(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4302489号
(P4302489)

(45)発行日　平成21年7月29日(2009.7.29)　(24)登録日　平成21年5月1日(2009.5.1)

(51)Int.Cl.		F I		
H04W 88/02	(2009.01)	H04Q	7/00	646
H04W 12/04	(2009.01)	H04Q	7/00	182
H04L 9/08	(2006.01)	H04L	9/00	601C
		H04L	9/00	601E

請求項の数 16　(全 31 頁)

(21)出願番号　特願2003-382854(P2003-382854)
(22)出願日　平成15年11月12日(2003.11.12)
(65)公開番号　特開2005-150949(P2005-150949A)
(43)公開日　平成17年6月9日(2005.6.9)
審査請求日　平成18年8月7日(2006.8.7)

（出願人による申告）平成１５年度通信・放送機構、研究テーマ「自律分散型無線ネットワークの研究開発」に関する委託研究、産業活力再生特別措置法第３０条の適用を受ける特許出願

(73)特許権者　503027931
学校法人同志社
京都府京都市上京区今出川通烏丸東入玄武町６０１
(73)特許権者　393031586
株式会社国際電気通信基礎技術研究所
京都府相楽郡精華町光台二丁目２番地２
(74)代理人　100112715
弁理士　松山　隆夫
(72)発明者　笹岡　秀一
京都府京田辺市多々羅都谷１－３　同志社大学内
(72)発明者　森　浩樹
京都府京田辺市多々羅都谷１－３　同志社大学内

最終頁に続く

(54)【発明の名称】無線通信システム及びコンピュータに実行させるためのプログラム

(57)【特許請求の範囲】
【請求項１】
指向性を電気的に切換え可能な第１のアンテナと、
第２のアンテナと、
前記第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する第１及び第２の無線装置と、
前記第１の無線装置または前記第２の無線装置から電波を受信する第３の無線装置とを備え、
前記第１の無線装置は、前記第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第２の無線装置から受信した複数の電波に基づいて第１の秘密鍵を生成し、
前記第２の無線装置は、前記第１のアンテナの指向性が前記所定のパターンにより複数個に変えられたときに前記第１の無線装置から受信した複数の電波に基づいて前記第１の秘密鍵と同じ第２の秘密鍵を生成し、
前記第３の無線装置は、前記第１のアンテナの指向性が前記所定のパターンにより複数個に変えられたときに前記第１の無線装置または前記第２の無線装置から受信した複数の電波に基づいて第３の秘密鍵を生成し、
前記所定のパターンは、前記第１および第２の秘密鍵と前記第３の秘密鍵との相関性が最も低くなるパターンである、無線通信システム。
【請求項２】

前記第１の無線装置は、前記複数の電波に基づいて前記複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて前記第１の秘密鍵を生成し、

前記第２の無線装置は、前記受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて前記第２の秘密鍵を生成する、請求項１に記載の無線通信システム。

【請求項３】

前記第１のアンテナは、前記第１の無線装置に搭載され、

前記第１の無線装置は、予め決定された前記所定のパターンを保持しており、その保持した所定のパターンにより前記第１のアンテナの指向性を前記複数個に変える、請求項１または請求項２に記載の無線通信システム。

【請求項４】

前記第１の無線装置は、前記第１の受信信号プロファイルを構成する前記複数の電波の強度を第１の基準値によりデジタル化して前記第１の秘密鍵を生成し、

前記第２の無線装置は、前記第２の受信信号プロファイルを構成する前記複数の電波の強度を第２の基準値によりデジタル化して前記第２の秘密鍵を生成する、請求項２または請求項３に記載の無線通信システム。

【請求項５】

前記第１の無線装置は、１つの基準値により前記複数の電波の強度をデジタル化して２値化された第１の秘密鍵を生成し、

前記第２の無線装置は、別の１つの基準値により前記複数の電波の強度をデジタル化して２値化された第２の秘密鍵を生成する、請求項４に記載の無線通信システム。

【請求項６】

前記第１の無線装置は、複数の基準値により前記複数の電波の強度をデジタル化して多値化された第１の秘密鍵を生成し、

前記第２の無線装置は、別の複数の基準値により前記複数の電波の強度をデジタル化して多値化された第２の秘密鍵を生成する、請求項４に記載の無線通信システム。

【請求項７】

前記第１及び第２の無線装置の各々は、ランダムなビームパターンからなる電波を前記第１および第２のアンテナを介して相互に送受信する、請求項１から請求項６のいずれか１項に記載の無線通信システム。

【請求項８】

前記第１及び第２の無線装置の各々は、マルチビームパターンからなる電波を前記第１および第２のアンテナを介して相互に送受信する、請求項１から請求項６のいずれか１項に記載の無線通信システム。

【請求項９】

前記第１及び第２の無線装置は、前記第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に通信する、請求項１から請求項８のいずれか１項に記載の無線通信システム。

【請求項１０】

２つの秘密鍵が一致する度合いを示す相関値が最小になるように無線通信において用いられる秘密鍵の作成をコンピュータに実行させるためのプログラムであって、

指向性を電気的に切換え可能なアレーアンテナを介して複数種類のパターンからなる指向性パターンに従って前記指向性を変えながら複数の電波を第１の無線装置から第２及び第３の無線装置へ送信する第１のステップと、

前記第２の無線装置が前記複数の電波の強度を検出する第２のステップと、

前記第３の無線装置が前記複数の電波の強度を検出する第３のステップと、

前記第２のステップにおいて検出された第１の複数の電波の強度をデジタル化して第１の秘密鍵を作成する第４のステップと、

前記第３のステップにおいて検出された第２の複数の電波の強度をデジタル化して第２

の秘密鍵を作成する第５のステップと、
前記指向性パターンを複数種類に変えながら前記第１から第５のステップを所定回数繰返して複数の第１の秘密鍵と、前記複数の第１の秘密鍵に対応する複数の第２の秘密鍵とを作成する第６のステップと、
対応する第１及び第２の秘密鍵の相関値を前記複数の第１及び第２の秘密鍵について演算し、その演算した複数の相関値から最小値を抽出する第７のステップと、
前記最小値が得られたときの前記アレーアンテナの最適指向性パターンを抽出する第８のステップと、
前記抽出された最適指向性パターンに従って前記指向性を前記複数種類に切換えながら前記複数の電波を前記第１の無線装置と前記第２の無線装置との間で送受信して前記無線通信において用いられる秘密鍵を作成する第９のステップとをコンピュータに実行させるためのプログラム。
【請求項１１】
前記第１のステップにおいて、前記複数の電波は、マルチビームパターンのビームによって第１の無線装置から第２及び第３の無線装置へ送信される、請求項１０に記載のコンピュータに実行させるためのプログラム。
【請求項１２】
前記第１のステップにおいて、前記複数の電波は、ランダムビームパターンのビームによって第１の無線装置から第２及び第３の無線装置へ送信される、請求項１０に記載のコンピュータに実行させるためのプログラム。
【請求項１３】
前記第４のステップは、
前記第１の複数の電波の強度から第１の基準値を抽出する第１のサブステップと、
前記抽出された第１の基準値によって前記第１の複数の電波の強度をデジタル化して前記第１の秘密鍵を作成する第２のサブステップとを含み、
前記第５のステップは、
前記第２の複数の電波の強度から第２の基準値を抽出する第３のサブステップと、
前記抽出された第２の基準値によって前記第２の複数の電波の強度をデジタル化して前記第２の秘密鍵を作成する第４のサブステップとを含む、請求項１０から請求項１２のいずれか１項に記載のコンピュータに実行させるためのプログラム。
【請求項１４】
前記第１及び第２の基準値は、１つの値からなる、請求項１３に記載のコンピュータに実行させるためのプログラム。
【請求項１５】
前記第１の基準値は、前記第１の複数の電波の強度の中央値であり、
前記第２の基準値は、前記第２の複数の電波の強度の中央値である、請求項１４に記載のコンピュータに実行させるためのプログラム。
【請求項１６】
前記第１及び第２の基準値の各々は、複数の値からなる、請求項１３に記載のコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、無線通信システムに関し、特に、暗号化した情報を無線により通信する無線通信システム及びそれにおいて用いられるコンピュータに実行させるためのプログラムに関するものである。
【背景技術】
【０００２】
最近、情報化社会の発展に伴い情報通信が益々重要になるとともに、情報の盗聴または不正利用がより深刻な問題となっている。このような情報の盗聴を防止するために従来か

ら情報を暗号化して送信することが行なわれている。

【０００３】

情報を暗号化して端末間で通信を行なう方式として公開鍵暗号方式と秘密鍵暗号方式とがある。公開鍵暗号方式は、安全性が高いが、大容量のデータの暗号化には向かない。

【０００４】

一方、秘密鍵暗号方式は、処理が比較的簡単であり、大容量のデータの高速暗号化も可能であるが、秘密鍵を通信の相手方に送信する必要がある。また、秘密鍵暗号方式は、同一の秘密鍵を使用し続けると、暗号解読の攻撃を受けやすく、安全性が損なわれる可能性がある。

