍵K_{i-1}と一致するか、又は秘密裡に受信して保持管理している認証鍵K_0と一致するか否かを判定する。

$$K_{i-1}=f(K_i) \qquad (式２)$$

【００１２】

前記した検証により、認証鍵が認証されると、受信時から保持し続けているパケットの認証子の認証を行う。すなわち、受信したパケットおよび認証鍵とＭＡＣ関数とを用いて認証用の認証子を生成し、生成した認証用認証子と受信して保持している認証子との比較判定を行う。

【００１３】

前記した比較判定により生成した認証用認証子と、先に受信して保持している認証子とが一致すると、受信先で受信したパケットは、送信元から送信されたパケットであると認証される。

【非特許文献１】“ＳＰＩＮＳ：Ｓｅｃｕｒｉｔｙ Ｐｒｏｔｏｃｏｌｓ ｆｏｒ Ｓｅｎｓｏｒ Ｎｅｔｗｏｒｋｓ”, Ａｄｒｉａｎ Ｐｅｒｒｉｇ, Ｒｏｂｅｒｔ Ｓｚｅｗｃｚｙｋ, Ｖｉｃｔｏｒ Ｗｅｎ, Ｄａｖｉｔ Ｃｕｌｌｅｒ Ｊ．Ｄ．Ｔｙｇａｒ, Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ Ｓｅｖｅｎｔｈ Ａｎｎｕａｌ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｍｏｂｉｌｅ Ｃｏｍｐｕｔｉｎｇ ａｎｄ Ｎｅｔｗｏｒｋｓ ＭＯＢＩＣＯＭ ２００１, ｊｕｌｙ ２００１.

【発明の開示】

【発明が解決しようとする課題】

【００１４】

ところで、前記した従来のメッセージ認証方法では、パケットおよび認証子が送信されて、受信先でパケットおよび認証子が受信された後に認証鍵を公開（送信）しないと、パケットおよび認証子を取得し、更に認証鍵を取得した第三者によって、パケットの改竄やなりすまし転送が行われる虞がある。従って、これを回避するには、認証鍵をパケットおよび認証子の送信から十分な時間遅延を有して認証鍵を公開しなければならず、このため受信先で認証鍵を取得してメッセージを認証するまでに時間遅延が生じ、これがが問題となっていた。

【００１５】

従って、前記した課題に鑑みて、本発明の目的はメッセージ認証のための時間遅延を必要としないメッセージの認証を行う方法を提供することにある。

更に、本発明の他の目的は、メッセージ認証のための時間遅延を必要としないメッセージの認証方法を用いた認証装置および認証システムを提供することにある。

【課題を解決するための手段】

【００１６】

本発明は、以上の点を解決するために、次の構成を採用する。

〈構成１〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行う認証方法において、認証鍵にインデックス情報を対応付けた認証鍵テーブルが送信装置および受信装置間で秘密裡に保持されており、送信装置において、メッセージに対する認証子を生成すること、生成した認証子、該認証子を生成するための認証鍵に対するインデックス情報およびメッセージを受信装置に送信すること、受信装置において、送信装置からのメッセージ、認証子およびインデックス情報を受信すること、インデックス情報を認証す

ること、認証したインデックス情報に基づいて保持している認証鍵テーブルを検索し、当該インデックス情報に対応する認証鍵を取得すること、取得した認証鍵および受信したメッセージに基づいて認証用認証子を生成すること、生成された認証用認証子を用いてメッセージの認証を行うこと、を特徴とする。

【００１７】

メッセージは各パケットから成り、受信装置で前記送信装置から順次送信される各パケットを順次認証すべく、送信装置は、予め任意に指定したインデックス情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にあるインデックス情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成すること、生成したインデックス情報チェーンにおいて、インデックス情報I_0を、予め受信装置に送付し、該受信装置で保持させること、受信装置は、メッセージおよび認証子と共に受信するインデックス情報I_iを受信すると、一方向性関数ｆを用いてｆ（I_i）を求め、該ｆ（I_i）と、保持しているインデックス情報I_{i-1}との比較照合を行なってインデックス情報I_iの認証を行うこと、インデックス情報I_iを認証すると、保持しているインデックス情報I_{i-1}に代えて、認証された前記インデックス情報I_iを保持することを特徴とする。

【００１８】

〈構成２〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行ってメッセージの認証を行うメッセージ認証方法において、認証鍵を生成するための鍵関数が送信装置および受信装置間で秘密裡に保持されており、送信装置において、認証鍵を得るための媒介径数情報を前記鍵関数に代入し、認証鍵を生成すること、生成した認証鍵を用いてメッセージに対する認証子を生成すること、生成した認証子と、該認証子を生成するための認証鍵に対する媒介径数情報と、メッセージとを受信装置に送信すること、受信装置において、送信装置からのメッセージ、認証子および媒介径数情報を受信すること、媒介径数情報を認証すること、認証された媒介径数情報を、保持している鍵関数に代入し、認証用認証鍵を生成すること、生成した認証用認証鍵および受信したメッセージに基づいて認証用認証子を生成すること、生成した認証用認証子を用いてメッセージの認証を行うこと、を特徴とする。

【００１９】

メッセージは各パケットから成り、受信装置で前記送信装置から順次送信される各パケットを順次認証すべく、送信装置は、予め任意に指定した媒介径数情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｉはパケットの総数、$n \geqq i \geqq 1$）と示す関係にある媒介径数情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成すること、生成した媒介径数情報チェーンにおいて、媒介径数情報I_0を、予め受信装置に送付し、該受信装置で保持させること、受信装置は、メッセージおよび認証子と共に受信する媒介径数情報I_iを受信すると、一方向性関数ｆを用いてｆ（I_i）を求め、該ｆ（I_i）と、保持している媒介径数情報I_{i-1}との比較照合を行なって媒介径数情報I_iの認証を行うこと、媒介径数情報I_nを認証すると、保持している媒介径数情報I_{i-1}に代えて、認証された媒介径数情報I_iを保持することを特徴とする。

【００２０】

〈構成３〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うメッセージ認証システムにおいて、認証鍵にインデックス情報を対応付けた認証鍵テーブルが送信装置および受信装置間で秘密裡に保持されており、送信装置は、メッセージに対す

る認証子を生成する認証子生成部と、生成した認証子、該認証子を生成するための認証鍵に対するインデックス情報およびメッセージを受信装置に送信する送信部とを備えており、受信装置は、送信装置からの前記メッセージ、認証子およびインデックス情報を受信する受信部と、インデックス情報を認証するインデックス情報認証部と、認証されたインデックス情報に基づいて保持している認証鍵テーブルを検索し、当該インデックス情報に対応する認証鍵を取得する認証鍵取得部と、取得した認証鍵および受信したメッセージに基づいて認証用認証子を生成する認証用認証子生成部と、生成した認証用認証子を用いてメッセージの認証を行う照合認証部とを備えることを特徴とするメッセージ認証システム。

【００２１】

メッセージは各パケットから成り、受信装置で前記送信装置から順次送信される各パケットを順次認証すべく、送信装置は、予め任意に指定したインデックス情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にあるインデックス情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成するインデックス情報チェーン生成部と、生成したインデックス情報チェーンにおいて、インデックス情報I_0を、予め前記受信装置に送付し、該受信装置で保持させるインデックス情報チェーン送信部とを備えており、インデックス情報認証部は、メッセージおよび認証子と共に受信するインデックス情報I_iを受信すると、一方向性関数ｆを用いて$f(I_i)$を求め、該$f(I_i)$と、保持しているインデックス情報I_{i-1}との比較照合を行なってインデックス情報I_iの認証を行う比較判定部と、インデックス情報I_iを認証すると、保持しているインデックス情報I_{i-1}に代えて、認証されたインデックス情報I_iを保持するインデックス情報保持部と、を備えることを特徴とする。

【００２２】

〈構成４〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行ってメッセージの認証を行うメッセージ認証システムにおいて、認証鍵を生成するための鍵関数が送信装置および受信装置間で秘密裡に保持されており、送信装置は、認証鍵を得るための媒介径数情報を鍵関数に代入し、認証鍵を生成する認証鍵生成部と、生成した認証鍵を用いてメッセージに対する認証子を生成する認証子生成部と、生成した認証子と、該認証子を生成するための認証鍵に対する媒介径数情報と、メッセージとを受信装置に送信する送信部とを備えており、受信装置は、送信装置からのメッセージ、認証子および媒介径数情報を受信する受信部と、媒介径数情報を認証する媒介径数情報認証部と、認証された媒介径数情報を、保持している鍵関数に代入し、認証用認証鍵を生成する認証鍵取得部と、生成した認証用認証鍵および受信したメッセージに基づいて認証用認証子を生成する認証用認証子生成部と、生成した認証用認証子を用いてメッセージの認証を行う照合認証部とを備えることを特徴とする。

