(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2010-62652
(P2010-62652A)
(43)公開日　平成22年3月18日(2010.3.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 9　ＯＬ　（全 17 頁）

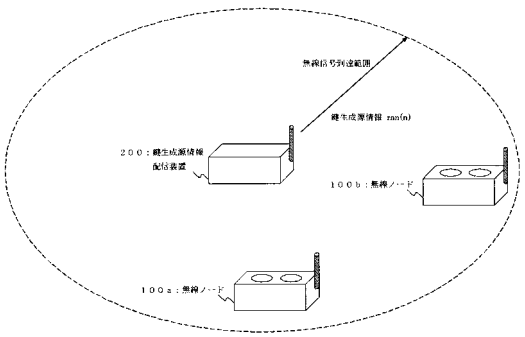
(21)出願番号　特願2008-223719 (P2008-223719)
(22)出願日　平成20年9月1日 (2008.9.1)

(71)出願人　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　100085198
弁理士　小林　久夫
(74)代理人　100098604
弁理士　安島　清
(74)代理人　100125494
弁理士　山東　元希
(74)代理人　100061273
弁理士　佐々木　宗治
(74)代理人　100070563
弁理士　大村　昇
(74)代理人　100087620
弁理士　高梨　範夫

最終頁に続く

(54)【発明の名称】共通鍵生成端末、鍵共有システム、共通鍵生成方法

(57)【要約】
【課題】共通鍵を確実かつ安全に共有することのできる共通鍵生成手法を得る。
【解決手段】鍵生成源情報ｒａｎを複数取得する鍵生成源取得部と、鍵生成源情報ｒａｎのうち所定操作入力前後の所定時間幅ｔｗ内に鍵生成源取得部が取得したものを記録する記録部１１１と、他端末が送信する情報を受信する受信部１３１と、鍵生成源情報ｒａｎの少なくともいずれかに、受信部１３１が受信した情報と合致するものがあるか否かを検証する受信情報検証部１１７と、鍵生成源情報ｒａｎの少なくともいずれかを用いて他端末に送信する情報を生成する送信情報生成部と、送信情報生成部が生成した情報を他端末に送信する送信部１３０と、鍵生成源情報ｒａｎと合致すると受信情報検証部１１７が検証した情報と、鍵生成源情報ｒａｎを用いて送信情報生成部が生成した情報とに基づき共通鍵を生成する共通鍵生成部と、を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
共通鍵暗号に用いる共通鍵を生成する端末であって、
前記共通鍵を生成する基となる鍵生成源情報を複数取得する鍵生成源取得部と、
操作入力を受け付ける操作部と、
前記鍵生成源情報のうち前記操作部が所定操作入力を受け付けた時点を基準とする所定時間幅内に前記鍵生成源取得部が取得したものを記録する記録部と、
他端末が送信する情報を受信する受信部と、
前記記録部が記録している鍵生成源情報の少なくともいずれかに、前記受信部が受信した情報と合致するものがあるか否かを検証する受信情報検証部と、
前記記録部が記録している鍵生成源情報の少なくともいずれかを用いて前記他端末に送信する情報を生成する送信情報生成部と、
前記送信情報生成部が生成した情報を前記他端末に送信する送信部と、
前記記録部に記録されている鍵生成源情報と合致すると前記受信情報検証部が検証した情報と、前記記録部に記録されている鍵生成源情報を用いて前記送信情報生成部が生成した情報とに基づき前記共通鍵を生成する共通鍵生成部と、
を備えることを特徴とする共通鍵生成端末。
【請求項２】
前記送信情報生成部は任意の第１チャレンジ情報を生成し、
前記受信情報検証部は、
前記受信部が受信した情報が、
前記記録部に記録されている鍵生成源情報と前記第１チャレンジ情報を所定演算式に適用して得られる情報と一致するか否かにより、
前記検証を実行する
ことを特徴とする請求項１記載の共通鍵生成端末。
【請求項３】
前記受信部は、
前記他端末が送信する任意の第２チャレンジ情報を受信し、
前記送信情報生成部は、
前記第２チャレンジ情報と前記記録部に記録されている鍵生成源情報を前記所定演算式に適用して前記第２チャレンジ情報に対するレスポンス情報を生成する
ことを特徴とする請求項２記載の共通鍵生成端末。
【請求項４】
前記送信部および前記受信部は、前記他端末と無線により通信する
ことを特徴とする請求項１ないし請求項３のいずれかに記載の共通鍵生成端末。
【請求項５】
前記鍵生成源情報を他端末に配信する手段を備えた
ことを特徴とする請求項１ないし請求項４のいずれかに記載の共通鍵生成端末。
【請求項６】
複数の前記鍵生成源情報を自ら生成する手段と、
その複数の鍵生成源情報を他端末との間で共有する手段と、
を備えることを特徴とする請求項１ないし請求項４のいずれかに記載の共通鍵生成端末。
【請求項７】
請求項１ないし請求項４のいずれかに記載の複数の共通鍵生成端末と、
前記鍵生成源情報を各前記共通鍵生成端末に配信する鍵生成源情報配信装置と、
を有することを特徴とする鍵共有システム。
【請求項８】
請求項５または請求項６記載の共通鍵生成端末を複数有する
ことを特徴とする鍵共有システム。