【０００５】

そこで、秘密鍵を相手方に送信せずに秘密鍵を共有する方法として、２つの端末間の伝送路の特性を測定し、その測定した特性に基づいて各端末で秘密鍵を生成する方法が提案されている（非特許文献１）。

【０００６】

この方法は、２つの端末間でデータを送受信したときの遅延プロファイルを各端末で測定し、その測定した遅延プロファイルをアナログ信号からデジタル信号に変換して各端末で秘密鍵を生成する方法である。即ち、伝送路を伝搬する電波は可逆性を示すために、一方の端末から他方の端末へデータを送信したときの遅延プロファイルは、他方の端末から一方の端末へ同じデータを送信したときの遅延プロファイルと同じになる。従って、一方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵は、他方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵と同じになる。

【０００７】

このように、伝送路特性を用いて秘密鍵を生成する方法は、同じデータを２つの端末間で相互に送信するだけで同じ秘密鍵を共有することができる。

【非特許文献１】堀池　元樹、笹岡　秀一，「陸上移動通信路の不規則変動に基づく秘密鍵共有方式」，信学技報，社団法人　電子情報通信学会，２００２年１０月，TECHNICAL REPORT OF IEICE RCS2002-173，ｐ．７－１２

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかし、２つの端末間で送信されるデータを盗聴者が各端末の近傍で傍受して遅延プロファイルを測定すれば、盗聴者は、各端末で測定した遅延プロファイルに近い遅延プロファイルを取得することができる。その結果、秘密鍵が解読される可能性がある。

【０００９】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、秘密鍵の盗聴を抑制可能な無線通信システムを提供することである。

【００１０】

また、この発明の別の目的は、２つの秘密鍵の相関値が最小になるように無線通信システムにおいて用いられる秘密鍵の作成をコンピュータに実行させるためのプログラムを提供することである。

【課題を解決するための手段】

【００１１】

この発明によれば、無線通信システムは、第１及び第２のアンテナと、第１及び第２の無線装置とを備える。第１のアンテナは、指向性を電気的に切換え可能である。第１及び第２の無線装置は、第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第１の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第２の無線装置から受信した複数の電波に基づいて第１の秘密鍵を生成する。また、第２の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第１の無線装置から受信した複数の電波に基づいて第１の秘密鍵と同じ第２の秘密鍵を生成する。第１および第２の秘密鍵は、第１のアンテナの指向性

が所定のパターンにより複数個に変えられたときに第３の無線装置が第１の無線装置または第２の無線装置から第１のアンテナを介して受信した複数の電波に基づいて生成された第３の秘密鍵と異なる。

【００１２】

好ましくは、第１の無線装置は、複数の電波に基づいて複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵を生成する。また、第２の無線装置は、受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて第２の秘密鍵を生成する。

【００１３】

好ましくは、所定のパターンは、第１および第２の秘密鍵と第３の秘密鍵との相関性が最も低くなるパターンである。

【００１４】

好ましくは、第１のアンテナは、第１の無線装置に搭載される。第１の無線装置は、予め決定された所定のパターンを保持しており、その保持した所定のパターンにより第１のアンテナの指向性を複数個に変える。

【００１５】

好ましくは、第１の無線装置は、第１の受信信号プロファイルを構成する複数の強度を第１の基準値によりデジタル化して第１の秘密鍵を生成する。第２の無線装置は、第２の受信信号プロファイルを構成する複数の強度を第２の基準値によりデジタル化して第２の秘密鍵を生成する。

【００１６】

好ましくは、第１の無線装置は、１つの基準値により複数の強度をデジタル化して２値化された第１の秘密鍵を生成する。第２の無線装置は、別の１つの基準値により複数の強度をデジタル化して２値化された第２の秘密鍵を生成する。

【００１７】

好ましくは、第１の無線装置は、複数の基準値により複数の強度をデジタル化して多値化された第１の秘密鍵を生成する。第２の無線装置は、別の複数の基準値により複数の強度をデジタル化して多値化された第２の秘密鍵を生成する。

【００１８】

好ましくは、第１及び第２の無線装置の各々は、ランダムなビームパターンからなる電波を第１および第２のアンテナを介して相互に送受信する。

【００１９】

好ましくは、第１及び第２の無線装置の各々は、マルチビームパターンからなる電波を第１および第２のアンテナを介して相互に送受信する。

【００２０】

好ましくは、第１及び第２の無線装置は、第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に通信する。

【００２１】

また、この発明によれば、２つの秘密鍵が一致する度合いを示す相関値が最小になるように無線通信において用いられる秘密鍵の作成をコンピュータに実行させるためのプログラムは、指向性を電気的に切換え可能なアレーアンテナを介して複数種類のパターンからなる指向性パターンに従ってアレーアンテナの指向性を変えながら複数の電波を第１の無線装置から第２及び第３の無線装置へ送信する第１のステップと、第２の無線装置が複数の電波の強度を検出する第２のステップと、第３の無線装置が複数の電波の強度を検出する第３のステップと、第２のステップにおいて検出された第１の複数の強度をデジタル化して第１の秘密鍵を作成する第４のステップと、第３のステップにおいて検出された第２の複数の強度をデジタル化して第２の秘密鍵を作成する第５のステップと、指向性パターンを複数種類に変えながら第１から第５のステップを所定回数繰返して複数の第１の秘密鍵と、複数の第１の秘密鍵に対応する複数の第２の秘密鍵とを作成する第６のステップと

、対応する第１及び第２の秘密鍵の相関値を複数の第１及び第２の秘密鍵について演算し、その演算した複数の相関値から最小値を抽出する第７のステップと、最小値が得られたときのアレーアンテナの最適指向性パターンを抽出する第８のステップと、抽出された最適指向性パターンに従って指向性を複数種類に切換えながら複数の電波を第１の無線装置と第２の無線装置との間で送受信して無線通信において用いられる秘密鍵を作成する第９のステップとをコンピュータに実行させるためのプログラムである。

【００２２】

好ましくは、第１のステップにおいて、複数の電波は、マルチビームパターンのビームによって第１の無線装置から第２及び第３の無線装置へ送信される。

【００２３】

好ましくは、第１のステップにおいて、複数の電波は、ランダムビームパターンのビームによって第１の無線装置から第２及び第３の無線装置へ送信される。

【００２４】

好ましくは、第４のステップは、第１の複数の強度から第１の基準値を抽出する第１のサブステップと、抽出された第１の基準値によって第１の複数の強度をデジタル化して第１の秘密鍵を作成する第２のサブステップとを含む。第５のステップは、第２の複数の強度から第２の基準値を抽出する第３のサブステップと、抽出された第２の基準値によって第２の複数の強度をデジタル化して第２の秘密鍵を作成する第４のサブステップとを含む。

【００２５】

好ましくは、第１及び第２の基準値は、１つの値からなる。

【００２６】

好ましくは、第１の基準値は、第１の複数の強度の中央値であり、第２の基準値は、第２の複数の強度の中央値である。

【００２７】

好ましくは、第１及び第２の基準値の各々は、複数の値からなる。

【発明の効果】

【００２８】

この発明による無線通信システムにおいては、第１及び第２の無線装置は、第１のアンテナの指向性を複数個に変えながら所定のデータを相互に送受信して複数の電波の強度を検出し、その検出した複数の電波の強度プロファイルを示す受信信号プロファイルを生成する。そして、第１及び第２の無線装置は、各受信信号プロファイルに基づいてそれぞれ第１及び第２の秘密鍵を作成する。この場合、無線装置は、盗聴装置において作成された秘密鍵Ｋｓ３と異なる秘密鍵Ｋｓ１，Ｋｓ２が生成されるようにアレーアンテナの指向性を複数種類に切換える。そして、第１及び第２の無線装置は、その作成した第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に無線通信を行なう。

【００２９】

従って、この発明によれば、第１の無線装置と第２の無線装置との間の無線通信において用いられる秘密鍵が第３の無線装置によって盗聴されるのを抑制できる。

【発明を実施するための最良の形態】

【００３０】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００３１】

図１は、この発明の実施の形態による無線通信システムの概略図である。無線通信システム１００は、無線装置１０，３０と、アンテナ１１と、アレーアンテナ２０とを備える。無線装置１０は、例えば、ユーザの移動体通信端末である。また、無線装置３０は、例えば、無線アクセスポイントである。盗聴装置５０は、例えば、無線装置３０の近くに配置される。

【００３２】

アンテナ１１は、無線装置１０に装着される。そして、アンテナ１１は、全方位性のアンテナである。アレーアンテナ２０は、アンテナ素子２１～２７を備える。アンテナ素子２４は、給電素子であり、アンテナ素子２１～２３，２５～２７は、無給電素子である。そして、アンテナ素子２４は、アンテナ素子２１～２３，２５～２７によって取り囲まれている。無給電素子であるアンテナ素子２１～２３，２５～２７は、可変容量素子であるバラクタダイオード（図示せず）が装荷されており、そのバラクタダイオードに印加する直流電圧を制御することにより、アレーアンテナ２０は、適応ビーム形成が可能である。