【００２３】

メッセージは各パケットから成り、受信装置で前記送信装置から順次送信される各パケットを順次認証すべく、送信装置は、予め任意に指定した媒介径数情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にある媒介径数情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成する媒介径数情報チェーン生成部と、生成した媒介径数情報チェーンにおいて、媒介径数情報I_0を、予め受信装置に送付し、該受信装置で保持させる媒介径数情報チェーン送信部とを備えており、受信装置は、メッセージおよび認証子と共に受信する媒介径数情報I_iを受信すると、一方向性関数ｆを用いて$f(I_i)$を求め、該$f(I_i)$と、保持している媒介径数情報I_{i-1}との比較照合を行なって媒介径数情報I_iの認証を行う比較判定部と、媒介径数情報I_iを認証すると、保持している媒介径数情報I_{i-1}に代えて、認証された媒介径数情報I_iを保持する媒介径数情報保持部とを備えることを特徴とする。

【００２４】

〈構成５〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行ってメッセージの認証を行うメッセージ認証装置において、認証鍵にインデックス情報を対応付けた認証鍵テーブルが送信装置および受信装置間で秘密裡に保持されており、送信装置において、メッセージに対する認証子が生成され、生成された認証子、該認証子を生成するための認証鍵に対するインデックス情報およびメッセージが受信装置に送信されており、送信装置からのメッセージ、認証子およびインデックス情報を受信する受信部と、インデックス情報を認証するインデックス情報認証部と、認証されたインデックス情報に基づいて保持している認証鍵テーブルを検索し、当該インデックス情報に対応する認証鍵を取得する認証鍵取得部と、取得した前記認証鍵および受信したメッセージに基づいて認証用認証子を生成する認証用認証子生成部と、生成した認証用認証子を用いてメッセージの認証を行う照合認証部とを備えることを特徴とする。

【００２５】

メッセージは各パケットから成り、受信装置で前記送信装置から順次送信される各パケットを順次認証すべく、送信装置では、予め任意に指定したインデックス情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にあるインデックス情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成し、生成したインデックス情報チェーンにおいて、インデックス情報I_0を、予め受信装置に送付し、該受信装置で保持させ、インデックス情報認証部は、メッセージおよび認証子と共に受信するインデックス情報I_iを受信すると、一方向性関数ｆを用いてｆ（I_i）を求め、該ｆ（I_i）と、保持しているインデックス情報I_{i-1}との比較照合を行なってインデックス情報I_iの認証を行う比較判定部と、インデックス情報I_iを認証すると、保持しているインデックス情報I_{i-1}に代えて、認証されたインデックス情報I_iを保持するインデックス情報保持部と、を備えることを特徴とする。

【００２６】

〈構成６〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行ってメッセージの認証を行うメッセージ認証装置において、認証鍵を生成するための鍵関数が送信装置および受信装置間で秘密裡に保持されており、送信装置において、認証鍵を得るための媒介径数情報が鍵関数に代入されて認証鍵が生成され、生成された認証鍵を用いてメッセージに対する認証子が生成され、生成された認証子と、該認証子を生成するための認証鍵に対する媒介径数情報と、メッセージとが受信装置に送信されており、送信装置からのメッセージ、認証子および媒介径数情報を受信する受信部と、媒介径数情報を認証する媒介径数情報認証部と、認証された媒介径数情報を、保持している鍵関数に代入し、認証用認証鍵を生成する認証鍵取得部と、生成した認証用認証鍵および受信したメッセージに基づいて認証用認証子を生成する認証用認証子生成部と、生成した認証用認証子を用いてメッセージの認証を行う照合認証部とを備えることを特徴とする。

【００２７】

メッセージは各パケットから成り、受信装置で送信装置から順次送信される各パケットを順次認証すべく、送信装置では、予め任意に指定した媒介径数情報I_nに対し一方向性関数ｆを用いて$I_{i-1}=f(I_i)$（但し、ｎはパケットの総数、$n \geqq i \geqq 1$）と示す関係にある媒介径数情報チェーン（I_0（$=f(I_1)$）、・・・、I_n）を生成し、生成した媒介径数情報チェーンにおいて、媒介径数情報I_0を、予め受信装置に送付し、該受信装置で保持させ、媒介径数情報認証部は、メッセージおよび認証子と共に受信する媒

介径数情報Ｉ$_{i}$を受信すると、一方向性関数ｆを用いてｆ（Ｉ$_{i}$）を求め、該ｆ（Ｉ$_{i}$）と、保持している媒介径数情報Ｉ$_{i-1}$との比較照合を行なって媒介径数情報Ｉ$_{i}$の認証を行う比較判定部と、媒介径数情報Ｉ$_{i}$を認証すると、保持している媒介径数情報Ｉ$_{i-1}$に代えて、認証された媒介径数情報Ｉ$_{i}$を保持する媒介径数情報保持部とを備えることを特徴とする。

【００２８】

〈構成７〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行って前記メッセージの認証を行うためのメッセージ認証送信装置において、認証鍵にインデックス情報を対応付けた認証鍵テーブルが送信装置および受信装置間で秘密裡に保持されており、メッセージに対する認証子を生成する認証子生成部と、生成した前記認証子、該認証子を生成するための認証鍵に対するインデックス情報およびメッセージを受信装置に送信する送信部とを備えることを特徴とする。

【００２９】

メッセージは各パケットから成り、受信装置で前記送信装置から順次送信される各パケットを順次認証すべく、予め任意に指定したインデックス情報Ｉ$_{n}$に対し一方向性関数ｆを用いてＩ$_{i-1}$＝ｆ（Ｉ$_{i}$）（但し、ｎはパケットの総数、ｎ≧ｉ≧１）と示す関係にあるインデックス情報チェーン（Ｉ$_{0}$（＝ｆ（Ｉ$_{1}$））、・・・、Ｉ$_{n}$）を生成するインデックスチェーン情報生成部と、生成したインデックス情報チェーンにおいて、インデックス情報Ｉ$_{0}$を、予め受信装置に送付し、該受信装置で保持させるインデックス情報チェーン送信部とを備えることを特徴とする。

【００３０】

〈構成８〉

送信装置から受信装置に送られたメッセージを認証すべく、送信装置において認証鍵を用いてメッセージに対する認証子を生成し、生成した認証子およびメッセージを受信装置に送信した後、受信装置において受信したメッセージに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子との比較照合を行ってメッセージの認証を行うメッセージ認証送信装置において、認証鍵を生成するための鍵関数が送信装置および受信装置間で秘密裡に保持されており、認証鍵を得るための媒介径数情報が鍵関数に代入し、認証鍵を生成する認証鍵生成部と、生成した認証鍵を用いてメッセージに対する認証子を生成する認証子生成部と、生成した認証子と、該認証子を生成するための認証鍵に対する媒介径数情報と、メッセージとを受信装置に送信する送信部とを備えることを特徴とする。

【００３１】

メッセージは各パケットから成り、受信装置で送信装置から順次送信される各パケットを順次認証すべく、予め任意に指定した媒介径数情報Ｉ$_{n}$に対し一方向性関数ｆを用いてＩ$_{i-1}$＝ｆ（Ｉ$_{i}$）（但し、ｎはパケットの総数、ｎ≧ｉ≧１）と示す関係にある媒介径数情報チェーン（Ｉ$_{0}$（＝ｆ（Ｉ$_{1}$））、・・・、Ｉ$_{n}$）を生成する媒介径数情報チェーン生成部と、生成した媒介径数情報チェーンにおいて、媒介径数情報Ｉ$_{0}$を、予め受信装置に送付し、該受信装置で保持させ媒介径数情報チェーン送信部とを備えることを特徴とする。

【発明の効果】

【００３２】

本発明によれば、メッセージを認証するための認証子の生成に用いる認証鍵がインデックス情報に対応付けらえている認証鍵テーブルを送信元および受信先との間で秘密裡に保持し、認証鍵を得るためのインデックス情報を、メッセージおよび認証子と共に送信元から受信先へ送信し、受信先で認証鍵テーブルを参照してインデックス情報に対応する認証鍵を取得する。従って、本発明によれば、認証鍵を送信元から受信先へ直接的に送付しな

くとも、受信先でインデックス情報に基づいてメッセージの認証に必要な認証鍵を取得することができ、認証鍵を取得するための時間遅延を必要とせず、即座に受信したメッセージの認証を行うことができる。

【００３３】

更に、本発明によれば、メッセージを認証するための認証子の生成に用いる認証鍵（認証用認証鍵）を生成するための鍵関数を、送信元および受信先との間で秘密裡に保持し、認証鍵を得るための媒介径数情報を、メッセージおよび認証子と共に送信元から受信先へ送信し、受信先で媒介径数情報を保持する鍵関数に代入して認証用認証鍵を生成する。従って、本発明によれば、認証鍵を送信元から受信先へ直接的に送付しなくとも、受信先で媒介径数情報を鍵関数に代入してメッセージの認証に必要な認証用認証鍵を取得することができ、該認証用認証鍵を取得するための時間遅延を必要とせず、即座に受信したメッセージの認証を行うことができる。

【発明を実施するための最良の形態】

【００３４】

以下、本発明の実施形態について、図を用いて詳細に説明する。以下の説明では、各実施の形態に用いる図面について同一の構成要素は同一の符号を付し、かつ重複する説明は可能な限り省略する。

【実施例１】

【００３５】

本発明のメッセージ認証システム１０は、図２に示すように、メッセージを送信する送信装置（送信元）２０と、該送信装置からのメッセージを受信して、当該メッセージが前記送信装置２０からのメッセージであるか否か認証判定を行う認証装置としての複数の受信装置（受信先）３０とを備える。