【請求項９】
共通鍵暗号に用いる共通鍵を生成する方法であって、
前記共通鍵を生成する基となる鍵生成源情報を複数取得する鍵生成源取得ステップと、
操作入力を受け付ける操作ステップと、
前記鍵生成源情報のうち前記操作ステップで所定操作入力を受け付けた時点を基準とする所定時間幅内に前記鍵生成源取得ステップで取得したものを記録する記録ステップと、
他端末が送信する情報を受信する受信ステップと、
前記記録ステップで記録した鍵生成源情報の少なくともいずれかに、前記受信ステップで受信した情報と合致するものがあるか否かを検証する受信情報検証ステップと、
前記記録ステップで記録した鍵生成源情報の少なくともいずれかを用いて前記他端末に送信する情報を生成する送信情報生成ステップと、
前記送信情報生成ステップで生成した情報を前記他端末に送信する送信ステップと、
前記記録ステップで記録した鍵生成源情報と合致すると前記受信情報検証ステップで検証した情報と、前記記録ステップで記録した鍵生成源情報を用いて前記送信情報生成ステップで生成した情報とに基づき前記共通鍵を生成する共通鍵生成ステップと、
を有することを特徴とする共通鍵生成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、共通鍵暗号を用いて情報を暗号化する際に用いる共通鍵を生成する端末およびその方法、共通鍵を共有するシステムに関するものである。
【背景技術】
【０００２】
従来、『複数の装置間で安全に鍵情報を共有することが可能な鍵共有システムを提供すること。』を目的とした技術として、『認証管理装置２０と複数の無線端末装置１０とからなる鍵共有システム１において，認証管理装置２０は，鍵生成源情報を定期的に生成して各無線端末装置１０に発信する。また，各無線端末装置１０は，認証管理装置２０から定期的に発信される鍵生成源情報を受信しつつ，無線端末装置１０に対して直接的に与えられる第１の外部入力の検出をトリガとして，上記受信される鍵生成源情報のうち１又は２以上の鍵生成源情報を選択して保持する。そして，各無線端末装置１０は，この保持された１又は２以上の鍵生成源情報に基づいて鍵情報を生成し，この鍵情報を認証管理装置２０と共有する。これにより，盗聴装置は，無線端末装置１０及び認証管理装置２０に対して直接的に与えられる第１の外部入力を検出できないので，装置間で鍵情報を安全に共有できる。』というものが提案されている（特許文献１）。
【０００３】
また、『無線ＬＡＮシステムでは、端末とアクセスポイント間の接続情報の通信が暗号化されていない無線通信により行われるため、無線出力を低減したとしても、第三者が高感度アンテナを用いて無線通信を盗聴した場合には、接続設定値が簡単に漏洩してしまう。このため、無線ＬＡＮのセキュリティが確保されない可能性がある。』ということを課題とした技術として、『無線ネットワーク接続設定値の秘匿性を高くするために、無線基地局と無線端末から成る無線システムの無線接続情報の設定方法は、無線基地局を無線端末の接続設定要求を受信する待機状態と無線端末の接続設定要求を拒否する閉塞状態を有する構成とし、無線基地局が待機状態のときに、無線端末のユーザに合図を送るステップと、合図に呼応して、ユーザの無線端末から無線基地局に該無線端末の公開鍵暗号を設定するステップと、公開鍵暗号により無線接続情報を暗号化して無線端末に送付するステップとから成るようにした。』というものが提案されている（特許文献２）。
【０００４】
【特許文献１】特開２００７－８８６２９号公報（要約）
【特許文献２】特開２００７－１８９５６５号公報（要約）
【発明の開示】

【発明が解決しようとする課題】
【０００５】
上記特許文献１に記載の技術では、鍵を共有したい２つの端末同士でユーザ操作を同時に行い、その直後に受信した鍵生成源情報を秘密情報として共有する。このユーザ操作は、ごく正確に同時発生することを想定している。
【０００６】
しかしながら、ユーザ操作として、例えば２つの機器にそれぞれ装着されているボタンを同時に押す場合を考えたとき、マニュアル操作であるため手元が狂い同時にボタンを押すことができない、といったことも考えられる。
この場合、ユーザ操作にタイムラグが発生するので、ユーザ操作直後に受信した鍵生成源情報が２つの端末間で異なり、共有可能な鍵生成源情報を一意に決定することができない場合もあり得る。すると、結果的に２つの端末間で共通鍵を生成することができないことになる。
【０００７】
特に、第３者からの盗聴が困難になるように鍵生成源情報を頻繁に配信している場合には、上述のタイムラグの間に複数の鍵生成源情報が各端末へ配信されることになり、共有可能な鍵生成源情報を各端末が一意に決定することができない可能性が高くなると考えられる。
【０００８】
上記特許文献２に記載の技術では、無線基地局は無線端末から受信した公開鍵を用いてメッセージを暗号化し、無線端末に安全にメッセージを送信する。
しかし、鍵情報そのものを無線信号で送信するため、第３者が容易に鍵情報を盗聴することができ、共通鍵暗号には不向きである。そのため、上記特許文献２では、非対称暗号方式を前提とし、公開鍵を無線配信することとしている。
【０００９】
以上のような背景から、共通鍵を確実かつ安全に共有することのできる共通鍵生成手法が望まれていた。
【課題を解決するための手段】
【００１０】
本発明に係る共通鍵生成端末は、共通鍵暗号に用いる共通鍵を生成する端末であって、前記共通鍵を生成する基となる鍵生成源情報を複数取得する鍵生成源取得部と、操作入力を受け付ける操作部と、前記鍵生成源情報のうち前記操作部が所定操作入力を受け付けた時点を基準とする所定時間幅内に前記鍵生成源取得部が取得したものを記録する記録部と、他端末が送信する情報を受信する受信部と、前記記録部が記録している鍵生成源情報の少なくともいずれかに、前記受信部が受信した情報と合致するものがあるか否かを検証する受信情報検証部と、前記記録部が記録している鍵生成源情報の少なくともいずれかを用いて前記他端末に送信する情報を生成する送信情報生成部と、前記送信情報生成部が生成した情報を前記他端末に送信する送信部と、前記記録部に記録されている鍵生成源情報と合致すると前記受信情報検証部が検証した情報と、前記記録部に記録されている鍵生成源情報を用いて前記送信情報生成部が生成した情報とに基づき前記共通鍵を生成する共通鍵生成部と、を備えるものである。
【発明の効果】
【００１１】
本発明に係る共通鍵生成端末によれば、操作部が所定操作入力を受け付けた時点を基準とする所定時間幅内に取得した鍵生成源情報を記録しておく。
そのため、操作入力を行うタイミングについて端末間のタイムラグがある場合でも、上記所定時間幅以内のタイムラグであれば吸収することができるので、共有可能な共通鍵を確実に生成することができる。
【００１２】
また、共通鍵そのものを配信するわけではなく、共通鍵を生成する基となる鍵生成源情