【００３３】

即ち、アレーアンテナ２０は、無線装置３０に含まれるバラクタダイオードに印加する直流電圧を変えることによって指向性が変えられる。従って、アレーアンテナ２０は、電気的に指向性を切換え可能なアンテナである。

【００３４】

無線装置１０と無線装置３０との間で通信が行われる場合、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による影響を受けて伝搬する。中間物４０としては、反射物及び障害物が想定される。中間物４０が反射物である場合、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって反射されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。また、中間物４０が障害物である場合、無線装置１０のアンテナ１１または無線措置３０のアレーアンテナ２０から出射した電波は、中間物４０によって回折されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。

【００３５】

このように、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による反射を受けて反射波として伝搬したり、中間物４０による回折を受けて回折波として伝搬したりする。そして、電波は、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する場合、直接伝搬成分、反射波成分及び回折波成分が混在しており、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬した電波がどのような成分により構成されるかによって無線装置１０と無線装置３０との間の伝送路の特性が決定される。

【００３６】

この発明においては、無線装置１０と無線装置３０との間で通信が行なわれる場合、アレーアンテナ２０の指向性を複数個に変えて時分割復信（ＴＤＤ：Ｔｉｍｅ　Ｄｉｖｉｓｉｏｎ　Ｄｕｐｌｅｘ）により所定のデータが同一の周波数で無線装置１０，３０間で送受信される。そして、無線装置１０，３０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波の強度を示す受信信号プロファイルＲＳＳＩを生成し、その生成した受信信号プロファイルＲＳＳＩに基づいて秘密鍵を作成する。

【００３７】

より具体的には、無線装置１０，３０は、盗聴装置５０がアンテナ５１を介して無線装置１０または３０から受信した複数の電波の強度を示す受信信号プロファイルに基づいて作成された秘密鍵と異なる秘密鍵を作成する。

【００３８】

秘密鍵が無線装置１０，３０において生成されると、無線装置１０，３０は、生成した秘密鍵により情報を暗号化して相手方へ送信し、相手方から受信した暗号化情報を復号して情報を取得する。

【００３９】

図２は、図１に示す一方の無線装置１０の内部構成を示す概略ブロック図である。無線装置１０は、信号発生部１１０と、送信処理部１２０と、アンテナ部１３０と、受信処理部１４０と、プロファイル生成部１５０と、鍵作成部１６０と、鍵一致確認部１７０と、

鍵記憶部１８０と、鍵一致化部１９０と、暗号部２００と、復号部２１０とを含む。

【００４０】

信号発生部１１０は、秘密鍵を生成するときに無線装置３０へ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部１２０へ出力する。送信処理部１２０は、変調、周波数変換、多元接続及び送信信号の増幅等の送信系の処理を行なう。アンテナ部１３０は、図１に示すアンテナ１１からなり、送信処理部１２０からの送信信号を無線装置３０へ送信し、無線装置３０からの受信信号を受信して受信処理部１４０並びにプロファイル生成部１５０へ供給する。

【００４１】

受信処理部１４０は、受信信号の増幅、多元接続、周波数変換及び復調等の受信系の処理を行なう。そして、受信処理部１４０は、受信処理を行なった信号を必要に応じて鍵一致確認部１７０、鍵一致化部１９０及び復号部２１０へ出力する。

【００４２】

プロファイル生成部１５０は、図１に示すアレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部１３０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。

【００４３】

鍵作成部１６０は、プロファイル生成部１５０からの受信信号プロファイルＲＳＳＩに基づいて秘密鍵Ｋｓ１を作成する。より具体的には、鍵作成部１６０は、受信信号プロファイルＲＳＳＩを１個または複数個の基準値によりデジタル化して秘密鍵Ｋｓ１を作成する。鍵作成部１６０は、受信信号プロファイルＲＳＳＩを１個の基準値によりデジタル化する場合、複数の強度の中央値を基準値として用いる。そして、鍵作成部１６０は、作成した秘密鍵Ｋｓ１を鍵一致確認部１７０及び鍵一致化部１９０へ出力する。

【００４４】

鍵一致確認部１７０は、鍵一致確認用のデータを送信処理部１２０、アンテナ部１３０及び受信処理部１４０を介して無線装置３０と送受信し、鍵作成部１６０によって作成された秘密鍵Ｋｓ１が無線装置３０において作成された秘密鍵Ｋｓ２に一致するか否かを後述する方法によって確認する。そして、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認したとき、秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。また、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に不一致であることを確認したとき、不一致信号ＮＭＴＨを生成して鍵一致化部１９０へ出力する。

【００４５】

鍵記憶部１８０は、鍵一致確認部１７０及び鍵一致化部１９０からの秘密鍵Ｋｓ１を記憶する。また、鍵記憶部１８０は、記憶した秘密鍵Ｋｓ１を暗号部２００及び復号部２１０へ出力する。なお、鍵記憶部１８０は、秘密鍵Ｋｓ１を一時的、例えば、無線装置３０との通信の間だけ記憶するようにしてもよい。

【００４６】

一方、鍵一致化部１９０は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受けると、後述する方法によって秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる。そして、鍵一致化部１９０は、一致させた秘密鍵が秘密鍵Ｋｓ２に一致することを鍵一致確認部１７０における方法と同じ方法によって確認する。

【００４７】

暗号部２００は、送信データを鍵記憶部１８０に記憶された秘密鍵Ｋｓ１によって暗号化して送信処理部１２０へ出力する。復号部２１０は、受信処理部１４０からの受信信号を鍵記憶部１８０からの秘密鍵Ｋｓ１によって復号して受信データを生成する。

【００４８】

図３は、図１に示す他方の無線装置３０の概略ブロック図である。無線装置３０は、無線装置１０のアンテナ部１３０をアンテナ部２２０に代え、指向性設定部２３０、鍵受信部２４０及び鍵相関処理部２５０を追加したものであり、その他は、図２に示す無線装置

１０と同じである。
【００４９】
なお、無線装置３０のプロファイル生成部１５０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部２２０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。
【００５０】
アンテナ部２２０は、図１に示すアレーアンテナ２０からなる。そして、アンテナ部２２０は、送信処理部１２０からの送信信号を指向性設定部２３０によって設定された指向性で無線装置１０へ送信し、無線装置１０からの受信信号を指向性設定部２３０によって設定された指向性で受信して受信処理部１４０またはプロファイル生成部１５０または鍵受信部２４０へ出力する。
【００５１】
指向性設定部２３０は、アンテナ部２２０の指向性を設定する。また、指向性設定部２３０は、無線装置１０，３０において秘密鍵Ｋｓ１，Ｋｓ２を生成するとき、鍵相関処理部２５０からの信号ＰＴＭに応じて、後述する方法により所定の指向性パターンに従ってアンテナ部２２０の指向性を順次切換える。この信号ＰＴＭは、秘密鍵Ｋｓ１，Ｋｓ２と、盗聴装置５０において作成された秘密鍵Ｋｓ３との相関値が最小となるときの指向性パターンを示す信号である。
【００５２】
更に、指向性設定部２３０は、アンテナ部２２０の指向性を変化させる所定の指向性パターンを決定するとき、後述する方法によって、アンテナ部２２０の指向性パターンを複数種類に変える。
【００５３】
鍵受信部２４０は、アンテナ部２２０が受信した盗聴装置５０の秘密鍵Ｋｓ３をアンテナ部２２０から受け、その受けた秘密鍵Ｋｓ３を鍵相関処理部２５０へ出力する。鍵相関処理部２５０は、鍵作成部１６０からの秘密鍵Ｋｓ２と鍵受信部２４０からの秘密鍵Ｋｓ３との相関値を後述する方法によって演算し、その相関値が最小となるときのアンテナ部２２０の指向性パターンを決定し、その決定した指向性パターンを示す信号ＰＴＭを生成して指向性設定部２３０へ出力する。
【００５４】
図４は、図３に示す指向性設定部２３０の概略ブロック図である。指向性設定部２３０は、制御電圧発生回路２３１と、バラクタダイオード２３２とを含む。制御電圧発生回路２３１は、制御電圧ＣＬＶ１～ＣＬＶｎ（ｎは自然数）を順次発生し、その発生した制御電圧ＣＬＶ１～ＣＬＶｎをバラクタダイオード２３２へ順次出力する。バラクタダイオード２３２は、制御電圧ＣＬＶ１～ＣＬＶｎに応じて無給電素子であるアンテナ素子２１～２３，２５～２７に装荷される容量を変え、アレーアンテナ２０の指向性を複数個に順次変える。
【００５５】
図５は、図１に示す盗聴装置５０の概略ブロック図である。盗聴装置５０は、アンテナ部３１０と、プロファイル生成部３２０と、鍵作成部３３０と、鍵送信部３４０とを含む。アンテナ部３１０は、図１に示すアンテナ５１に相当する。アンテナ部３１０は、無線装置１０または３０から複数の電波を受信し、その受信した複数の電波をプロファイル生成部３２０へ出力する。また、アンテナ部３１０は、鍵送信部３４０からの秘密鍵Ｋｓ３を無線装置３０へ出力する。
【００５６】
プロファイル生成部３２０は、アンテナ部３１０からの複数の電波の強度を検出して受信信号プロファイルＲＳＳＩを生成し、その生成した受信信号プロファイルＲＳＳＩを鍵作成部３３０へ出力する。
【００５７】