【００３６】

ところで送信装置２０からのメッセージの配信方法としては、複数の受信装置３０から特定の１つの受信装置３０を指定し、指定した受信装置３０に対しメッセージを配信するユニキャストや、所定のグループに属する受信装置３０に対しメッセージを配信するマルチキャストや、全ての受信装置３０に対しメッセージを配信するブロードキャストなどの方法があるが、本実施例では、特にブロードキャストを例に以降の説明を行う。また本実施例では、メッセージとして複数のパケットP_i（但し、$n \geqq i \geqq 1$、ｎはパケットの総数）の認証を行う例で説明する。

【００３７】

本発明のメッセージの認証方法の概念を図１を用いて説明するが、図１の概念図において、送信装置２０での処理内容が上段に示されており、受信装置３０での処理内容が下段に示されており、処理順序の番号が丸囲い文字で示されている。

【００３８】

ここで、先ずパケット認証の処理内容の大まかな概要を説明した後、本発明のメッセージ認証方法の概念を図１を用いて説明する。

送信装置２０から受信装置３０に送られたパケットが、送信装置２０から送信されたパケットであると認証するには、先ず送信装置２０において、パケットと、該パケットに対応する認証鍵とに基づいて認証子を生成する。

【００３９】

認証鍵は、パケット毎に対応付けられており、各パケットP_iに各認証鍵K_iが対応づけられている。ところで認証鍵の総数はパケットの総数より少なくてもよく、例えばパケットの総数が１００であり、認証鍵の総数が５である場合、５個の認証鍵の何れかが各パケットにそれぞれ対応付けられる。

【００４０】

尚、以降の説明において、認証鍵の総数がＮ個であるとき、各認証鍵をＫ[０]、Ｋ[１]・・・Ｋ[Ｎ－２]、Ｋ[Ｎ－１]と表記する。

【００４１】

認証子は、各パケット毎に生成され、例えば公知のＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）関数を用いて生成される。具体的には、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）暗号などの共通鍵ブロック暗号を用いたＣＢＣ－ＭＡＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ－ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）などを用いて認証子が送信装置２０で生成される。

例えば、認証鍵K_iおよびパケットP_nをパラメータとしてＣＢＣ－ＭＡＣを用いて認証子を生成すると、認証子ＭＡＣ（K_i・P_i）と示される認証子が生成される。

【００４２】

生成した認証子ＭＡＣ（K_i・P_i）およびパケットP_iは送信装置２０から受信装置３０に送信される。これらを受信した受信装置２０は、送信装置３０との間で秘密裡に保持している認証鍵と、受信パケットとに基づいて認証用の認証子を生成し、該認証用認証子と受信した認証子とを比較照合する。この比較照合において、認証用認証子および受信した認証子が一致すると、受信装置３０は、受信したパケットは送信装置２０から送られてきたと認証する。

【００４３】

ところで、本発明は前述のＮ個の認証鍵Ｋ（認証鍵Ｋ[０]、・・・、Ｋ[Ｎ－１]）に、該各認証鍵を得るためのインデックス情報Ｉ（０≦Ｉ≦Ｎ－１）を対応付けてテーブル管理することを特徴としており、認証鍵Ｋとインデックス情報Ｉとを対応付けた認証鍵テーブルＫ[Ｉ]を生成する。

【００４４】

ところで本発明のメッセージ認証方法では、認証鍵テーブルＫ[Ｉ]（認証鍵Ｋ[０]・・・Ｋ[Ｎ－１]）を送信装置２０および受信装置３０間で秘密裡に保持管理する。

従って、送信装置２０から受信装置３０に認証鍵を直接送信しなくても、インデックス情報を送信装置２０から受信装置３０に送信すれば、該受信装置３０で受信したインデックス情報に基づいて認証鍵テーブルを検索し、インデックス情報に対応する認証鍵を取得することができる。これにより、受信装置３０で取得した認証鍵を用いてパケットの認証を行うことができる。

【００４５】

前記したパケットの認証方法の概念を図１を用いて説明する。

先ず、送信装置２０および受信装置３０間で秘密裡に認証鍵テーブルＫ[Ｉ]（Ｋ[０]・・・Ｋ[Ｎ－１]）が保持される（図１の１）。

【００４６】

次に、送信装置２０は、乱数などにおいて任意に選定した数値をインデックス情報I_nとし、該インデックス情報I_nに対し、後述する一方向性関数を用いて各認証鍵に対応した一連のインデックス情報をインデックス情報チェーンとして生成する（図１の２）。

【００４７】

このとき、インデックス情報チェーンにおける各インデックス情報は、認証鍵テーブルにおける何れかの認証鍵に対応している。すなわち、各インデックス情報は、認証鍵テーブルにおける認証鍵Ｋ[０]、・・・、Ｋ[Ｎ－１]の何れかを示している。

【００４８】

ところで、一方向性関数は要約関数又はメッセージダイジェスト（圧縮）関数と称される関数であり、具体的にはＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ５）やＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）などである。このような一方向性関数を用いて、式３に示す演算を行う。

$$I_{n-1}=f(I_n) \qquad \text{（式３）}$$

【００４９】

式３による演算結果をパラメータとして一方向性関数ｆに逐次入力する。すなわち、式３による演算結果を入力パラメータとして、再度式３に入力することを繰返す。これにより、数値列I_n、・・・、I_1（＝ｆ（I_2））、I_0（＝ｆ（I_1））がインデックス

情報チェーンとして生成される。
送信装置２０で生成したインデックス情報チェーンI_n・・・I_0において、インデックス情報I_0は、予め秘密裡に受信装置３０に送られ、該受信装置３０で保持管理される（図１の３）。
【００５０】
その後、送信装置２０は、送信すべきパケットP_iと、該パケットP_iに対応するインデックス情報I_iに基づいて特定される認証鍵K[I_i]とに基づいて認証子ＭＡＣ（K[I_n]・P_i）を生成する。認証子は、各パケット毎に生成されており、認証子を生成した送信装置は、パケットP_iと認証子ＭＡＣ（K[I_i]・P_i）とインデックス情報I_iとから成る１組の情報をパケット毎に受信装置に送信する。
【００５１】
送信装置２０からの情報を受信した受信装置３０は、先ずインデックス情報I_iの認証を行う。
インデックス情報の認証は、例えば受信したインデックス情報がインデックス情報I_iであるとき、該インデックス情報I_iを一方向性関数ｆに入力した結果が、式４に示すように、以前に公開されて保持管理しているインデックス情報I_{i-1}と一致するか、又は秘密裡に受信して保持管理しているインデックス情報I_0と一致するか否か照合判定することにより行われる。

$$I_{i-1}=f(I_i) \qquad \text{（式４）}$$

【００５２】
具体的には、送信装置２０からのインデックス情報がI_1である場合、該I_1を式３に示す式を用いて演算を行い、得た結果が、式４に示すように、秘密裡に保持管理しているI_0と同じであるか否か照合判定を行い、一致するとインデックス情報I_1が認証される。
【００５３】
次に、認証したインデックス情報I_iに基づいて認証鍵テーブル（K[０]・・・・K[Ｎ－１]）を検索し、インデックス情報I_iに対応する認証鍵K[I_i]を取得する。具体的には、インデックス情報がI_1である場合、認証鍵テーブルから認証鍵K[I_1]を取得する。尚、認証鍵K[I_1]は、認証鍵K[０]・・・・K[Ｎ－１]の何れかである。
【００５４】
受信装置３０は、取得した認証鍵K[I_i]と、受信したパケットP_iとに基づいて認証用の認証子ＭＡＣ（K[I_i]・P_i）を生成する。
その後、受信装置３０は、認証用認証子ＭＡＣ（K[I_i]・P_i）と、受信した認証子ＭＡＣ（K[I_i]・P_i）との比較照合を行なう。この照合で、認証用認証子ＭＡＣ（K[I_i]・P_i）および受信した認証子ＭＡＣ（K[I_i]・P_i）が一致すると、認証子と共に受信したパケットP_iは送信装置２０から送信されたパケットであると認証される（図１の４）。
【００５５】
ここで、本発明のメッセージ認証方法を用いた送信装置２０と、該送信装置２０からのメッセージを受信して認証する受信装置３０とを図を用いて詳細に説明する。
送信装置２０は、図３に示すように、パケットを生成するパケット生成部２１と、インデックス情報を生成して管理するインデックス情報生成部２２と、パケットの認証に用いる認証鍵にインデックス情報を対応付けた認証鍵テーブルを保持する認証鍵テーブル保持部２３と、該認証鍵テーブルおよびインデックス情報とに基づいてパケットに対する認証子を生成する認証子生成部２４と、生成した認証子および認証情報、パケット、インデックス情報を受信装置３０に対し送信する送信部２５とを備える。
【００５６】
パケット生成部２１は、パケットを順次生成する。
インデックス情報生成部２２は、インデックス情報チェーン生成部２２１と、該インデックス情報チェーン生成部で生成されるインデックス情報チェーンを保持するインデック