報を共有するので、各端末は安全に共通鍵を生成することができる。
【発明を実施するための最良の形態】
【００１３】
実施の形態１.
図１は、本発明の実施の形態１に係る鍵共有システムの構成図である。
本実施の形態１に係る鍵共有システムは、無線ノード１００ａおよび１００ｂ、鍵生成源情報配信装置２００を有する。
【００１４】
無線ノード１００ａおよび１００ｂは、鍵生成源情報配信装置２００が配信する鍵生成源情報を受信することができる位置に存在する。また、無線ノード１００ａと１００ｂは互いに通信することのできる位置に存在する。
【００１５】
鍵生成源情報配信装置２００は、鍵生成源情報を配信する。
鍵生成源情報とは、共通鍵を生成する基となる情報のことであり、例えば擬似乱数のシード、あるいは乱数そのものなどがこれに相当する。
【００１６】
無線ノード１００ａと１００ｂは、無線通信を行う通信端末である。無線ノード１００ａと１００ｂは、後述の図５～図７で説明する手法を用いて、鍵生成源情報に基づき共有可能な共通鍵を生成する。
【００１７】
無線ノード１００ａと１００ｂは同様の構成を有するため、以下ではこれらを総称するときは無線ノード１００と呼び、アルファベットの添字を省略する。各無線ノードが備える構成部についても同様である。
【００１８】
図２は、無線ノード１００の外観図である。
無線ノード１００の筐体外部には、表示灯１０５、スイッチ１１０が設けられている。また、無線ノード１００は、他のノードと通信するための無線アンテナ１０４を備える。
ユーザはスイッチ１１０を操作することにより、無線ノード１００に指示を行ったり、外部のイベントを通知したりする。
外部のイベントとは、無線ノードの外部に設置したセンサなどにより検出された外部事象を指す。例えば、無線ノードに外部接続した振動センサの値の変化を外部イベントとして無線ノードに通知する、などが考えられる。この場合、振動センサの値の変化によって、共通鍵の更新（再設定やリフレッシュ）が行われるような利用例が想定される。
表示灯１０５は、ＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）などの表示手段で構成され、点灯により無線ノード１００内部状態を外部に知らせる役割を果たす。例えば、チャレンジレスポンスに成功した、共通鍵の生成に成功したなどの無線ノード内部の処理経過を示す。これにより、ユーザは内部処理を肉眼確認できる。
【００１９】
図３は、鍵生成源情報配信装置２００の外観図である。
鍵生成源情報配信装置２００は、無線通信するための無線アンテナ２０４を備える。
鍵生成源情報配信装置２００は、電源が投入されると、乱数や時刻情報などから構成される鍵生成源情報を所定時間間隔で無線配信する役割を有する。したがって、無線ノード１００のようにスイッチや表示灯は必ずしも必要ない。
本発明では、鍵生成源情報をｒａｎ（ｎ）と表す。ｎは、鍵生成源情報の通番である。
【００２０】
図４は、本実施の形態１に係る無線ノード１００の機能ブロック図である。
無線ノード１００は、スイッチ１１０、鍵生成源情報記録部１１１、一時記録メモリ１１２、記録テーブル１１３、共通秘密情報格納部１１４、ウインドウ時間タイマ１１５、レスポンス生成部１１６、チャレンジ検証部１１７、チャレンジ生成部１１８、ウインドウ時間設定部１２０、送信部１３０、受信部１３１を備える。

また、無線ノード１００は、共通秘密情報格納部１１４が格納する秘密情報を用いて共通鍵を生成する共通鍵生成部（図示せず）を備える。

【００２１】

スイッチ１１０は、鍵生成源情報記録部１１１、一時記録メモリ１１２、ウインドウ時間タイマ１１５に接続されている。

【００２２】

鍵生成源情報記録部１１１は、受信部１３１が受信した鍵生成源情報ｒａｎ（ｎ）のうち、ユーザがスイッチ１１０を押下した直後のもののみを記録する。詳細は後述の図５で改めて説明する。

鍵生成源情報記録部１１１は、共通秘密情報格納部１１４とレスポンス生成部１１６に接続されている。

【００２３】

一時記録メモリ１１２は、受信部１３１が受信した鍵生成源情報ｒａｎ（ｎ）を受信部１３１から経常的に受け取って記録する。ｒａｎ（ｎ）を記録しておく時間は、例えば、後述の図５で説明するユーザ操作ｔ１の前ウインドウ時間ｔｗから始まり、少なくともユーザ操作ｔ１のあとウインドウ時間ｔｗまでに受信した鍵生成源情報を記録する、などとする。

また、スイッチ１１０が押下されたとき、押下時刻の前後それぞれウインドウ時間ｔｗ分の幅内（即ち、時間２ｔｗの幅内）に記録した鍵生成源情報ｒａｎ（ｎ）を、記録テーブル１１３に移動する。詳細は後述の図５で改めて説明する。

【００２４】

記録テーブル１１３は、チャレンジ検証部１１７に接続されている。

【００２５】

共通秘密情報格納部１１４は、無線ノード１００ａと１００ｂで共有する秘密情報を格納する。

本実施の形態１では、鍵生成源情報記録部１１１に記録された鍵生成源情報ｒａｎ（ｎ）と、チャレンジ検証部１１７が検証した鍵生成源情報の２つを、無線ノード１００ａと１００ｂで共有する秘密情報とする。共有手法は、後述の図５～図７で改めて説明する。

【００２６】

ウインドウ時間タイマ１１５は、スイッチ１１０が押下された後、少なくともウインドウ時間ｔｗが経過したとき、その旨をチャレンジ生成部１１８に通知する。

【００２７】

レスポンス生成部１１６は、受信部１３１が受信したチャレンジ情報と、鍵生成源情報記録部１１１に記録されている鍵生成源情報ｒａｎ（ｎ）とを用いて、レスポンス情報を生成する。チャレンジ情報とレスポンス情報については、後述の図５で改めて説明する。

レスポンス生成部１１６は、生成したレスポンス情報を、送信部１３０を介してチャレンジ情報の送信元端末に送信する。

【００２８】

チャレンジ検証部１１７は、記録テーブル１１３の中に、受信部１３１が受信したレスポンス情報と合致する鍵生成源情報が存在するか否かを検証し特定する。特定した鍵生成源情報は、共通秘密情報格納部１１４に格納される。