鍵作成部３３０は、プロファイル生成部３２０からの受信信号プロファイルＲＳＳＩを基準値によりデジタル化して秘密鍵Ｋｓ３を作成し、その作成した秘密鍵Ｋｓ３を鍵送信部３４０へ出力する。

【００５８】

鍵送信部３４０は、鍵作成部３３０からの秘密鍵Ｋｓ３に対して変調、周波数変換、多元接続及び送信信号の増幅等の送信系の処理を行ない、その処理を施した秘密鍵Ｋｓ３をアンテナ部３１０へ出力する。

【００５９】

図６は、図２及び図３に示す鍵一致確認部１７０の概略ブロック図である。鍵一致確認部１７０は、データ発生部１７１と、データ比較部１７２と、結果処理部１７３とを含む。なお、無線装置１０，３０の鍵一致確認部１７０は、同じ構成からなるが、図６においては、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認する動作を説明するために、無線装置３０においてはデータ発生部１７１のみを示す。

【００６０】

無線装置１０のデータ発生部１７１は、鍵作成部１６０から秘密鍵Ｋｓ１を受けると、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認するための鍵確認用データＤＣＦＭ１を発生し、その発生した鍵確認用データＤＣＦＭ１を送信処理部１２０及びデータ比較部１７２へ出力する。

【００６１】

この場合、データ発生部１７１は、秘密鍵Ｋｓ１から非可逆的な演算及び一方向的な演算等により、鍵確認用データＤＣＦＭ１を発生する。より具体的には、データ発生部１７１は、秘密鍵Ｋｓ１またはＫｓ２のハッシュ値を演算することにより、鍵確認用データＤＣＦＭ１を発生する。

【００６２】

データ比較部１７２は、データ発生部１７１から鍵確認用データＤＣＦＭ１を受け、無線装置３０のデータ発生部１７１で発生された鍵確認用データＤＣＦＭ２を受信処理部１４０から受ける。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１を鍵確認用データＤＣＦＭ２と比較する。データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致するとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。

【００６３】

また、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１７２は、不一致信号ＮＭＴＨを鍵一致化部１９０へ出力し、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００６４】

結果処理部１７３は、データ比較部１７２から一致信号ＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１を鍵記憶部１８０へ送って記憶する。

【００６５】

図７は、図２及び図３に示す鍵一致化部１９０の概略ブロック図である。鍵一致化部１９０は、擬似シンドローム作成部１９１と、不一致ビット検出部１９２と、鍵不一致訂正部１９３と、データ発生部１９４と、データ比較部１９５と、結果処理部１９６とを含む。

【００６６】

なお、無線装置１０，３０の鍵一致化部１９０は、同じ構成からなるが、図７においては、秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる動作を説明するために、無線装置３０においては擬似シンドローム作成部１９１のみを示す。

【００６７】

擬似シンドローム作成部１９１は、鍵一致確認部１７０のデータ比較部１７２から不一致信号ＮＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１のシンドロームx_1

を演算する。より具体的には、擬似シンドローム作成部１９１は、秘密鍵Ｋｓ１のビットパターンx_1を検出し、ビットパターンx_1に対して検査行列Ｈを乗算してシンドローム$s1=x_1H^T$を演算する。そして、擬似シンドローム作成部１９１は、ビットパターンx_1を鍵不一致訂正部１９３へ出力し、演算したシンドローム$s1=x_1H^T$を不一致ビット検出部１９２へ出力する。

【００６８】

なお、これらの演算は、ｍｏｄ２の演算であり、H^Tは、検査行列Ｈの転置行列である。

【００６９】

不一致ビット検出部１９２は、擬似シンドローム作成部１９１からシンドロームｓ１を受け、無線装置３０の擬似シンドローム作成部１９１によって演算されたシンドローム$s2=x_2H^T$を受信処理部１４０から受ける。そして、不一致ビット検出部１９２は、シンドロームｓ１とシンドロームｓ２との差分ｓ＝ｓ１－ｓ２を演算する。

【００７０】

なお、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンの差分（鍵不一致のビットパターン）を$e=x_1-x_2$とすると、$s=eH^T$の関係が成立する。ｓ＝０の場合、ｅ＝０となり、秘密鍵Ｋｓ１のビットパターンは、秘密鍵Ｋｓ２のビットパターンに一致する。

【００７１】

不一致ビット検出部１９２は、演算した差分ｓが０でないとき（即ち、$e\neq0$のとき）、鍵不一致のビットパターンｅを鍵不一致訂正部１９３へ出力する。

【００７２】

鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からビットパターンx_1を受けるとともに不一致ビット検出部１９２から鍵不一致のビットパターンｅを受け、ビットパターンx_1から鍵不一致のビットパターンｅを減算することにより相手方の秘密鍵のビットパターン$x_2=x_1-e$を演算する。

【００７３】

このように、鍵一致化部１９０は、秘密鍵Ｋｓ１，Ｋｓ２の不一致を誤りと見なして誤り訂正の応用により秘密鍵Ｋｓ１，Ｋｓ２の不一致を解消する。

【００７４】

この秘密鍵を一致させる方法は、鍵不一致のビット数が誤り訂正能力以上である場合に鍵の一致化に失敗する可能性があるので、鍵一致化の動作を行なった後に鍵一致の確認を行なう必要がある。

【００７５】

データ発生部１９４は、一致化後の鍵$x_2=x_1-e$を鍵不一致訂正部１９３から受けると、鍵x_2に基づいて鍵確認用データＤＣＦＭ３を発生させ、その発生させた鍵確認用データＤＣＦＭ３をデータ比較部１９５へ出力する。また、データ発生部１９４は、発生させた鍵確認用データＤＣＦＭ３を送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００７６】

なお、データ発生部１９４は、鍵一致確認部１７０のデータ発生部１７１による鍵確認用データＤＣＦＭ１の発生方法と同じ方法により鍵確認用データＤＣＦＭ３を発生する。

【００７７】

データ比較部１９５は、データ発生部１９４から鍵確認用データＤＣＦＭ３を受けるとともに無線装置３０で発生された鍵確認用データＤＣＦＭ４を受信処理部１４０から受ける。そして、データ比較部１９５は、鍵確認用データＤＣＦＭ３を鍵確認用データＤＣＦＭ４と比較する。

【００７８】

データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に一致するとき、一致信号ＭＴＨを生成して結果処理部１９６へ出力する。

【００７９】

また、データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１９５は、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

【００８０】

結果処理部１９６は、データ比較部１９５から一致信号ＭＴＨを受けると、鍵不一致訂正部１９３から受けた鍵$x_2 = x_1 - e$を鍵記憶部１８０へ送って記憶する。

【００８１】

このように、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における確認方法と同じ方法によって一致化が施された鍵の一致を確認する。

【００８２】

図８は、受信信号プロファイルＲＳＳＩの概念図である。無線装置３０の指向性設定部２３０の制御電圧発生回路２３１は、各々が電圧Ｖ１～Ｖ６からなる制御電圧ＣＬＶ１～ＣＬＶｎを順次発生してバラクタダイオード２３２へ出力する。この場合、電圧Ｖ１～Ｖ６は、それぞれ、アンテナ素子２１～２３，２５～２７に装荷される容量を変えるための電圧であり、０～２０Ｖの範囲で変えられる。

【００８３】

バラクタダイオード２３２は、パターンＰ１からなる制御電圧ＣＬＶ１に応じてアレーアンテナ２０の指向性をある１つの指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ１を検出する。

【００８４】

次に、バラクタダイオード２３２は、パターンＰ２からなる制御電圧ＣＬＶ２に応じてアレーアンテナ２０の指向性を別の指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ２を検出する。

【００８５】

以後、同様にして、バラクタダイオード２３２は、それぞれ、パターンＰ３～Ｐｎからなる制御電圧ＣＬＶ３～ＣＬＶｎに応じてアレーアンテナ２０の指向性を順次変える。そして、アレーアンテナ２０は、各々設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ３～ＷＩｎを順次検出する。

【００８６】

なお、パターンＰ１～Ｐｎは、秘密鍵Ｋｓ１，Ｋｓ２と秘密鍵Ｋｓ３との相関値ρが最小となるときの制御電圧パターンＰ１ｏｐｔ～Ｐｎｏｐｔである。

【００８７】

そして、プロファイル生成部１５０は、強度ＷＩ１～ＷＩｎからなる強度プロファイルを示す受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。