ス情報チェーン保持部２２２とを備えている。

【００５７】

インデックス情報チェーン生成部２２１は、乱数やランダムな文字列などから任意の数値列（文字列）をインデックス情報I_nとして選定し、該インデックス情報を式３に示す一方向性関数に代入し、求めた値を更に式３に代入することを繰返し、次に示すI_n、・・・I_1（＝ｆ（I_2））、I_0（＝ｆ（I_1））成る数値列をインデックス情報チェーンとして生成する。インデックス情報チェーン生成部２２１で生成されたインデックス情報チェーンは、インデックス情報チェーン保持部２２２で保持される。

【００５８】

ところで、Ｎ個の認証鍵Ｋは、インデックス情報Ｉ（０≦Ｉ≦Ｎ－１）に対応付けられたテーブル形式で管理されており、各認証鍵Ｋに各インデックス情報Ｉが対応付けられた認証鍵テーブルK[I_i]（K[０]・・・K[Ｎ－１]）が図示しない認証鍵テーブル生成部で生成され、生成された認証鍵テーブルが認証鍵テーブル保持部２３で保持される。

【００５９】

認証子生成部２４は、パケットと該パケットに対応する認証鍵とに基づいて認証子を生成する。認証子生成部２４は、ＡＥＳ暗号などの共通鍵ブロック暗号を用いたＣＢＣ－ＭＡＣなどを用いて認証子を生成する。

例えば、認証鍵K[I_1]およびパケットP_1をパラメータとしてＣＢＣ－ＭＡＣを用いて認証子を生成すると、認証子ＭＡＣ（K[I_1]・P_1）と示される認証子が生成される。

【００６０】

送信部２５は、認証子生成部２４で生成した認証子ＭＡＣ（K[I_i]・P_i）と、パケットP_iと、インデックス情報I_iと、受信装置３０に送信する。

【００６１】

一方の受信装置３０は、図４に示すように、送信装置２０で保持する認証鍵テーブルと同様の認証用認証鍵テーブルを保持する認証用認証鍵テーブル保持部３１と、送信装置２０からの情報を受信する受信部３２と、受信したインデックス情報の認証を行うインデックス情報認証部３３と、認証されたインデックス情報に基づいて認証用認証鍵テーブルを検索して認証鍵を取得する認証鍵取得部３４と、取得した認証鍵および受信したパケットに基づいて認証用認証子を生成する認証用認証子生成部３５と、生成した認証用認証子と受信した認証子とに基づいて受信したパケットの認証を行う照合認証部３６と、認証したパケットに対する処理を行うパケット処理部３７とを備える。

【００６２】

受信部３２は、送信装置２０から送られてくるインデックス情報I_i、パケットP_i、および認証子ＭＡＣ（K[I_i]・P_i）を受信する。

【００６３】

認証用認証鍵テーブル保持部３１は、送信装置２０の認証鍵テーブル保持部２３で保持する認証鍵テーブルと同様のテーブルを保持する。尚、以降の説明では、便宜的に受信装置３０で保持する認証テーブルを認証用認証鍵テーブルと称し、該テーブルにおける認証鍵を認証用認証鍵と称する。

【００６４】

前記した認証鍵テーブルおよび認証用認証鍵テーブルは、送信装置２０および受信装置３０間で秘密裡に保持されている。

【００６５】

インデックス情報認証部３３は、インデックス情報保持部３３１と、インデックス情報比較判定部３３２とを備えている。

インデックス情報保持部３３１は、受信した最新のインデックス情報を保持しており、保持するインデックス情報は、後述するインデックス情報比較判定部３３２において認証されたインデックス情報である。

【００６６】

インデックス情報比較判定部３３２は、例えば受信したインデックス情報がインデックス情報I_iであるとき、該インデックス情報I_iを一方向性関数ｆに入力した結果が、式４に示すように、以前に公開されて保持管理しているインデックス情報I_{i-1}と一致するか、又は秘密裡に受信して保持管理しているインデックス情報I_0と一致するか否か照合判定し、一致するときインデックス情報I_iは認証される。

$$I_{i-1}=f(I_i) \qquad (式４)$$

【００６７】

認証されたインデックス情報I_iは、インデックス情報保持部３３１でインデックス情報I_{i-1}に代わって保持される。

尚、インデックス情報比較判定部３３２において、インデックス情報が認証できない場合、後述するパケットの認証処理を行うことなく、インデックス情報の不認証をパケット処理部３７に通知し、該パケット処理部３７で通知結果に対応する処理が行われる。

【００６８】

認証鍵取得部３４は、認証されたインデックス情報I_iに基づいて認証用認証鍵テーブル保持部３１で保持する認証用認証鍵テーブルを参照し、インデックス情報I_iに対応する認証用認証鍵$K[I_i]$を取得する。例えば、認証鍵取得部３４は、インデックス情報I_1に対応する認証用認証鍵$K[I_1]$を取得する。

【００６９】

認証用認証子生成部３５は、認証鍵取得部３４で取得した認証用認証鍵と受信部３２で受信したパケットとに基づいて、ＡＥＳ暗号などの共通鍵ブロック暗号を用いたＣＢＣ－ＭＡＣなどを用いて認証用認証子を生成する。

例えば、認証用認証鍵$K[I_1]$およびパケットP_1をパラメータとしてＣＢＣ－ＭＡＣを用いて認証子を生成すると、認証子ＭＡＣ（$K[I_1]$・P_1）と示される認証用認証子が生成される。

【００７０】

照合認証部３６は、認証用認証子生成部３５で生成した認証用認証子と、受信部３２で受信した認証子との比較照合を行ない、認証用認証子および受信した認証子の内容が一致すると、当該認証子と共に送られてきたパケットは送信装置２０から送信されたパケットであると認証する。

【００７１】

パケット処理部３７は、インデックス情報認証部３３および照合認証部３６での認証結果に応じて、受信したパケットの処理を行う。例えば照合認証部３６でパケットが認証されない場合、受信したパケットを破棄する。

【００７２】

次に、本発明のメッセージ認証システム１０の動作をフローチャートを用いて説明する。

尚、便宜的に本発明のメッセージ認証システム１０を構成する送信装置２０の動作を説明した後、受信装置３０の動作を説明する。

【００７３】

送信装置２０は、図５のフローチャートに示すように、認証鍵テーブル（認証用認証鍵テーブル）を受信装置３０との間で秘密裡に共有すべく、認証鍵テーブル保持部２３で保持する（ステップＳ３０１）。

認証鍵テーブルの共有は、例えば暗号化などの方法を用いた通信によるインストールや、予め送信装置２０および受信装置３０に認証鍵テーブル（認証用認証鍵テーブル）の組み込み（インストール）を行い、送信装置２０および受信装置３０との間で秘密裡に共有することができる。

【００７４】

次に、インデックス情報チェーン生成部２２１で生成してインデックス情報チェーン保持部２２２で保持するインデックス情報チェーンにおいて、全てのインデックス情報を使い切ったか否かを判定する（ステップＳ３０２）。

【００７５】
全てのインデックス情報が使われているとき、インデックス情報チェーン生成部２２１は、再度インデックス情報チェーンを生成し、一番最後に生成されたインデックス情報を初期値I_0として受信装置３０に送信する（ステップＳ３０３）。
尚、ステップＳ３０２において、通信の最初は、インデックス情報チェーンが生成されていないので、インデックス情報チェーンが生成されていなくとも、ステップＳ３０３のインデックス情報チェーンを生成し、初期値I_0の送信処理が行われる。
【００７６】
ステップＳ３０２において、インデックス情報チェーンにおける未使用のインデックス情報が存在するとき、又はステップＳ３０３における処理が終了した後、インデックス情報に対応する認証鍵と、パケットとに基づいて認証子生成部２４で認証子を生成する（ステップＳ３０４）。
【００７７】
認証子生成部２４で生成された認証子と、該認証子の生成に用いたパケットと、インデックス情報とが送信部２５により受信装置３０へ送信される。
【００７８】
その後、パケット生成部２１でパケットが生成されると、前記したステップＳ３０２からの処理を繰返し、当該パケットを受信装置３０に送信する。
【００７９】
次に、受信装置３０の動作を図６のフローチャートに沿って説明する。
認証用認証鍵テーブル（認証鍵テーブル）を送信装置２０との間で秘密裡に共有すべく、認証用認証鍵テーブル保持部３１で保持する（ステップＳ４０１）。
認証用認証鍵テーブルの共有は、例えば暗号化などの方法を用いた通信によるインストールや、予め受信装置３０および送信装置２０に認証用認証鍵テーブル（認証鍵テーブル）の組み込み（インストール）を行い、送信装置２０および受信装置３０との間で秘密裡に共有することができる。
【００８０】
次に、送信装置２０からのインデックス情報の初期値I_0を受信部３２で受信すると（ステップＳ４０２）、該初期値I_0がインデックス情報保持部３３１で保持される（ステップＳ４０３）。
【００８１】
その後、受信部３２がメッセージとしてのパケットと、インデックス情報と、認証子とを受信すると（ステップＳ４０４）、インデックス情報比較判定部３３２でインデックス情報の認証を行う（ステップＳ４０５）。インデックス情報比較判定部３３２は、受信したインデックス情報を一方向性関数ｆに入力し、その出力結果をインデックス情報保持部３３１で保持するインデックス情報と比較照合し、照合が一致すると受信したインデックス情報が認証される。
【００８２】
一方、不一致であると、一方向性関数ｆの出力結果を再度一方向性関数ｆに入力し、その出力結果と、インデックス情報保持部３３１で保持するインデックス情報との比較照合を行なう（ステップＳ４０５）。
【００８３】
前記したインデックス情報の比較照合を所定の回数行い、該回数内で照合が一致すると、インデックス情報は認証され、所定の回数内で照合が一致しない場合には、インデックス情報は不認証として、共に受信したパケットの認証、すなわち当該パケットを認証するための認証子の認証処理を行うことなく、前記したステップＳ４０２からの処理を繰返す。
【００８４】
一方、前記したステップＳ４０５において、インデックス情報が認証されると、認証鍵取得部３４はインデックス情報に基づいて認証用認証鍵テーブルを参照し、該テーブルか