【００２９】

チャレンジ生成部１１８は、例えば乱数で構成される任意のチャレンジ情報を生成し、送信部１３０を介して送信する。

【００３０】

ウインドウ時間設定部１２０は、ウインドウ時間ｔｗの値をユーザが入力して設定するためのインターフェース等から構成される。

【００３１】

送信部１３０は、レスポンス生成部１１６とチャレンジ生成部１１８が出力するそれぞれの信号に、送信アドレス、受信アドレス、コード番号を付与したパケットを生成し、他

の無線ノードに送信する。パケット形式は、後述の図１０～図１１で改めて説明する。
【００３２】
受信部１３１は、鍵生成源情報配信装置２００が配信する鍵生成源情報ｒａｎ（ｎ）を受信し、一時記録メモリ１１２に格納する。
また、他の無線ノード１００から受信したパケットの、送信アドレス、受信アドレス、コード番号を検査した後、鍵生成源情報記録部１１１、一時記録メモリ１１２、レスポンス生成部１１６、チャレンジ検証部１１７に、各部が受け取る信号を出力する。
【００３３】
ウインドウ時間タイマ１１５、レスポンス生成部１１６、チャレンジ検証部１１７、チャレンジ生成部１１８、ウインドウ時間設定部１２０、共通鍵生成部は、これらの機能を実現する回路デバイスのようなハードウェアで構成することもできるし、マイコンやＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）のような演算装置とその動作を規定する回路デバイスで構成することもできる。
【００３４】
鍵生成源情報記録部１１１、一時記録メモリ１１２、記録テーブル１１３、共通秘密情報格納部１１４は、メモリ装置等の記憶手段で構成することができる。これらを共通の記憶手段で構成することもできる。
【００３５】
送信部１３０、受信部１３１は、無線通信を行うためのインターフェースや信号処理部等を適宜備える。
【００３６】
本実施の形態１における「鍵生成源取得部」は、受信部１３１が相当する。
また、「受信情報検証部」は、チャレンジ検証部１１７が相当する。
また、「送信情報生成部」は、レスポンス生成部１１６、チャレンジ生成部１１８が相当する。
【００３７】
以上、本実施の形態１に係る鍵共有システムと無線ノード１００の構成を説明した。
次に、無線ノード１００ａと１００ｂの間で共通鍵を共有する手順を説明する。
【００３８】
無線ノード１００ａと１００ｂの間で共通鍵を共有するに際し、以下の２つの事項について事前に申し合わせておくこととする。
【００３９】
＜事前の申し合わせ１＞
ユーザは、無線ノード１００ａのスイッチ１１０ａを押下した後に、無線ノード１００ｂのスイッチ１１０ｂを押下するものとする。
＜事前の申し合わせ２＞
ユーザが無線ノード１００ａと１００ｂのスイッチ１１０を押下する時間差は、ウインドウ時間ｔｗ以内であるものとする。
【００４０】
図５は、無線ノード１００ａと１００ｂが共通鍵を共有する過程を示すシーケンス図である。以下、図５の各ステップについて説明する。
【００４１】
（Ｓ５０１）：記録開始
無線ノード１００ａと１００ｂが動作を始める時刻よりも前に、鍵生成源情報配信装置２００が鍵生成源情報ｒａｎ（ｎ）を配信しているものとする。
無線ノード１００ａの受信部１３１ａは、鍵生成源情報ｒａｎ（ｎ）を受信し、一時記録メモリ１１２ａへ記録する動作を開始する（時刻ｔ０）。
【００４２】
（Ｓ５０２）：ユーザ操作
ユーザは、無線ノード１００ａのスイッチ１１０ａを押下する（時刻ｔ１）。ここでは

ｒａｎ（０９）とｒａｎ（１０）の間にスイッチ１１０ａを押下したものとする。
この時点では、一時記録メモリ１１２ａには鍵生成源情報ｒａｎ（０９）までが記録されている。
鍵生成源情報記録部１１１ａは、ユーザがスイッチ１１０ａを押下した直後に受信部１３１ａが受信した鍵生成源情報を記録する。図５の例では、ｒａｎ（１０）が鍵生成源情報記録部１１１ａに記録される。
このｒａｎ（１０）は、以後の処理において、無線ノード１００ａが保持する秘密情報として取り扱われる。
【００４３】
（Ｓ５０３）：ユーザ操作
ユーザは、無線ノード１００ａのスイッチ１１０ａを押下してからウインドウ時間ｔｗが経過するまでの間に、無線ノード１００ｂのスイッチ１１０ｂを押下する（時刻ｔ２）。ここではｒａｎ（１１）とｒａｎ（１２）の間にスイッチ１１０ｂを押下したものとする。
この時点では、一時記録メモリ１１２ｂには鍵生成源情報ｒａｎ（１１）までが記録されている。
鍵生成源情報記録部１１１ｂは、ユーザがスイッチ１１０ｂを押下した直後に受信部１３１ｂが受信した鍵生成源情報を記録する。図５の例では、ｒａｎ（１２）が鍵生成源情報記録部１１１ｂに記録される。
このｒａｎ（１２）は、以後の処理において、無線ノード１００ｂが保持する秘密情報として取り扱われる。
【００４４】
（Ｓ５０４）：タイマ検査
各無線ノードのウインドウ時間タイマ１１５は、ステップＳ５０２とＳ５０３それぞれのユーザ操作からウインドウ時間ｔｗが経過したか否かを検査する。
【００４５】
（Ｓ５０５）：鍵生成源情報移行
時刻ｔ１からウインドウ時間ｔｗ経過後（時刻ｔ３）、一時記録メモリ１１２ａは、ユーザがスイッチ１１０ａを押下した時刻ｔ１前後のウインドウ時間ｔｗ幅内に記録した鍵生成源情報ｒａｎ（ｎ）を、記録テーブル１１３ａに移行する。
図５の例では、ｒａｎ（０７）～ｒａｎ（１２）が該当する。このときの記録テーブル１１３ａの内容は、後述の図８で改めて示す。
【００４６】
（Ｓ５０６）：鍵生成源情報移行
時刻ｔ２からウインドウ時間ｔｗ経過後（時刻ｔ４）、一時記録メモリ１１２ｂは、ユーザがスイッチ１１０ｂを押下した時刻ｔ２前後のウインドウ時間ｔｗ幅内に記録した鍵生成源情報ｒａｎ（ｎ）を、記録テーブル１１３ｂに移行する。
図５の例では、ｒａｎ（０９）～ｒａｎ（１４）が該当する。このときの記録テーブル１１３ｂの内容は、後述の図９で改めて示す。
【００４７】
（Ｓ５０７）：チャレンジ送信
無線ノード１００ａは、時刻ｔ３からさらに少なくともウインドウ時間ｔｗを経過するまで待機する。
次に、チャレンジ生成部１１８ａは、送信部１３０ａを介して、任意のチャレンジ情報ｃｈｌ＿１をブロードキャストする。
ブロードキャストを行うのは、無線ノード１００ａが無線ノード１００ｂの存在を知らない可能性があることによる。即ち、共通の秘密情報を所望する全ての無線ノードにチャレンジ情報ｃｈｌ＿１を配布することを意図したものである。このときのパケット形式は後述の図１０で改めて説明する。
【００４８】