【００８８】

パターンＰ１～Ｐｎによってアレーアンテナ２０の指向性を複数個に順次切換えて無線装置３０から無線装置１０へデータを送信したとき、無線装置１０のプロファイル生成部１５０が受信信号プロファイルＲＳＳＩを生成する。

【００８９】

鍵作成部１６０は、プロファイル生成部１５０から受信信号プロファイルＲＳＳＩを受け、受信信号プロファイルＲＳＳＩから中央値ＷＩｃｅｎｔ（＝ＷＩ７）を検出する。この中央値ＷＩｃｅｎｔ（＝ＷＩ７）は、複数の強度ＷＩ１～ＷＩｎを強度の高い順に並べたときの中央値である。そして、鍵作成部１６０は、中央値ＷＩｃｅｎｔ（＝ＷＩ７）に

よって受信信号プロファイルＲＳＳＩをデジタル化し、各強度ＷＩ１～ＷＩｎを２値化する。鍵作成部１６０は、２値化した各値を検出し、その検出した各値をビットパターンとする秘密鍵Ｋｓ１またはＫｓ２を作成する。

【００９０】

図９は、図８に示すパターンＰ１～Ｐｎを決定するための制御電圧パターンと受信信号プロファイルを示す図である。秘密鍵Ｋｓ１，Ｋｓ２と秘密鍵Ｋｓ３との相関値が最小になる制御電圧パターンＰ１～Ｐｎを決定する場合、制御電圧パターンは、制御電圧パターンＰ１１～Ｐｎ１，Ｐ１２～Ｐｎ２，・・・，Ｐ１ｊ～Ｐｎｊ（ｊは、自然数）に従って変えられる。

【００９１】

制御電圧パターンＰ１１～Ｐｎ１，Ｐ１２～Ｐｎ２，・・・，Ｐ１ｊ～Ｐｎｊの各々は、電圧Ｖ１～Ｖ６からなる。無給電素子２１～２３，２５～２７に印加される電圧が制御電圧パターンＰ１１～Ｐｎ１，Ｐ１２～Ｐｎ２，・・・，Ｐ１ｊ～Ｐｎｊに従って変えられるとき、アレーアンテナ２０の指向性パターンは、指向性パターンＤ１１～Ｄｎ１，Ｄ１２～Ｄｎ２，・・・，Ｄ１ｊ～Ｄｎｊと変えられる。

【００９２】

無線装置３０は、制御電圧パターンＰ１１～Ｐｎ１，Ｐ１２～Ｐｎ２，・・・，Ｐ１ｊ～Ｐｎｊに従ってアレーアンテナ２０の指向性パターンを変化させて所定の信号を構成する電波を無線装置１０との間で送受信する。この場合、電波は、盗聴装置５０にも到達する。

【００９３】

この場合、無線装置１０，３０は、制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊに対応して受信信号プロファイルＲＳＳ１１，ＲＳＳＩ２１，・・・，ＲＳＳＩｊ１を受信し、盗聴装置５０は、制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊに対応して受信信号プロファイルＲＳＳ１３，ＲＳＳＩ２３，・・・，ＲＳＳＩｊ３を受信する。

【００９４】

そして、無線装置１０，３０は、受信信号プロファイルＲＳＳ１１，ＲＳＳＩ２１，・・・，ＲＳＳＩｊ１を基準値によってデジタル化してそれぞれ秘密鍵Ｋｓ１１～Ｋｓ１ｊ，Ｋｓ２１～Ｋｓ２ｊを作成し、盗聴装置５０は、受信信号プロファイルＲＳＳ１３，ＲＳＳＩ２３，・・・，ＲＳＳＩｊを基準値によってデジタル化して秘密鍵Ｋｓ３１～Ｋｓ３ｊを作成する。

【００９５】

図１０は、２つの秘密鍵の相関値ρを演算する概念図である。秘密鍵６０と秘密鍵７０との相関値ρを演算するとき、秘密鍵６０を構成する各ビットを順番に抽出し、その抽出したビットに対応する秘密鍵７０の各ビットを順番に抽出する。そして、対応する２つのビットを比較し、２つのビットが一致するとき「１」を加算し、２つのビットが不一致であるとき「０」を加算して和を演算する。和の演算後、その和をサンプル数で除算して加算平均を演算する。そして、この加算平均を秘密鍵６０と秘密鍵７０との相関値ρとする。

【００９６】

具体的には、秘密鍵６０の最初のビットである「０」と秘密鍵７０の最初のビットである「０」とを抽出し、両者が一致しているので、「１」を加算し、次に、秘密鍵６０のビット「１」と秘密鍵７０のビット「１」とを抽出し、両者が一致しているので「１」を加算して和「２」を演算する。

【００９７】

その後、秘密鍵６０のビット「１」と秘密鍵７０のビット「０」とを抽出し、両者が不一致であるので、「０」を加算して和「２」を演算する。以下、同様にして和を演算して加算平均を演算する。

【００９８】

制御電圧パターンが制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊに従って変えられるとき、無線装置１０，３０においてそれぞれ秘密鍵Ｋｓ１１～Ｋｓ１ｊ，Ｋｓ２１～Ｋｓ２ｊが生成され、盗聴装置５０において秘密鍵Ｋｓ３１～Ｋｓ３ｊが生成される。

【００９９】

秘密鍵Ｋｓ１１～Ｋｓ１ｊは、秘密鍵Ｋｓ２１～Ｋｓ２ｊと同じであるので、例えば、秘密鍵Ｋｓ２１～Ｋｓ２ｊと秘密鍵Ｋｓ３１～Ｋｓ３ｊとの相関値ρ１～ρｊを上述した方法によって演算する。

【０１００】

そして、相関値ρ１～ρｊから最小値ρｍｉｎを検出し、最小値ρｍｉｎが得られるときの制御電圧パターンを制御電圧パターンＰ１～Ｐｎとして決定する。例えば、図９に示す制御電圧パターンＰ１２～Ｐｎ２のときに最小値ρｍｉｎが得られたとすると、制御電圧パターンＰ１２～Ｐｎ２を制御電圧パターンＰ１～Ｐｎとして決定する。

【０１０１】

図３に示す無線装置３０の指向性設定部２３０は、図９に示す制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊを保持しており、制御電圧パターンＰ１～Ｐｎを決定する場合、制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊに従ってアレーアンテナ２０（アンテナ部２２０）の指向性パターンを順次変える。

【０１０２】

また、図３に示す無線装置３０の鍵相関処理部２５０も、制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊを保持しており、制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊの順番に従って秘密鍵Ｋｓ２１～Ｋｓ２ｊが鍵作成部１６０から順次入力され、制御電圧パターンＰ１１～Ｐｎ１；Ｐ１２～Ｐｎ２；・・・；Ｐ１ｊ～Ｐｎｊの順番に従って秘密鍵Ｋｓ３１～Ｋｓ３ｊが鍵受信部２４０から順次入力されることを認識する。

【０１０３】

そして、鍵相関処理部２５０は、秘密鍵Ｋｓ２１及びＫｓ３１を受けると、秘密鍵Ｋｓ２１と秘密鍵Ｋｓ３１との相関値ρ１を上述した方法によって演算し、記憶する。鍵相関処理部２５０は、相関値ρ１～ρｊの全てを演算すると、相関値ρ１～ρｊから最小値ρｍｉｎを検出し、その最小値ρｍｉｎが得られたときの制御電圧パターンＰ１～Ｐｎを検出する。最小値ρｍｉｎが秘密鍵Ｋｓ２２と秘密鍵Ｋｓ３２との相関値であるならば、鍵相関処理部２５０は、最小値ρｍｉｎが得られたときの制御電圧パターンＰ１～Ｐｎとして制御電圧パターンＰ１２～Ｐｎ２を検出する。

【０１０４】

そして、鍵相関処理部２５０は、制御電圧パターンＰ１２～Ｐｎ２が制御電圧パターンＰ１～Ｐｎであることを示す信号ＰＴＭを生成して指向性設定部２３０へ出力する。指向性設定部２３０は、無線装置１０と無線装置３０との通信においては、制御電圧パターンＰ１２～Ｐｎ２に従ってアレーアンテナ２０（アンテナ部２２０）の指向性を順次変える。これにより、無線装置１０，３０は、秘密鍵Ｋｓ３との相関値ρが最小である秘密鍵Ｋｓ１，Ｋｓ２を作成し、その作成した秘密鍵Ｋｓ１，Ｋｓ２を用いて相互にデータを無線通信する。

【０１０５】

図１１は、盗聴装置５０において作成される秘密鍵Ｋｓ３との相関値が最小である秘密鍵Ｋｓ１，Ｋｓ２を無線装置１０，３０において作成するためのアレーアンテナ２０の指向性パターンを決定する動作を説明するためのフローチャートである。