らインデックス情報に対応する認証用認証鍵を取得する。
その後、認証用認証子生成部３５は、取得した認証用認証鍵と受信パケットとに基づいて認証用認証子を生成する。
【００８５】
照合認証部３６は、認証用認証子とパケットと共に受信した認証子とを比較照合し、認証用認証子および受信した認証子の内容が一致すると、当該認証子と共におくられてきたパケットは送信装置２０から送信されたパケットであると認証する。
【００８６】
照合認証部３６からの認証結果を受けたパケット処理部３７は、認証結果に応じたパケット処理を行い、前記したステップＳ４０２からの処理を繰返す。
【００８７】
前記したように、実施例１のメッセージ認証システム１０によれば、認証鍵とインデックス情報とを対応付けた認証鍵テーブル（認証用認証鍵テーブル）を送信装置２０および受信装置３０間で秘密裡に共有した後、パケットに対応する認証鍵を用いて認証子を生成し、該認証子とインデックス情報とパケットとを送信装置２０から受信装置３０へ送信する。受信装置３０は、認証子、パケットおよびインデックス情報を受信すると、インデックス情報を認証し、認証されたインデックス情報に基づいて認証用認証鍵テーブルから、当該インデックス情報に対応する認証用認証鍵を取得し、取得した認証用認証鍵と受信パケットとに基づいて認証用認証子を生成し、該認証用認証子と受信した認証子との比較照合を行なうことから、送信装置２０から受信装置３０へ認証鍵を送信しなくてもよい。従って、送信装置２０からパケットを送信後、つまりパケットの送信から十分な時間遅延の後に認証鍵を送信装置２０から受信装置３０へ送信する必要がなく、受信装置３０でインデックス情報および認証子と共に受信するパケットの認証をパケットなどの情報を受信後、即座に行うことができる。
【実施例２】
【００８８】
次に、実施例１では認証鍵テーブル（認証用認証鍵テーブル）を送信装置２０および受信装置３０間で秘密裡に共有する例を説明したが、実施例２では認証鍵テーブル（認証用認証鍵テーブル）の共有に代えて、認証鍵（認証用認証鍵）を得るための関数を共有する例を説明する。尚、実施例２の各説明において、前記した実施例１と同様である場合には、その説明を割愛し、実施例２の特徴となる内容のみを説明する。
【００８９】
実施例２のメッセージの認証方法の概念を図８を用いて説明するが、図８の概念図において、送信装置２０での処理内容が上段に示されており、受信装置３０での処理内容が下段に示されており、処理順序の番号が丸囲い文字で示されている。
【００９０】
先ず、送信装置２０および受信装置３０間で秘密裡に認証鍵（認証用認証鍵）を得るための鍵関数Ｆが秘密裡に共有される（図８の１）。
【００９１】
鍵関数Ｆは認証鍵を得るための媒介径数情報が入力されると、当該媒介径数情報に対応する認証鍵（認証用認証鍵）を生成する関数である。
【００９２】
尚、各媒介径数情報はそれぞれ認証鍵に対応しており、各媒介径数情報から成る一連の情報が媒介径数情報チェーンと称され、該媒介径数情報チェーンは、前記した実施例１のインデックス情報チェーンと同様に一方向性関数を用いて生成される。
【００９３】
尚、媒介径数情報は、実施例１のインデックス情報と同様に認証鍵を取得するための情報であることから、媒介径数情報をインデックス情報と称し、媒介径数情報チェーンをインデックス情報チェーンと称して以降の説明を行う。
【００９４】

前記した鍵関数Ｆが秘密裡に共有された後、送信装置２０は、乱数などにおいて任意に選定した数値をインデックス情報$Ｉ_{n}$とし、該インデックス情報$Ｉ_{n}$に対し、後述する一方向性関数を用いて各認証鍵に対応した一連のインデックス情報をインデックス情報チェーンとして生成する（図８の２）。

【００９５】

このとき、インデックス情報チェーンにおける各インデックス情報は、鍵関数に基づいて得る各認証鍵に対応している。

【００９６】

ところで、一方向性関数は要約関数又はメッセージダイジェスト（圧縮）関数と称される関数であり、具体的にはＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ５）やＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　１）などである。このような一方向性関数を用いて、式３に示す演算を行う。

【００９７】

式３による演算結果をパラメータとして一方向性関数ｆに逐次入力する。すなわち、式３による演算結果を入力パラメータとして、再度式３に入力することを繰返す。これにより、数値列$Ｉ_{n}$、・・・、$Ｉ_{1}$（＝ｆ（$Ｉ_{2}$））、$Ｉ_{0}$（＝ｆ（$Ｉ_{1}$））がインデックス情報チェーンとして生成される。

【００９８】

送信装置２０で生成したインデックス情報チェーン$Ｉ_{n}$・・・$Ｉ_{0}$において、初期値としてのインデックス情報$Ｉ_{0}$は、予め秘密裡に受信装置３０に送られ、該受信装置３０で保持管理される（図８の３）。

【００９９】

その後、送信装置２０は、インデックス情報$Ｉ_{i}$に対する認証鍵を鍵関数を用いて生成し、生成した認証鍵Ｆ（$Ｉ_{i}$）と、送信すべきパケット$Ｐ_{i}$とに基づいて認証子ＭＡＣ（Ｆ（$Ｉ_{i}$）・$Ｐ_{i}$）を生成する。認証子は、各パケット毎に生成されており、認証子を生成した送信装置は、パケット$Ｐ_{i}$と認証子ＭＡＣ（Ｆ（$Ｉ_{i}$）・$Ｐ_{i}$）とインデックス情報$Ｉ_{i}$とから成る１組の情報をパケット毎に受信装置に送信する。

【０１００】

送信装置２０からの情報を受信した受信装置３０は、先ずインデックス情報$Ｉ_{i}$の認証を行う。

インデックス情報の認証は、前記した実施例１と同様であり、例えば受信したインデックス情報がインデックス情報$Ｉ_{i}$であるとき、該インデックス情報$Ｉ_{i}$を一方向性関数ｆに入力した結果が、式４に示すように、以前に公開されて保持管理しているインデックス情報$Ｉ_{i-1}$と一致するか、又は秘密裡に受信して保持管理しているインデックス情報$Ｉ_{0}$と一致するか否か照合判定することにより行われる。

【０１０１】

次に、認証したインデックス情報$Ｉ_{i}$を受信装置３０で保持している鍵関数に代入し、当該インデックス情報$Ｉ_{i}$に対応する認証鍵Ｆ（$Ｉ_{i}$）を認証用認証鍵として生成する。

【０１０２】

受信装置３０は、生成した認証用認証鍵Ｆ（$Ｉ_{i}$）と、受信したパケット$Ｐ_{i}$とに基づいて認証用の認証子ＭＡＣ（Ｆ（$Ｉ_{i}$）・$Ｐ_{i}$）を生成する。

その後、受信装置３０は、認証用認証子ＭＡＣ（Ｆ（$Ｉ_{i}$）・$Ｐ_{i}$）と、受信した認証子ＭＡＣ（Ｆ（$Ｉ_{i}$）・$Ｐ_{i}$）との比較照合を行なう。この照合で、認証用認証子ＭＡＣ（Ｆ（$Ｉ_{i}$）・$Ｐ_{i}$）および受信した認証子ＭＡＣ（Ｆ（$Ｉ_{i}$）・$Ｐ_{i}$）が一致すると、認証子と共に受信したパケット$Ｐ_{i}$は送信装置２０から送信されたパケットであると認証される（図８の４）。