（Ｓ５０８）：レスポンス送信
無線ノード１００ｂの受信部１３１ｂがチャレンジ情報ｃｈｌ＿１を受信した場合、レスポンス生成部１１６ｂは、レスポンス情報ｒｓｐ＿１を生成し、送信部１３０ｂを介して無線ノード１００ａに送信する。
レスポンス生成部１１６ｂは、受信したチャレンジ情報ｃｈｌ＿１と、無線ノード１００ｂの鍵生成源情報記録部１１１ｂに記録されている鍵生成源情報ｒａｎ（１２）とを規定演算式Ｆに適用して、下記式のようにレスポンス情報ｒｓｐ＿１を生成する。
ｒｓｐ＿１＝Ｆ（ｃｈｌ＿１，ｒａｎ（１２））
このときのパケット形式は、後述の図１１で改めて説明する。
また、無線ノード１００ｂは、チャレンジ情報のパケットに含まれる無線ノード１００ａの番号を、適当なメモリ等に記録しておく。

【００４９】
（Ｓ５０９）：レスポンス検証
無線ノード１００ａの受信部１３１ａがレスポンス情報ｒｓｐ＿１を受信すると、チャレンジ検証部１１７ａは、記録テーブル１１３ａの中に、レスポンス情報ｒｓｐ＿１と合致する鍵生成源情報ｒａｎ（ｎ）が記録されているか否かを検証する。
具体的には、ステップＳ５０８で説明した規定の演算式と同じ演算式Ｆを用いて、Ｆ（ｃｈｌ＿１，ｒａｎ（０７））～Ｆ（ｃｈｌ＿１，ｒａｎ（１２））の値を計算し、ｒｓｐ＿１と一致するものがあるか否かを検索する。
ここでは、Ｆ（ｃｈｌ＿１，ｒａｎ（１２））がｒｓｐ＿１と一致するので、ｒａｎ（１２）と無線ノード１００ｂの番号を一時的に適当なメモリ等へ記録しておく。
もし、記録テーブル１１３ａの中に、上述の演算によってレスポンス情報ｒｓｐ＿１と合致する鍵生成源情報ｒａｎ（ｎ）が記録されていなかったときは、無線ノード１００ａと１００ｂは秘密情報を共有することができなかったとみなし、以後の処理を中断する。
本ステップにより、無線ノード１００ｂがステップＳ５０３で秘密情報として記録した鍵生成源情報ｒａｎ（１２）が、無線ノード１００ａと無線ノード１００ｂの間で共有される。

【００５０】
（Ｓ５１０）：チャレンジ送信
無線ノード１００ｂは、時刻ｔ４からさらに少なくともウインドウ時間ｔｗ経過するまで待機する。
次に、チャレンジ生成部１１８ｂは、送信部１３０ｂを介して、任意のチャレンジ情報ｃｈｌ＿２をブロードキャストする。
本ステップの趣旨は、ステップＳ５０７と同様である。

【００５１】
（Ｓ５１１）：レスポンス送信
無線ノード１００ａの受信部１３１ａがチャレンジ情報ｃｈｌ＿２を受信した場合、レスポンス生成部１１６ａは、レスポンス情報ｒｓｐ＿２を生成し、送信部１３０ａを介して無線ノード１００ｂに送信する。
レスポンス生成部１１６ａは、受信したチャレンジ情報ｃｈｌ＿２と、無線ノード１００ａの鍵生成源情報記録部１１１ａに記録されている鍵生成源情報ｒａｎ（１０）とを規定演算式Ｆに適用して、下記式のようにレスポンス情報ｒｓｐ＿２を生成する。
ｒｓｐ＿２＝Ｆ（ｃｈｌ＿２，ｒａｎ（１０））
また、無線ノード１００ａは、チャレンジ情報のパケットに含まれる無線ノード１００ｂの番号を、適当なメモリ等に記録しておく。

【００５２】
（Ｓ５１２）：レスポンス検証
無線ノード１００ｂの受信部１３１ｂがレスポンス情報ｒｓｐ＿２を受信すると、チャレンジ検証部１１７ｂは、記録テーブル１１３ｂの中に、レスポンス情報ｒｓｐ＿２と合致する鍵生成源情報ｒａｎ（ｎ）が記録されているか否かを検証する。

具体的には、ステップＳ５０８で説明した規定の演算式と同じ演算式Ｆを用いて、Ｆ（ｃｈｌ＿２，ｒａｎ（０９））～Ｆ（ｃｈｌ＿２，ｒａｎ（１４））の値を計算し、ｒｓｐ＿２と一致するものがあるか否かを検索する。

ここでは、Ｆ（ｃｈｌ＿２，ｒａｎ（１０））がｒｓｐ＿２と一致するので、ｒａｎ（１０）と無線ノード１００ａの番号を一時的に適当なメモリ等へ記録しておく。

もし、記録テーブル１１３ｂの中に、上述の演算によってレスポンス情報ｒｓｐ＿２と合致する鍵生成源情報ｒａｎ（ｎ）が記録されていなかったときは、無線ノード１００ａと１００ｂは秘密情報を共有することができなかったとみなし、以後の処理を中断する。

本ステップにより、無線ノード１００ａがステップＳ５０２で秘密情報として記録した鍵生成源情報ｒａｎ（１０）が、無線ノード１００ａと無線ノード１００ｂの間で共有される。

【００５３】

（Ｓ５１３）：ノード番号一致確認

無線ノード１００ａと１００ｂのチャレンジ検証部１１７は、チャレンジ情報受信時とレスポンス検証時それぞれでパケットから抽出した相手方ノード番号が相互に一致するか否かを確認する。

一致したことが確認できればステップＳ５１４へ進み、一致が確認できなければ、無線ノード１００ａと１００ｂは秘密情報を共有することができなかったとみなし、以後の処理を中断する。

【００５４】

（Ｓ５１４）：秘密情報を共有

以上のステップにより、無線ノード１００ａと１００ｂは、互いのノード番号を共有したことになる。

さらには、無線ノード１００ａは無線ノード１００ｂが秘密情報として保持する鍵生成源情報ｒａｎ（１２）を特定し、無線ノード１００ｂは無線ノード１００ａが秘密情報として保持する鍵生成源情報ｒａｎ（１０）を特定したことになる。

したがって、無線ノード１００ａと１００ｂの間で、互いのノード番号、鍵生成源情報ｒａｎ（１０）、鍵生成源情報ｒａｎ（１２）が共有されたことになる。

これらは無線ノード１００ａと１００ｂの間で共有する秘密情報として、共通秘密情報格納部１１４に格納される。以後、各無線ノードの共通鍵生成部は、この秘密情報を用いて共通鍵を生成する。