【０１０６】

一連の動作が開始されると、無線装置３０の送信処理部１２０は、ｋ＝１，ｒ＝１，ｐ＝１を設定する（ステップＳ１）。なお、ｋは、指向性パターンの個数を表し、ｒは、変化させる制御電圧パターンの個数を表し、ｐは、無線装置３０を移動させる位置数を表す

。そして、ｋは、１～ｎの範囲の自然数であり、ｒは、１～ｊの範囲の自然数であり、ｐは、１～ｍの範囲の自然数である。

【０１０７】

ステップＳ１の後、無線装置３０の指向性設定部２３０は、制御電圧パターンＰ１１～Ｐｎ１のパターンＰ１１からなる電圧Ｖ１～Ｖ６をバラクタダイオード２３２へ出力し、アレーアンテナ２０（アンテナ部２２０）の指向性を指向性Ｄ１１１に設定する（ステップＳ２）。そして、無線装置１０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アンテナ１１を介して無線装置３０へ所定の信号を構成する電波を送信する（ステップＳ３）。無線装置３０のアレーアンテナ２０は、ステップＳ２において設定された指向性Ｄ１１１で電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アレーアンテナ２０から受けた電波の強度Ｉ１ｋｒを検出する（ステップＳ４）。

【０１０８】

その後、無線装置３０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アレーアンテナ２０を介して無線装置１０及び盗聴装置５０へ所定の信号を構成する電波を送信する（ステップＳ５）。無線装置１０において、アンテナ１１は、無線装置３０からの電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ１１から受けた電波の強度Ｉ２ｋｒを検出する（ステップＳ６）。また、盗聴装置５０において、アンテナ５１は、無線装置３０からの電波を受信し、その受信した電波をプロファイル生成部３２０へ出力する（図５参照）。プロファイル生成部３２０は、アンテナ５１から受信した電波の強度Ｉ３ｋｒを検出する（ステップＳ７）。

【０１０９】

その後、無線装置３０の送信処理部１２０は、ｋ＝ｎであるか否かを判定し（ステップＳ８）、ｋ＝ｎでないとき、ｋ＝ｋ＋１を設定する（ステップＳ９）。そして、ステップＳ８において、ｋ＝ｎであると判定されるまで、ステップＳ２～ステップＳ９が繰り返し実行される。

【０１１０】

これにより、無線装置３０のプロファイル生成部１５０は、複数の強度Ｉ１１ｒ～Ｉ１ｎｒを検出し、無線装置１０のプロファイル生成部１５０は、複数の強度Ｉ２１ｒ～Ｉ２ｎｒを検出し、盗聴装置５０のプロファイル生成部３２０は、複数の強度Ｉ３１ｒ～Ｉ３ｎｒを検出する。即ち、無線装置３０及び盗聴装置５０は、図９に示す制御電圧パターンＰ１１～Ｐｎ１に対応して、それぞれ、複数の強度Ｉ２１ｒ～Ｉ２ｎｒ及び複数の強度Ｉ３１ｒ～Ｉ３ｎｒを検出する。

【０１１１】

ステップＳ８において、ｋ＝ｎであると判定されると、無線装置３０の鍵作成部１６０は、プロファイル生成部１５０から複数の強度Ｉ１１ｒ～Ｉ１ｎｒを受け、その受けた複数の強度Ｉ１１ｒ～Ｉ１ｎｒから中央値を検出する。そして、鍵作成部１６０は、複数の強度Ｉ１１ｒ～Ｉ１ｎｒを中央値によってデジタル化して秘密鍵Ｋｓ２ｒｐを作成する（ステップＳ１０）。即ち、無線装置３０は、図９に示す受信信号プロファイルＲＳＳ１１に対応して秘密鍵Ｋｓ２ｒｐを作成する。

【０１１２】

そして、盗聴装置５０の鍵作成部３３０は、プロファイル生成部３２０から複数の強度Ｉ３１ｒ～Ｉ３ｎｒを受け、その受けた複数の強度Ｉ３１ｒ～Ｉ３ｎｒから中央値を検出する。そして、鍵作成部３３０は、複数の強度Ｉ３１ｒ～Ｉ３ｎｒを中央値によってデジタル化して秘密鍵Ｋｓ３ｒｐを作成する（ステップＳ１１）。即ち、盗聴装置５０は、図９に示す受信信号プロファイルＲＳＳ１３に対応して秘密鍵Ｋｓ３ｒｐを作成する。

【０１１３】

その後、無線装置３０の送信処理部１２０は、ｒ＝ｊであるか否かを判定し（ステップ

Ｓ１２）、ｒ＝ｊでないとき、ｒ＝ｒ＋１を設定する（ステップＳ１３）。そして、ステップＳ１２において、ｒ＝ｊであると判定されるまで、ステップＳ２～ステップＳ１３が繰り返し実行される。

【０１１４】

これにより、無線装置３０の鍵作成部１６０は、複数の秘密鍵Ｋｓ１１ｐ～Ｋｓ１ｊｐを作成し、盗聴装置５０の鍵作成部３３０は、複数の秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐを作成する。即ち、無線装置３０は、図９に示す受信信号プロファイルＲＳＳＩ１１～ＲＳＳＩｊ１に対応して複数の秘密鍵Ｋｓ１１ｐ～Ｋｓ１ｊｐを作成し、盗聴装置５０は、図９に示す受信信号プロファイルＲＳＳＩ１３～ＲＳＳＩｊ３に対応して複数の秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐを作成する。

【０１１５】

そして、ステップＳ１２において、ｒ＝ｊであると判定されると、盗聴装置５０の鍵作成部３３０は、作成した秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐを鍵送信部３４０へ出力する。鍵送信部３４０は、秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐに対して上述した送信系の処理を施し、アンテナ５１（アンテナ部３１０）を介して秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐを無線装置３０へ送信する（ステップＳ１４）。無線装置３０のアンテナ１１（アンテナ部２２０）は、盗聴装置５０から秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐを受信し（ステップＳ１５）、その受信した秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐを鍵受信部２４０へ出力する。そして、鍵受信部２４０は、アンテナ１１（アンテナ部２２０）から受けた秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐを鍵相関処理部２５０へ出力する。

【０１１６】

その後、無線装置３０の鍵相関処理部２５０は、ステップＳ１０において作成された秘密鍵Ｋｓ１１ｐ～Ｋｓ１ｊｐを鍵作成部１６０から受け、その受けた秘密鍵Ｋｓ１１ｐ～Ｋｓ１ｊｐと鍵受信部２４０からの秘密鍵Ｋｓ３１ｐ～Ｋｓ３ｊｐとの相関値ρ１～ρｊを上述した方法によって演算し、その演算した相関値ρ１～ρｊから最小値ρｍｉｎを検出する。鍵相関処理部２５０は、最小値ρｍｉｎを検出すると、最小値ρｍｉｎが得られたときの制御電圧パターンＰ１１ｍｉｎ～Ｐ１ｎｍｉｎを上述した方法により抽出する。そして、鍵相関処理部２５０は、抽出した制御電圧パターンＰ１１ｍｉｎ～Ｐ１ｎｍｉｎが制御電圧パターンＰ１ｏｐｔ～Ｐｎｏｐｔであることを示す信号ＰＴＭを生成して指向性設定部２３０へ出力する。これにより、無線装置３０は、最小値ρｍｉｎが得られたときの指向性パターンＤｐを抽出する（ステップＳ１７）。

【０１１７】

その後、無線装置３０の送信処理部１２０は、ｐ＝ｍであるか否かを判定し（ステップＳ１８）、ｐ＝ｍでないとき、ｐ＝ｐ＋１を設定する（ステップＳ１９）。そして、ステップＳ１８において、ｐ＝ｍであると判定されるまで、ステップＳ２～ステップＳ１９が繰り返し実行される。

【０１１８】

これにより、無線装置３０は、ｍ個の指向性パターンＤ１～Ｄｍを抽出する。そして、ステップＳ１８において、ｐ＝ｍであると判定されると、指向性パターンＤ１～Ｄｍから相関値ρが最小となる指向性パターンＤｏｐｔを抽出する（ステップＳ２０）。無線装置３０は、抽出した指向性パターンＤｏｐｔを指向性設定部２３０により保持する。これにより、一連の動作は終了する。

【０１１９】

図１１に示すフローチャートにおいては、無線装置３０の配置位置をｍ個の位置に変化させ、その変化させた各位置において、無線装置３０に装着されたアレーアンテナ２０の指向性パターンＤｋｒｐを図９に示す制御電圧パターンＰ１１～Ｐｎ１，Ｐ１２～Ｐｎ２，・・・，Ｐ１ｊ～Ｐｎｊに従って変化させて、秘密鍵Ｋｓ１１１～Ｋｓ１ｊ１，Ｋｓ１１２～Ｋｓ１ｊ２，・・・，Ｋｓ１１ｍ～Ｋｓ１ｊｍと、秘密鍵Ｋｓ３１１～Ｋｓ３ｊ１，Ｋｓ３１２～Ｋｓ３ｊ２，・・・，Ｋｓ３１ｍ～Ｋｓ３ｊｍとの相関値が最小となる指向性パターンＤｏｐｔを抽出する。