【０１０３】

ここで、実施例２のメッセージ認証方法を用いたメッセージ認証システムを説明する。

実施例２のメッセージ認証システムは、前記した実施例１と同様に、送信装置２０および受信装置３０を備えている。

【０１０４】
実施例２の送信装置２０は、図９に示すように、パケットを生成するパケット生成部２１と、インデックス情報を生成して管理するインデックス情報生成部２２と、認証鍵を生成するための鍵関数を保持する鍵関数保持部２６と、該鍵関数保持部２６で保持する鍵関数とインデックス情報とに基づいて認証鍵を生成する認証鍵生成部２７と、生成した認証鍵に基づいてパケットに対する認証子を生成する認証子生成部２８と、生成した認証子、パケットおよびインデックス情報を受信装置３０に対し送信する送信部２５とを備える。
【０１０５】
インデックス情報生成部２２は、前記した実施例１と同様に、インデックス情報チェーン生成部２２１と、該インデックス情報チェーン生成部で生成されるインデックス情報チェーンを保持するインデックス情報チェーン保持部２２２とを備えている。
【０１０６】
インデックス情報チェーン生成部２２１は、乱数やランダムな文字列などから任意の数値列（文字列）をインデックス情報I_nとして選定し、該インデックス情報を式３に示す一方向性関数に代入し、求めた値を更に式３に代入することを繰返し、次に示すI_n、・・・I_1（＝ｆ（I_2））、I_0（＝ｆ（I_1））成る数値列をインデックス情報チェーンとして生成する。インデックス情報チェーン生成部２２１で生成されたインデックス情報チェーンは、インデックス情報チェーン保持部２２２で保持される。
【０１０７】
鍵関数保持部２６は、認証鍵を生成するための鍵関数Ｆを保持しており、認証鍵生成部２７は、鍵関数保持部２６で保持する鍵関数Ｆにインデックス情報生成部２２で生成したインデックス情報I_iを入力し、その結果を認証鍵Ｆ（I_i）として取得する。すなわち、認証鍵生成部２７は、鍵関数Ｆとインデックス情報I_iとに基づいて、認証鍵Ｆ（I_i）を生成する。生成された認証鍵は、パケットの認証子生成に用いられる。
【０１０８】
認証子生成部２８は、認証鍵生成部２７で生成した認証鍵Ｆ（I_i）とパケットP_iに基づいて、ＡＥＳ暗号などの共通鍵ブロック暗号を用いたＣＢＣ－ＭＡＣなどにより、認証子ＭＡＣ（Ｆ（I_i）・P_i）を生成する。
送信部２５は、認証子生成部２８で生成した認証子ＭＡＣ（Ｆ（I_i）・P_i）と、パケットP_iと、インデックス情報I_iとを受信装置３０に送信する。
【０１０９】
一方の実施例２の受信装置３０は、図１０に示すように、送信装置２０で保持する鍵関数と同様の認証用鍵関数を保持する認証用鍵関数保持部３８と、送信装置２０からの情報を受信する受信部３２と、受信したインデックス情報の認証を行うインデックス情報認証部３３と、認証されたインデックス情報と認証用鍵関数保持部３８で保持する認証用鍵関数とに基づいて認証用の認証鍵を生成する認証用認証鍵生成部３９と、生成した認証用認証鍵と、受信したパケットとに基づいて認証用認証子を生成する認証用認証子生成部３５と、生成した認証用認証子と受信した認証子とに基づいて受信したパケットの認証を行う照合認証部３６と、認証したパケットに対する処理を行うパケット処理部３７とを備える。
【０１１０】
認証用鍵関数保持部３８は、送信装置２０の鍵関数保持部２６で保持する鍵関数と同様の認証用鍵関数を保持する。尚、送信装置２０および受信装置３０との間で鍵関数（認証用鍵関数）が秘密裡に保持されている。
【０１１１】
インデックス情報認証部３３は、前記した実施例１と同様に、インデックス情報保持部３３１と、インデックス情報比較判定部３３２とを備えている。
インデックス情報保持部３３１は、受信した最新のインデックス情報を保持しており、保持するインデックス情報は、後述するインデックス情報比較判定部３３２において認証されたインデックス情報である。

【０１１２】
インデックス情報比較判定部３３２は、例えば受信したインデックス情報がインデックス情報I_iであるとき、該インデックス情報I_iを一方向性関数ｆに入力した結果が、式４に示すように、以前に公開されて保持管理しているインデックス情報I_{i-1}と一致するか、又は秘密裡に受信して保持管理しているインデックス情報I_0と一致するか否か照合判定し、一致するときインデックス情報I_iは認証される。認証されたインデックス情報I_iは、インデックス情報保持部３３１でインデックス情報I_{i-1}に代わって保持される。
【０１１３】
尚、インデックス情報比較判定部３３２において、インデックス情報が認証できない場合、後述するパケットの認証処理を行うことなく、インデックス情報の不認証をパケット処理部３７に通知し、該パケット処理部３７で通知結果に対応する処理が行われる。
【０１１４】
認証用認証鍵生成部３９は、認証されたインデックス情報I_iを認証用鍵関数保持部３８で保持する認証用鍵関数に代入し、インデックス情報I_iに対応する認証用認証鍵Ｆ（I_i）を生成する。
【０１１５】
認証用認証子生成部３５は、認証用認証鍵生成部３９で生成した認証用認証鍵Ｆ（I_i）と受信部３２で受信したパケットP_iとに基づいて、ＡＥＳ暗号などの共通鍵ブロック暗号を用いたＣＢＣ－ＭＡＣなどにより認証用認証子ＭＡＣ（Ｆ（I_i）・P_i）を生成する。
【０１１６】
次に、本発明のメッセージ認証システム１０の動作をフローチャートを用いて説明する。
尚、便宜的に本発明のメッセージ認証システムを構成する送信装置２０の動作を説明した後、受信装置３０の動作を説明する。
【０１１７】
実施例２の送信装置２０は、図１１のフローチャートに示すように、鍵関数（認証用鍵関数）を受信装置３０との間で秘密裡に共有すべく、鍵関数を鍵関数保持部２６で保持する（ステップＳ７０１）。
鍵関数の共有は、例えば暗号化などの方法を用いた通信によるインストールや、予め送信装置２０および受信装置３０に鍵関数（認証用鍵関数）の組み込み（インストール）を行い、送信装置２０および受信装置３０との間で秘密裡に共有することができる。
【０１１８】
次に、インデックス情報チェーン生成部２２１で生成してインデックス情報チェーン保持部２２２で保持するインデックス情報チェーンにおいて、全てのインデックス情報を使い切ったか否かを判定する（ステップＳ７０２）。
【０１１９】
全てのインデックス情報が使われているとき、インデックス情報チェーン生成部２２１は、再度インデックス情報チェーンを生成し、一番最後に生成されたインデックス情報を初期値I_0として受信装置３０に送信する（ステップＳ７０３）。
尚、ステップＳ７０２において、通信の最初は、インデックス情報チェーンが生成されていないので、インデックス情報チェーンが生成されていなくとも、ステップＳ７０３のインデックス情報チェーンを生成し、初期値I_0の送信処理が行われる。
【０１２０】
ステップＳ７０２において、インデックス情報チェーンにおける未使用のインデックス情報が存在するとき、又はステップＳ７０３における処理が終了した後、インデックス情報に基づいて認証鍵を認証鍵生成部２７で生成する。その後、生成した認証鍵およびパケットに基づいて認証子生成部２８で認証子を生成する（ステップＳ７０４）。
【０１２１】

認証子生成部２８で生成された認証子と、該認証子の生成に用いたパケットと、インデックス情報とが送信部２５により受信装置３０へ送信される。

【０１２２】

その後、パケット生成部２１でパケットが生成されると、前記したステップＳ７０２からの処理を繰返し、当該パケットを受信装置３０に送信する。

【０１２３】

次に、実施例２の受信装置３０の動作を図１２のフローチャートに沿って説明する。

認証用鍵関数（鍵関数）を送信装置２０との間で秘密裡に共有すべく、認証用鍵関数を認証用鍵関数保持部３８で保持する（ステップＳ８０１）。

認証用鍵関数の共有は、例えば暗号化などの方法を用いた通信によるインストールや、予め受信装置３０および送信装置２０に認証用鍵関数（鍵関数）の組み込み（インストール）を行い、送信装置２０および受信装置３０との間で秘密裡に共有することができる。

【０１２４】

次に、送信装置２０からのインデックス情報の初期値I_0を受信部３２で受信すると（ステップＳ８０２）、該初期値I_0がインデックス情報保持部３３１で保持される（ステップＳ８０３）。

【０１２５】

その後、受信部３２がメッセージとしてのパケットと、インデックス情報と、認証子とを受信すると（ステップＳ８０４）、インデックス情報比較判定部３３２でインデックス情報の認証を行う（ステップＳ８０５）。インデックス情報比較判定部３３２は、受信したインデックス情報を一方向性関数ｆに入力し、その出力結果をインデックス情報保持部３３１で保持するインデックス情報と比較照合し、照合が一致すると受信したインデックス情報が認証される。

【０１２６】

一方、不一致であると、一方向性関数ｆの出力結果を再度一方向性関数ｆに入力し、その出力結果と、インデックス情報保持部３３１で保持するインデックス情報との比較照合を行なう（ステップＳ８０５）。

【０１２７】

前記したインデックス情報の比較照合を所定の回数行い、該回数内で照合が一致すると、インデックス情報は認証され、所定の回数内で照合が一致しない場合には、インデックス情報は不認証として、共に受信したパケットの認証、すなわち当該パケットを認証するための認証子の認証処理を行うことなく、前記したステップＳ８０２からの処理を繰返す。

【０１２８】

一方、前記したステップＳ８０５において、インデックス情報が認証されると、認証用認証鍵生成部３９はインデックス情報に基づいて認証用鍵関数保持部３８で保持する認証用鍵関数を用いて認証用認証鍵を生成する。

その後、認証用認証子生成部３５は、取得した認証用認証鍵と受信パケットとに基づいて認証用認証子を生成する。

【０１２９】

照合認証部３６は、認証用認証子とパケットと共に受信した認証子とを比較照合し、認証用認証子および受信した認証子の内容が一致すると、当該認証子と共に送られてきたパケットは送信装置２０から送信されたパケットであると認証する。