これにより、共有する秘密情報を用いて共通鍵を生成することになるので、各端末では同一の共通鍵を生成することができ、共通鍵そのものを無線送信することなく安全にノード間で共有することができるのである。

【００５５】

以上、無線ノード１００ａと１００ｂが共通鍵を共有する過程を、図５のシーケンス図で説明した。

【００５６】

図６は、図５のシーケンス図を各無線ノードの動作フローとして表した図である。

両図の対応関係を表すため、同じ処理には同じステップ番号を付した。図５のステップを図６において複数のステップで表す場合は、図６のステップ番号に補助番号を添えた。

図６の処理フローの内容は、図５の各ステップと同様である。

【００５７】

図７は、図５のステップＳ５０９やＳ５１２におけるレスポンス検証処理のフローチャートである。以下、図７の各ステップについて説明する。なお、ここでは無線ノード１００ａにおけるＳ５０９の処理を説明する。

【００５８】

（Ｓ７００）

無線ノード１００ａの受信部１３１ａがレスポンス情報ｒｓｐ＿１を受信すると、本処理フローが開始される。

（Ｓ７０１）
チャレンジ検証部１１７ａは、記録テーブル１１３ａの中に、レスポンス情報ｒｓｐ＿１と合致する鍵生成源情報ｒａｎ（ｎ）が記録されているか否かを検証する。
具体的には、ステップＳ５０８で説明した規定の演算式と同じ演算式Ｆを用いて、Ｆ（ｃｈｌ＿１，ｒａｎ（０７））～Ｆ（ｃｈｌ＿１，ｒａｎ（１２））の値を計算し、ｒｓｐ＿１と一致するものがあるか否かを検索する。
【００５９】
（Ｓ７０２）
ｒｓｐ＿１と一致するものを検索できればステップＳ７０３へ進み、検索できなければステップＳ７０４へ進む。
（Ｓ７０３）
チャレンジ検証部１１７ａは、検索した鍵生成源情報（ここではｒａｎ（１２））と無線ノード１００ｂの番号を一時的に適当なメモリ等へ記録しておく。
（Ｓ７０４）
チャレンジ検証部１１７ａは、以後の処理を中断する。
【００６０】
図８は、図５のステップＳ５０５における記録テーブル１１３ａの記録内容を示す図である。ステップＳ５０５では、時刻ｔ１の前後ウインドウ時間ｔｗ幅内に受信した鍵生成源情報ｒａｎ（０７）～ｒａｎ（１２）が記録される。
【００６１】
図９は、図５のステップＳ５０６における記録テーブル１１３ｂの記録内容を示す図である。ステップＳ５０６では、時刻ｔ２の前後ウインドウ時間ｔｗ幅内に受信した鍵生成源情報ｒａｎ（０９）～ｒａｎ（１４）が記録される。
【００６２】
図１０は、チャレンジ情報のパケット構成を示す図である。
チャレンジ情報パケットは、送信アドレス部、受信アドレス部、データ部を有する。
送信アドレス部には、チャレンジ情報パケットの送信元ノード番号が格納される。
受信アドレス部には、ブロードキャストパケットである旨を示す値が格納される。
データ部には、チャレンジ生成部１１８が生成したチャレンジ情報が格納される。
【００６３】
図１１は、レスポンス情報のパケット構成を示す図である。
レスポンス情報パケットは、送信アドレス部、受信アドレス部、データ部を有する。
送信アドレス部には、レスポンス情報パケットの送信元ノード番号が格納される。
受信アドレス部には、レスポンス情報パケットの送信先ノード番号が格納される。
データ部には、レスポンス生成部１１６が生成したレスポンス情報が格納される。
【００６４】
以上、無線ノード１００ａと１００ｂが共通鍵を共有する手順について説明した。
各記憶手段がデータを出力する際には、各記憶手段自体がデータ出力機能を備えていてもよいし、他の機能部やその他の演算装置などが各記憶手段にアクセスし、データを読み取るようにしてもよい。
【００６５】
以上のように、本実施の形態１によれば、鍵生成源情報ｒａｎ（ｎ）が盗聴されたとしても、スイッチ１１０がいつ押下されたかを盗聴端末が知ることはできないので、各端末がいずれの鍵生成源情報を秘密情報として保持しているかを隠蔽することができる。
【００６６】
また、本実施の形態１によれば、ユーザが無線ノード１００ａと１００ｂで行う操作（スイッチ１１０の押下）のタイムラグが、事前に申し合わせたウインドウ時間ｔｗ以内に収まっていれば、各無線ノード１００の記録テーブル１１３には、他の無線ノードが保持する鍵生成源情報ｒａｎ（ｎ）が格納されていることになる。
そのため、ユーザ操作にタイムラグがあっても、各無線ノード１００で、鍵生成源情報

ｒａｎ（ｎ）を秘密情報として共有することができる。
これにより、ユーザは厳密に時刻を同期させることなく、特段の注意を払わずに操作を行うことができるので、共通鍵を簡易かつ安全に共有することができる。
【００６７】
また、本実施の形態１によれば、レスポンス生成部１１６は、鍵生成源情報記録部１１１が記録している鍵生成源情報、即ちユーザ操作直後に記録された鍵生成源情報を、チャレンジ情報とともに演算式Ｆに適用してレスポンス情報を生成する。
これにより、演算式Ｆを共有している前提の下、鍵生成源情報記録部１１１が記録している鍵生成源情報を、安全に他の無線ノードに送信することができる。
【００６８】
また、本実施の形態１によれば、共通鍵そのものを他の無線ノードに送信するのではなく、共通鍵を生成する基となる鍵生成源情報を無線ノード間で共有し、これに基づき各無線ノードは自ら共通鍵を生成する。
したがって、共通鍵が無線ネットワーク内に流れることがないので、公開鍵暗号方式を用いる必要はなく、安全に共通鍵を無線ノード間で共有することができる。
さらには、共通鍵暗号は一般に公開鍵暗号よりも演算負荷が少ないので、共通鍵を安全に共有する利点をさらに高めることができる。
【００６９】
また、本実施の形態１によれば、ウインドウ時間ｔｗをウインドウ時間設定部１２０から入力して変更することにより、ユーザ操作に伴うユーザ負担を変え、無線ノード１００の設置状態やユーザの操作状況に合わせることができる。
例えば、２つの無線ノード１００が離れて設置されている場合、１人のユーザが双方の無線ノード１００の操作を行うと、ユーザ操作に伴う移動時間に起因して、必然的にユーザ操作のタイムラグが大きくなる。
このような場合は、設置状況に合わせたタイムラグを許容するように、ウインドウ時間ｔｗを大きく設定するとよい。
【００７０】
実施の形態２．
実施の形態１では、無線ノード１００ａのスイッチ１１０ａを先に押下する例を説明したが、押下する順番は無線ノード１００ｂが先でもよい。本実施の形態２では、このときの動作について説明する。
【００７１】
図１２は、ユーザが無線ノード１００ｂのスイッチ１１０ｂを先に押下した場合において、無線ノード１００ａと１００ｂが共通鍵を共有する過程を示すシーケンス図である。
図１２の動作シーケンスは、図５と同様である。図１２の例では、各無線ノード１００において行われたユーザ操作の直後に受信した鍵生成源情報、ここではｒａｎ（０８）とｒａｎ（１０）が、無線ノード間で共有されることになる。
【００７２】
実施の形態３．
実施の形態１～２では、ユーザ操作直後に受信した鍵生成源情報ｒａｎ（ｎ）を鍵生成源情報記録部１１１に記録することを説明したが、これに限られず、例えばユーザ操作直前に受信した鍵生成源情報ｒａｎ（ｎ）を鍵生成源情報記録部１１１に記録するようにしてもよい。
図５の例では、ｒａｎ（０９）とｒａｎ（１１）が、鍵生成源情報記録部１１１に記録されることになる。
【００７３】
ユーザ操作は、各無線ノードで秘密情報として使用し、さらに他の無線ノードに共有させたい秘密情報を指示するために行うものである。そのため、その指示内容を特定できるのであれば、記録する鍵生成源情報ｒａｎ（ｎ）は、ユーザ操作の直前直後のいずれであってもよいのである。