【０１２０】
従って、図１１に示すフローチャートに従って抽出された指向性パターンＤｏｐｔは、盗聴装置５０が無線装置１０，３０に対してどのような位置に配置されていても、無線装置１０，３０において作成された秘密鍵Ｋｓ１，Ｋｓ２は、盗聴装置５０において作成された秘密鍵Ｋｓ３との相関値ρが最小となる秘密鍵である。即ち、秘密鍵Ｋｓ１，Ｋｓ２は、秘密鍵Ｋｓ３と異なる。
【０１２１】
なお、秘密鍵Ｋｓ３との相関値が最小となる秘密鍵Ｋｓ１を作成する動作は、実際には、無線装置１０，３０に搭載されたＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）によって行なわれ、無線装置３０のＣＰＵは、図１１に示す各ステップＳ１，Ｓ２，Ｓ４，Ｓ５，Ｓ８，Ｓ９，Ｓ１０，Ｓ１２，Ｓ１３，Ｓ１５～Ｓ２０を備えるプログラムをＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）から読出し、無線装置１０のＣＰＵは、図１１に示すステップＳ３，Ｓ６を備えるプログラムをＲＯＭから読出し、盗聴装置５０のＣＰＵは、図１１に示す各ステップＳ７，Ｓ１１，Ｓ１４を備えるプログラムをＲＯＭから読出し、無線装置１０，３０及び盗聴装置５０に搭載された３つのＣＰＵは、その読出したプログラムを実行して図１１に示すフローチャートに従って秘密鍵Ｋｓ３との相関値が最小となる秘密鍵Ｋｓ１を作成する。
【０１２２】
従って、ＲＯＭは、秘密鍵Ｋｓ３との相関値が最小となる秘密鍵Ｋｓ１を作成する動作をコンピュータ（ＣＰＵ）に実行させるためのプログラムを記録したコンピュータ（ＣＰＵ）読取り可能な記録媒体に相当する。
【０１２３】
そして、図１１に示す各ステップを備えるプログラムは、秘密鍵Ｋｓ３との相関値が最小となる秘密鍵Ｋｓ１の作成をコンピュータ（ＣＰＵ）に実行させるプログラムである。
【０１２４】
図１１に示すフローチャートに従って秘密鍵Ｋｓ２，Ｋｓ３の作成をシミュレートした例について説明する。図１２は、シミュレーションに用いた無線装置１０，３０及び盗聴装置５０の平面配置図である。シミュレーションに用いられた部屋８０は、縦が８ｍであり、横幅が１０ｍであり、周囲が壁８１によって囲まれた部屋である。部屋８０における各位置は、Ｘ軸－Ｙ軸からなる直交座標によって表わされる。
【０１２５】
アレーアンテナ２０を装着した無線装置３０は、部屋８０の中心（Ｘ－Ｙ座標の原点）に配置され、無線装置１０は、座標［３，１］に配置され、盗聴装置５０は、座標［２，－１］に配置された。
【０１２６】
また、シミュレーションに用いられた鍵長は、１２８ビットである。即ち、図１１に示すフローチャートにおいてｎ＝１２８に設定された。
【０１２７】
図１３は、無線装置１０における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ１と盗聴装置５０における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ３とを示す図である。なお、図１３の（ａ）及び（ｂ）において、横軸は、測定回数を表わし、縦軸は、受信した電波の強度を表わす。
【０１２８】
図１３の（ａ）は、無線装置１０のプロファイル生成部１５０によって生成された受信信号プロファイルＲＳＳＩ１１を表わし、図１３の（ｂ）は、盗聴装置５０のプロファイル生成部３２０によって生成された受信信号プロファイルＲＳＳＩ１３を表わす。また、図１３の（ｃ）は、無線装置１０の鍵作成部１６０によって受信信号プロファイルＲＳＳＩ１１に基づいて作成された秘密鍵Ｋｓ１を表わし、図１３の（ｄ）は、盗聴装置５０の鍵作成部３３０によって受信信号プロファイルＲＳＳＩ１３に基づいて作成された秘密鍵Ｋｓ３を表わす。

【０１２９】
図１４は、無線装置３０のアレーアンテナ２０から出射されるビームパターンであり、図１３の（ａ）及び（ｂ）に示す受信信号プロファイルＲＳＳＩ１１，ＲＳＳＩ１３は、この図１４に示すビームパターンからなるビームを用いて測定された。
【０１３０】
受信信号プロファイルＲＳＳＩ１１と受信信号プロファイルＲＳＳＩ１３との相関値は、“０．７７”であり、無線装置１０は、盗聴装置５０における受信信号プロファイルＲＳＳＩ１３と異なる受信信号プロファイルＲＳＳＩ１１の電波を受信している。
【０１３１】
この発明においては、２つの受信信号プロファイルＲＳＳＩＡ，ＲＳＳＩＢの相関値ρ_{RSSI}は、次式により演算される。
【０１３２】
ρ_{RSSI}＝＜RSSIA＞・＜RSSIB＞／（｜＜RSSIA＞｜×｜RSSIB＞｜）・・・（１）
なお、＜ＲＳＳＩＡ＞及び＜ＲＳＳＩＢ＞は、それぞれ、受信信号プロファイルＲＳＳＩＡ，ＲＳＳＩＢを構成する複数の強度を要素とするベクトルを表す。
【０１３３】
従って、受信信号プロファイルＲＳＳＩ１１と受信信号プロファイルＲＳＳＩ１３との相関値を演算する場合、受信信号プロファイルＲＳＳＩ１１，ＲＳＳＩ１３をそれぞれ式（１）の＜ＲＳＳＩＡ＞及び＜ＲＳＳＩＢ＞に代入して相関値を演算する。このようにして得られた相関値が”０．７７”である。
【０１３４】
このように、受信信号プロファイルＲＳＳＩ１１と受信信号プロファイルＲＳＳＩ１３との相関値は、“０．７７”であり、受信信号プロファイルＲＳＳＩ１１は、受信信号プロファイルＲＳＳＩ１３と相関性が低いが、無線装置１０において作成された秘密鍵Ｋｓ１と盗聴装置５０において作成された秘密鍵Ｋｓ３との相関値は、“１”であり、２つの秘密鍵Ｋｓ１，Ｋｓ３は一致する。従って、２つの受信信号プロファイルが相互に異なる場合でも、２つの受信信号プロファイルからそれぞれ生成された２つの秘密鍵は一致する場合もある。
【０１３５】
図１５は、ランダムビームが用いられたときの無線装置１０及び盗聴装置５０における受信信号プロファイルを示す図であり、図１５の（ａ）は、無線装置１０のプロファイル生成部１５０によって生成された受信信号プロファイルＲＳＳＩ２１を表わし、図１５の（ｂ）は、盗聴装置５０のプロファイル生成部３２０によって生成された受信信号プロファイルＲＳＳＩ２３を表わす。
【０１３６】
式（１）を用いて演算された受信信号プロファイルＲＳＳＩ２１と受信信号プロファイルＲＳＳＩ２３との相関値は、“０．５”であり、受信信号プロファイルＲＳＳＩ２１を中央値によってデジタル化して作成した秘密鍵Ｋｓ１と受信信号プロファイルプロファイルＲＳＳＩ２３を中央値によってデジタル化して作成した秘密鍵Ｋｓ３との相関値は、“０．４３”である。
【０１３７】
このように、無線装置３０のアレーアンテナ２０から出射されるビームのパターンをランダムなパターンにすることによって、秘密鍵Ｋｓ１と秘密鍵Ｋｓ３との相関値を“１”から“０．４３”へ大幅に低下させることができる。
【０１３８】
従って、秘密鍵Ｋｓ３との相関値が最小になる秘密鍵Ｋｓ１，Ｋｓ２を作成するためには、好ましくは、ランダムビームが用いられる。
【０１３９】
図１６は、マルチビームのパターンである。また、図１７は、図１６に示すマルチビームを用いた場合の無線装置１０及び盗聴装置５０における受信信号プロファイルを示す図

であり、図１７の（ａ）は、無線装置１０のプロファイル生成部１５０によって生成された受信信号プロファイルＲＳＳＩ３１を表わし、図１７の（ｂ）は、盗聴装置５０のプロファイル生成部３２０によって生成された受信信号プロファイルＲＳＳＩ３３を表わす。

【０１４０】

式（１）を用いて演算された受信信号プロファイルＲＳＳＩ３１と受信信号プロファイルＲＳＳＩ３３との相関値は、“０．１２”であり、受信信号プロファイルＲＳＳＩ３１を中央値によってデジタル化して作成した秘密鍵Ｋｓ１と受信信号プロファイルプロファイルＲＳＳＩ３３を中央値によってデジタル化して作成した秘密鍵Ｋｓ３との相関値は、“０．１１”である。