【０１３０】

照合認証部３６からの認証結果を受けたパケット処理部３７は、認証結果に応じたパケット処理を行い、前記したステップＳ８０２からの処理を繰返す。

【０１３１】

前記したように、実施例２のメッセージ認証システムによれば、インデックス情報に基づいて認証鍵を生成するための鍵関数（認証用鍵関数）を送信装置２０および受信装置３０間で秘密裡に共有した後、パケットに対応する認証鍵を用いて認証子を生成し、該認証

子とインデックス情報とパケットとを送信装置２０から受信装置３０へ送信する。受信装置３０は、認証子、パケットおよびインデックス情報を受信すると、インデックス情報を認証し、認証されたインデックス情報に基づいて保持している認証用鍵関数を用いて認証用認証鍵を生成し、該認証用認証鍵と受信パケットとに基づいて認証用認証子を生成し、該認証用認証子と受信した認証子との比較照合を行なうことから、送信装置２０から受信装置３０へ認証鍵を送信しなくてもよい。従って、送信装置２０からパケットを送信後、つまりパケットの送信から十分な時間遅延の後に認証鍵を送信装置２０から受信装置３０へ送信する必要がなく、受信装置３０でインデックス情報および認証子と共に受信するパケットの認証をパケットなどの情報を受信後、即座に行うことができる。

【０１３２】

ところで、一斉同報通信と称されるブロードキャストは、送信装置２０と各受信装置３０との間が有線や無線などの媒体でネットワーク構築されており、図２に示すように、例えば無線によるネットワークであって、該ネットワークに接続する受信装置３０において、メッセージを受信して認証する他に、中継装置（ルータ）として機能するマルチホップ無線通信と称される通信システムに、本発明を適用してもよい。

【０１３３】

従来のメッセージ認証方法でマルチホップ無線通信システムを構築すると、パケットおよび認証子が送信装置から受信装置へブロードキャストされ、全ての受信装置で受信が完了した後に認証鍵を公開（ブロードキャスト）しないと、ブロードキャストされる情報に盗用された認証鍵で改竄が行われる虞がある。

【０１３４】

従ってブロードキャストされる情報が改竄されないように、認証鍵を十分な時間遅延の後送信する必要があった。この時間遅延の間にも受信装置は、送信装置からブロードキャストされる多数のパケットを受信し続ける必要がある。すなわち、受信装置は、受信したパケットおよび認証子を、認証鍵が公開されてパケットおよび認証子の認証が完了するまで、長時間に渡って保持し続けなければならず、そのため順次送られてくるパケットおよび認証子を保持するための大容量の受信バッファが必要であた。

【０１３５】

一方、本発明のメッセージ認証方法でマルチホップ無線通信システムを構築すると、前記したように、送信装置から同時的に送られてくるインデックス情報および認証子およびパケットを受信装置３０で受信後、該受信装置３０は即座にパケットの認証を行って、受信パケットの処理を行うことから、受信した情報を認証鍵を取得するまで保持し続ける必要がなく、よって該各情報を保持するための受信バッファの容量を低減することができる。従って、マルチホップ無線通信システムに発明のメッセージ認証方法を適用することにより、低容量の受信バッファで受信装置を製造することができ、受信装置の製造コストを低減することができる。

【産業上の利用可能性】

【０１３６】

前記した実施例では、メッセージの配信方法としてブロードキャストを例に説明したが、これに限る必要はなく、ユニキャストやマルチキャストに本発明を適用してもよい。

【図面の簡単な説明】

【０１３７】

【図１】実施例１のメッセージ認証方法の概念図である。

【図２】本発明のメッセージ認証システムのシステム構成およびマルチホップ無線通信を示す図である。

【図３】実施例１の送信装置のブロック図である。

【図４】実施例１の受信装置のブロック図である。

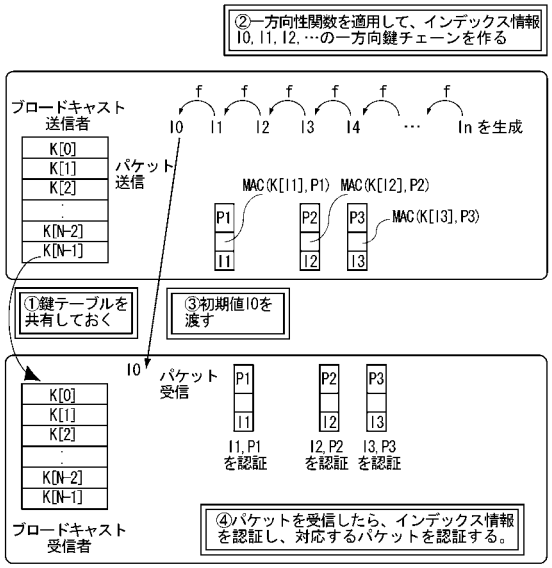
【図５】実施例１の送信装置の動作を示すフローチャートである。

【図６】実施例１の受信装置の動作を示すフローチャートである。

【図７】従来のメッセージ認証方法の概念図である。

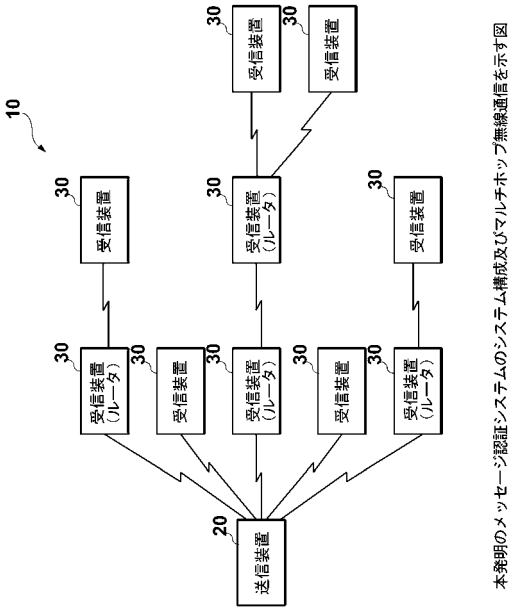
【図８】実施例２のメッセージ認証方法の概念図である。
【図９】実施例２の送信装置のブロック図である。
【図１０】実施例２の受信装置のブロック図である。
【図１１】実施例２の送信装置の動作を示すフローチャートである。
【図１２】実施例２の受信装置の動作を示すフローチャートである。
【符号の説明】
【０１３８】
１０　メッセージ認証システム
２０　送信装置
２１　パケット生成部
２２　インデックス情報生成部
２３　認証鍵テーブル保持部
２４　認証子生成部
２５　送信部
２６　鍵関数保持部
２７　認証鍵生成部
２８　認証子生成部
３０　受信装置
３１　認証用認証鍵テーブル保持部
３２　受信部
３３　インデックス情報認証部
３４　認証鍵取得部
３５　認証用認証子生成部
３６　照合認証部
３７　パケット処理部
３８　認証用鍵関数保持部
３９　認証用認証鍵生成部
２２１　インデックス情報チェーン生成部
２２２　インデックス情報チェーン保持部
３３１　インデックス情報保持部
３３２　インデックス情報比較判定部