また、これ以外にも、ユーザ操作を契機として記録する鍵生成源情報ｒａｎ（ｎ）を確定できるのであれば、ユーザ操作の直前や直後以外に受信した鍵生成源情報ｒａｎ（ｎ）を鍵生成源情報記録部１１１に記録するようにしてもよい。

【００７４】

実施の形態４．

以上の実施の形態１～３では、鍵生成源情報ｒａｎ（ｎ）は、鍵生成源情報配信装置２００が配信することとしたが、各無線ノードのいずれかが鍵生成源情報ｒａｎ（ｎ）を配信する機能を備えていてもよい。

例えば、鍵生成源情報配信装置２００が鍵生成源情報ｒａｎ（ｎ）の一次配信元となり、これを受信した各無線ノードが他の無線ノードに鍵生成源情報ｒａｎ（ｎ）を転送する、といった形態が考えられる。

【００７５】

実施の形態５．

以上の実施の形態１～４では、鍵生成源情報配信装置２００と各無線ノード１００は同一の周波数を用いて無線通信を行うことを想定したが、これに限る必要はなく、各無線ノード１００が共通に受信することのできる無線信号を用いればよい。

例えば、電波時計が受信する時計情報を含む標準電波を用いることができる。

この場合、各無線ノード１００は、標準電波を受信する標準電波受信部と、無線ノード１００間で無線通信を行う送信部１３０および受信部１３１とを、ともに備えることになる。

【００７６】

実施の形態６．

以上の実施の形態１～５では、各無線ノード１００間で共有する鍵生成源情報を特定する手法として、チャレンジ／レスポンス方式を用いたが、これに限る必要はなく、その他の方式を用いて鍵生成源情報を共有することもできる。

【００７７】

実施の形態７．

以上の実施の形態１～６では、各無線ノード１００は、鍵生成源情報ｒａｎ（ｎ）は鍵生成源情報配信装置２００から受信することを説明したが、無線ノード１００自身が鍵生成源情報ｒａｎ（ｎ）を生成し、これを各無線ノード１００間で同期させる手段を各無線ノード１００が備えるようにしてもよい。

【００７８】

例えば、各無線ノード１００は正確な時計または相互に正確に同期可能な時計を備え、鍵生成源情報配信装置２００から鍵生成源情報ｒａｎ（ｎ）を受信することに代えて、各無線ノード１００は、自ら生成する時刻情報を鍵生成源情報ｒａｎ（ｎ）として用いる。

【００７９】

この場合、各無線ノード１００では、同一の値を持つ鍵生成源情報ｒａｎ（ｎ）が同時刻に生成されるので、鍵生成源情報配信装置２００から鍵生成源情報ｒａｎ（ｎ）を受信するのと同等の動作状況となる。したがって、以上の実施の形態で説明した構成と動作をそのまま適用することができる。

【００８０】

本実施の形態７における「鍵生成源情報取得部」は、自ら鍵生成源情報ｒａｎ（ｎ）を生成して取得する手段が相当する。

【００８１】

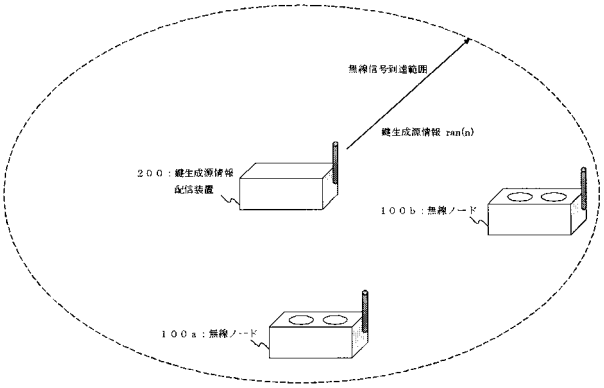
実施の形態８．

以上の実施の形態１～７において、無線ノード１００は無線通信を行う送信部１３０と受信部１３１を備えることを説明したが、同様の手法を有線通信に用いることもできる。

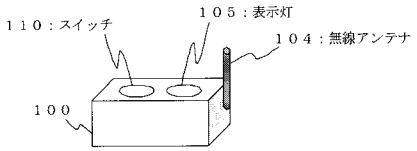
また、送信部１３０と受信部１３１をノード１００から切り離して外部装置に設け、ノード１００は共通鍵共有に係る処理のみを行って、その外部装置を介して他ノードと各情報を送受信するように構成してもよい。

【図面の簡単な説明】
【００８２】
【図１】実施の形態１に係る鍵共有システムの構成図である。
【図２】無線ノード１００の外観図である。
【図３】鍵生成源情報配信装置２００の外観図である。
【図４】実施の形態１に係る無線ノード１００の機能ブロック図である。
【図５】無線ノード１００ａと１００ｂが共通鍵を共有する過程を示すシーケンス図である。
【図６】図５のシーケンス図を各無線ノードの動作フローとして表した図である。
【図７】図５のステップＳ５０９やＳ５１２におけるレスポンス検証処理のフローチャートである。
【図８】図５のステップＳ５０５における記録テーブル１１３ａの記録内容を示す図である。
【図９】図５のステップＳ５０６における記録テーブル１１３ｂの記録内容を示す図である。
【図１０】チャレンジ情報のパケット構成を示す図である。
【図１１】レスポンス情報のパケット構成を示す図である。
【図１２】ユーザが無線ノード１００ｂのスイッチ１１０ｂを先に押下した場合において、共通鍵を共有する過程を示すシーケンス図である。
【符号の説明】
【００８３】
１００ａ～１００ｂ　無線ノード、１１０　スイッチ、１１１　鍵生成源情報記録部、１１２　一時記録メモリ、１１３　記録テーブル、１１４　共通秘密情報格納部、１１５　ウインドウ時間タイマ、１１６　レスポンス生成部、１１７　チャレンジ検証部、１１８　チャレンジ生成部、１２０　ウインドウ時間設定部、１３０　送信部、１３１　受信部、２００　鍵生成源情報配信装置。

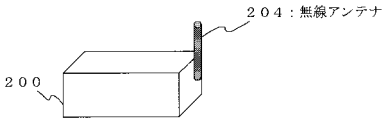
【図１】



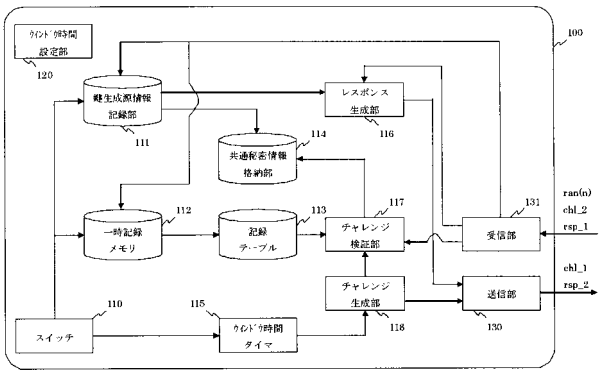
【図２】



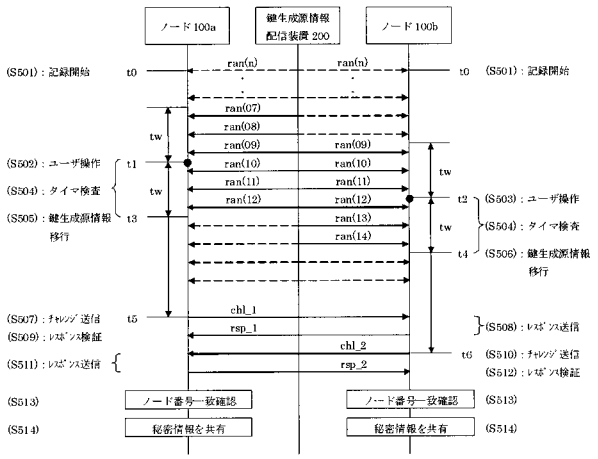
【図３】



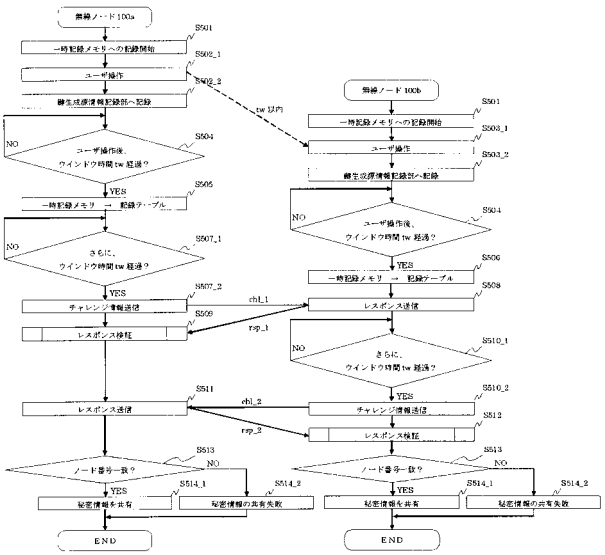
【図４】



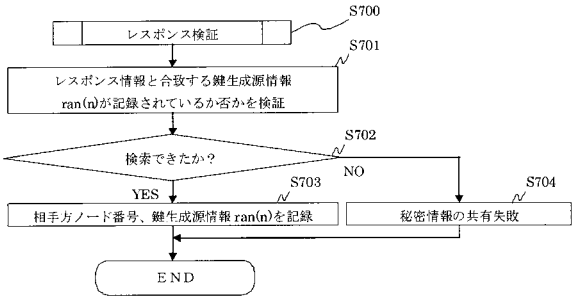
【図５】



【図６】



【図７】



【図８】

ran(07)
ran(08)
ran(09)
ran(10)
ran(11)
ran(12)

【図９】

ran(09)
ran(10)
ran(11)
ran(12)
ran(13)
ran(14)

【図１０】

<チャレンジ情報パケット>

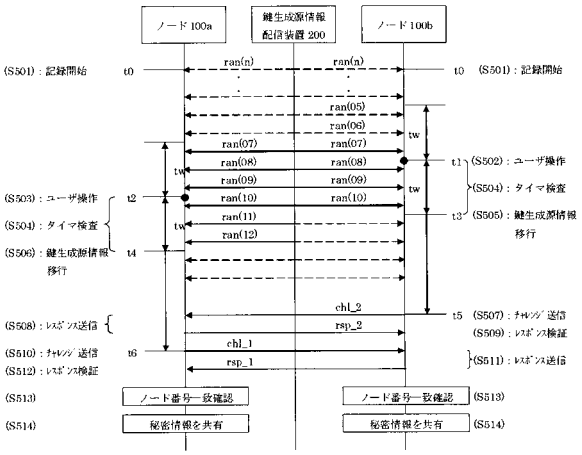
送信ノード番号	－	チャレンジ情報（乱数）
送信アドレス部	受信アドレス部	データ部

【図１１】

<レスポンス情報パケット>

送信ノード番号	受信ノード番号	レスポンス情報
送信アドレス部	受信アドレス部	データ部

【図１２】



フロントページの続き

(72)発明者　小沼　良平
東京都港区西新橋三丁目１６番１１号　沖電気工業株式会社内
Ｆターム(参考) 5J104 AA16　EA23　JA03　PA07