【図１】



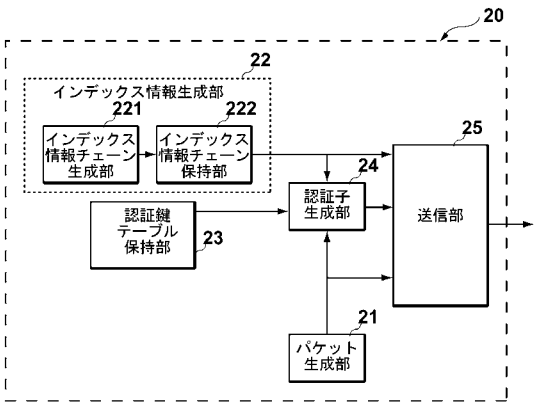
実施例１のメッセージ認証方法の概念図

【図２】



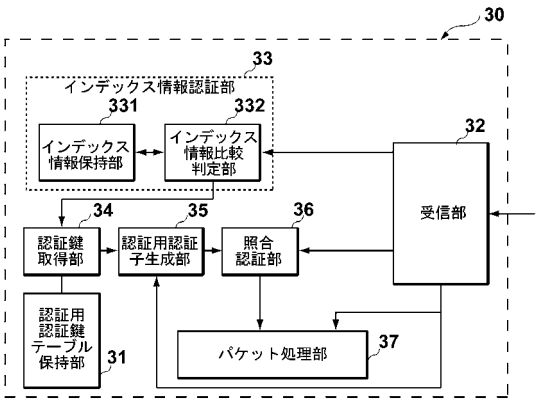
本発明のメッセージ認証システムのシステム構成及びマルチホップ無線通信を示す図

【図３】



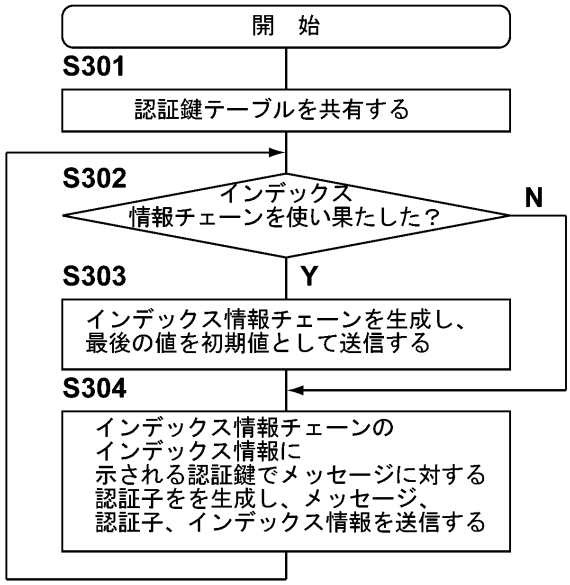
実施例１の送信装置のブロック図

【図４】



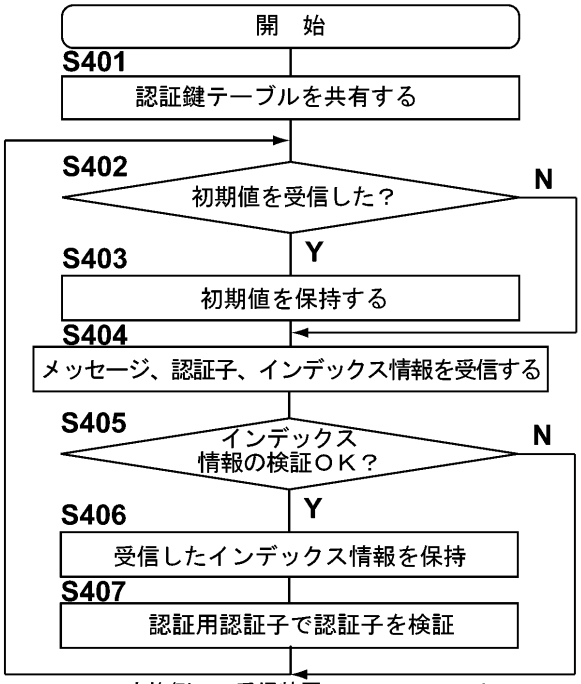
実施例１の受信装置のブロック図

【図５】



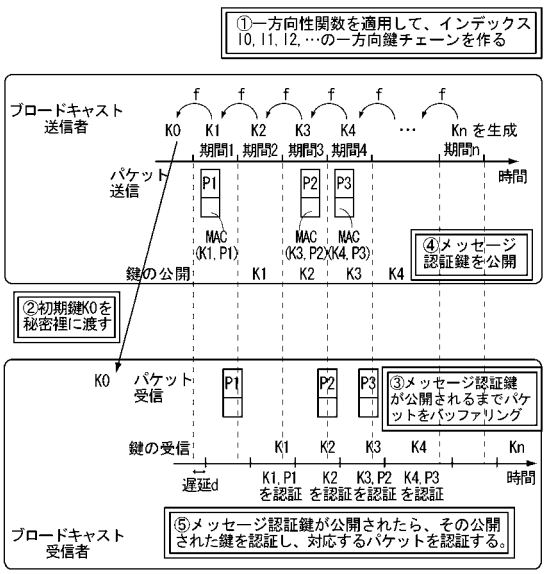
実施例１の送信装置のフローチャート

【図６】



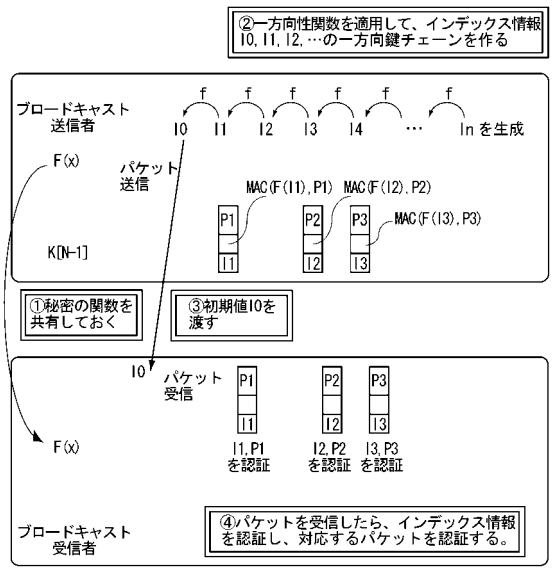
実施例１の受信装置のフローチャート

【図７】



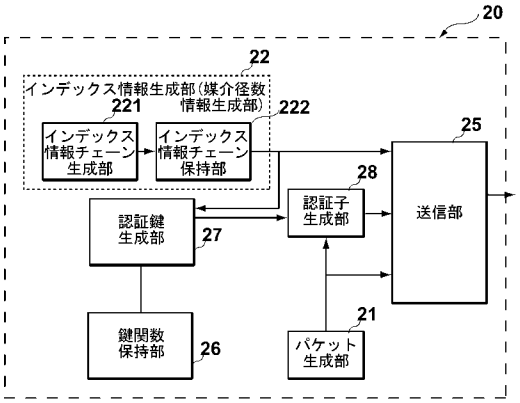
従来のメッセージ認証方法の概念図

【図８】



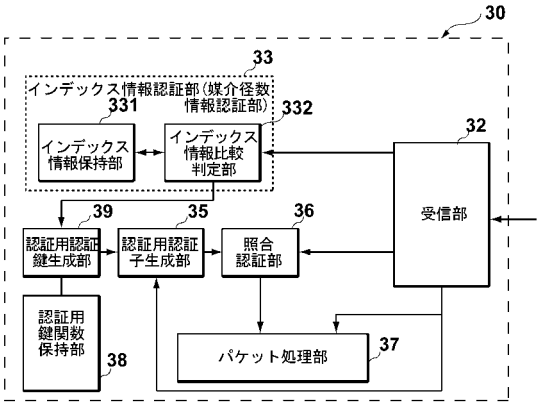
実施例２のメッセージ認証方法の概念図

【図９】



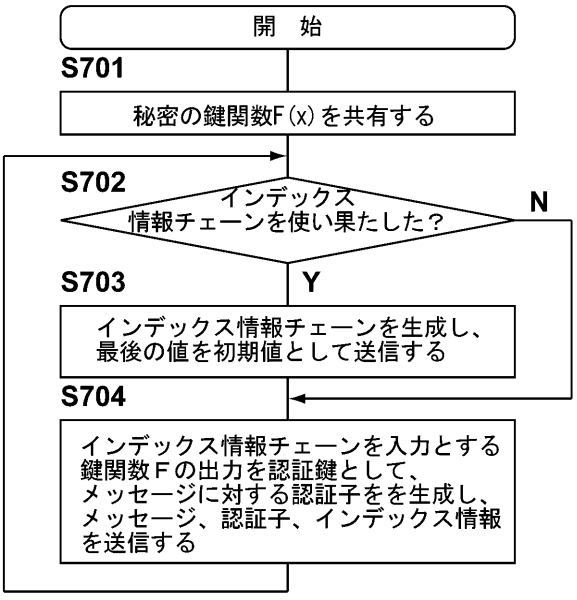
実施例２の送信装置のブロック図

【図１０】



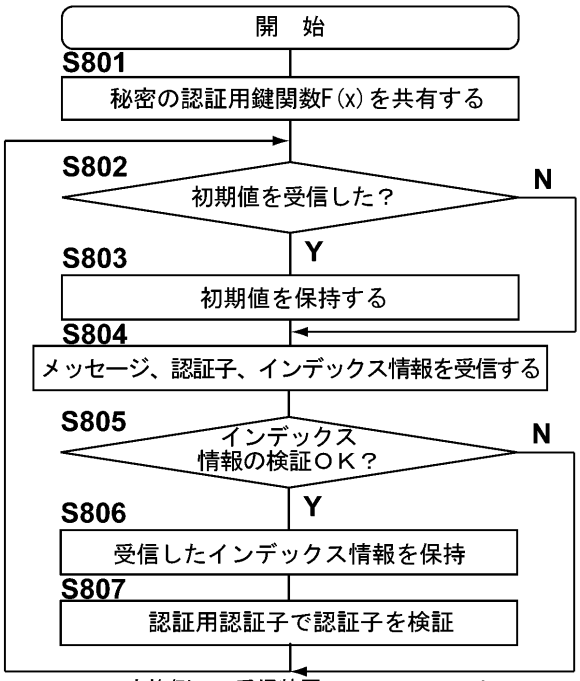
実施例２の受信装置のブロック図

【図１１】



実施例２の送信装置のフローチャート

【図１２】



実施例２の受信装置のフローチャート

フロントページの続き

(56)参考文献 特開２００３－１５００５１（ＪＰ，Ａ）
特開２０００－３３２７４２（ＪＰ，Ａ）
特開２００３－２８３４８９（ＪＰ，Ａ）
国際公開第０１／０４９０５８（WO，Ａ１）
特開２００１－２５１２９６（ＪＰ，Ａ）
特開２００２－２０８９２２（ＪＰ，Ａ）
特開２００２－２１７８９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　１２／１４
Ｈ０６Ｆ　１５／００
Ｈ０４Ｎ　　５／９１
Ｈ０４Ｎ　　７／１６７
Ｈ０４Ｌ　１２／００
Ｈ０４Ｌ　１３／００