【０１４１】

このように、無線装置３０のアレーアンテナ２０から出射されるビームのパターンを図１６に示すマルチビームのパターンにすることによって、秘密鍵Ｋｓ１と秘密鍵Ｋｓ３との相関値を“１”から“０．１１”へ大幅に低下させることができる。

【０１４２】

従って、秘密鍵Ｋｓ３との相関値が最小になる秘密鍵Ｋｓ１，Ｋｓ２を作成するためには、より好ましくは、マルチビームが用いられる。

【０１４３】

図１８は、シミュレーションに用いた無線装置１０，３０及び盗聴装置５０の他の平面配置図である。盗聴装置５０は、座標［３．１１，１．０４］に配置された。即ち、盗聴装置５０は、無線装置１０の近傍に配置される。なお、無線装置１０，３０の配置位置は、図１２に示す配置位置と同じである。

【０１４４】

図１９は、図１８に示す配置位置において、無線装置１０における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ１と盗聴装置５０における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ３とを示す図であり、図１９の（ａ）は、無線装置１０のプロファイル生成部１５０によって生成された受信信号プロファイルＲＳＳＩ４１を表わし、図１９の（ｂ）は、盗聴装置５０のプロファイル生成部３２０によって生成された受信信号プロファイルＲＳＳＩ４３を表わす。また、図１９の（ｃ）は、無線装置１０の鍵作成部１６０によって受信信号プロファイルＲＳＳＩ４１に基づいて作成された秘密鍵Ｋｓ１を表わし、図１９の（ｄ）は、盗聴装置５０の鍵作成部３３０によって受信信号プロファイルＲＳＳＩ４３に基づいて作成された秘密鍵Ｋｓ３を表わす。

【０１４５】

式（１）を用いて演算された受信信号プロファイルＲＳＳＩ４１と受信信号プロファイルＲＳＳＩ４３との相関値は、“０．９３”であり、無線装置１０において作成された秘密鍵Ｋｓ１と盗聴装置５０において作成された秘密鍵Ｋｓ３との相関値は、“０．６５”である。

【０１４６】

従って、盗聴装置５０が正規のユーザである無線装置１０の極く近傍（約１２ｃｍ：１波長に相当する距離）に存在していても、秘密鍵Ｋｓ３との相関値が小さい秘密鍵Ｋｓ１を作成することができる。

【０１４７】

図２０は、無線装置１０において作成された秘密鍵Ｋｓ１と盗聴装置５０において作成された秘密鍵Ｋｓ３とを示す図である。図２０の（ａ）は、図１３の（ａ）に示す受信受信プロファイルＲＳＳＩ１１を４値化処理して作成した秘密鍵Ｋｓ１を表し、図２０の（ｂ）は、図１３の（ｂ）に示す受信信号プロファイルＲＳＳＩ１３を４値化処理して作成した秘密鍵Ｋｓ３を表わす。

【０１４８】

図２０に示す秘密鍵Ｋｓ１と秘密鍵Ｋｓ３との相関値は、“０．６３”である。従って、受信信号プロファイルＲＳＳＩ１１，ＲＳＳＩ１３を４値化処理することにより、秘密鍵Ｋｓ１と秘密鍵Ｋｓ３との相関値は、“１”から“０．６３”に小さくできる。

【０１４９】
この発明においては、鍵作成部１６０は、プロファイル作成部１５０から受けた受信信号プロファイルを複数の基準値によって多値化して秘密鍵Ｋｓ１，Ｋｓ２を作成してもよい。
【０１５０】
上述したように、この発明においては、図１１に示すフローチャートに従って制御電圧パターンＰ１ｏｐｔ～Ｐｎｏｐｔを決定すれば、秘密鍵Ｋｓ３との相関値が最小である秘密鍵Ｋｓ１、Ｋｓ２を作成できるが、図１１に示すフローチャートを実行しても、秘密鍵Ｋｓ３との相関値が最小である秘密鍵Ｋｓ１、Ｋｓ２を作成できない場合、上述したように、ビームパターンをマルチビームパターン（図１６参照）またはランダムパターンに変えて図１１に示すフローチャートを実行してもよく、鍵作成部１６０において受信信号プロファイルＲＳＳＩを多値化処理するようにしてもよい。
【０１５１】
これにより、秘密鍵Ｋｓ３との相関値が最小である秘密鍵Ｋｓ１、Ｋｓ２をより正確に作成できる。
【０１５２】
図２１は、図１に示す２つの無線装置１０，３０間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置３０の送信処理部１２０は、ｋ＝１を設定する（ステップＳ３１）。そして、指向性設定部２３０は、パターンＰ１によりアレーアンテナ２０の指向性を１つの指向性Ｄｋｏｐｔに設定する（ステップＳ３２）。即ち、指向性設定部２３０は、図１１に示すフローチャートに従って決定された指向性パターンＤｏｐｔの最初の指向性にアレーアンテナ２０の指向性を設定する。
【０１５３】
その後、無線装置１０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アンテナ１１を介して無線装置３０へ所定の信号を構成する電波を送信する（ステップＳ３３）。
【０１５４】
無線装置３０において、アレーアンテナ２０は、無線装置１０からの電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アレーアンテナ２０から受けた電波の強度Ｉ１ｋを検出する（ステップＳ３４）。
【０１５５】
その後、無線装置３０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アレーアンテナ２０を介して無線装置１０へ所定の信号を構成する電波を送信する（ステップＳ３５）。
【０１５６】
無線装置１０において、アンテナ１１は、無線装置３０からの電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ１１から受けた電波の強度Ｉ２ｋを検出する（ステップＳ３６）。
【０１５７】
その後、無線装置３０の送信処理部１２０は、ｋ＝ｎであるか否かを判定する（ステップＳ３７）。そして、ｋ＝ｎでないとき、送信処理部１２０は、ｋ＝ｋ＋１を設定し（ステップＳ３８）、ステップＳ３２～Ｓ３８が繰返し実行される。即ち、アレーアンテナ２０の指向性がパターンＰ１～Ｐｎによってｎ個に変えられて、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間で所定の信号を構成する電波が送受信され、強度Ｉ１１～Ｉ１ｎ及びＩ２１～Ｉ２ｎが検出されるまで、ステップＳ３２～Ｓ３８が繰返し実行される。
【０１５８】
ステップＳ３７において、ｋ＝ｎであると判定されると、無線装置３０において、プロファイル生成部１５０は、強度Ｉ１１～Ｉ１ｎから受信信号プロファイルＲＳＳＩ１を作成して鍵作成部１６０へ出力する。

【０１５９】
鍵作成部１６０は、受信信号プロファイルＲＳＳＩ１から中央値ＷＩｃｅｎｔ１を検出し、その検出した中央値ＷＩｃｅｎｔ１によって受信信号プロファイルＲＳＳＩ１をデジタル化し、強度Ｉ１１～Ｉ１ｎを２値化する。そして、鍵作成部１６０は、２値化した各値をビットパターンとする秘密鍵Ｋｓ２を生成する（ステップＳ３９）。
【０１６０】
また、無線装置１０のプロファイル生成部１５０は、強度Ｉ２１～Ｉ２ｎから受信信号プロファイルＲＳＳＩ２を作成して鍵作成部１６０へ出力する。鍵作成部１６０は、受信信号プロファイルＲＳＳＩ２から中央値ＷＩｃｅｎｔ２を検出し、その検出した中央値ＷＩｃｅｎｔ２によって受信信号プロファイルＲＳＳＩ２をデジタル化し、強度Ｉ２１～Ｉ２ｎを２値化する。そして、鍵作成部１６０は、２値化した各値をビットパターンとする秘密鍵Ｋｓ１を生成する（ステップＳ４０）。
【０１６１】
その後、無線装置１０において、鍵作成部１６０は、秘密鍵Ｋｓ１を鍵一致確認部１７０へ出力する。鍵一致確認部１７０のデータ発生部１７１は、上述した方法によって鍵確認用データＤＣＦＭ１を発生して送信処理部１２０及びデータ比較部１７２へ出力する。送信処理部１２０は、鍵確認用データＤＣＦＭ１に変調等の処理を施し、アンテナ部１３０を介して無線装置３０へ鍵確認用データＤＣＦＭ１を送信する。
【０１６２】
そして、アンテナ部１３０は、無線装置３０において発生された鍵確認用データＤＣＦＭ２を無線装置３０から受信し、その受信した鍵確認用データＤＣＦＭ２を受信処理部１４０へ出力する。受信処理部１４０は、鍵確認用データＤＣＦＭ２に所定の処理を施し、鍵一致確認部１７０のデータ比較部１７２へ鍵確認用データＤＣＦＭ２を出力する。
【０１６３】
データ比較部１７２は、データ発生部１７１からの鍵確認用データＤＣＦＭ１を受信処理部１４０からの鍵確認用データＤＣＦＭ２と比較する。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致しているとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。結果処理部１７３は、一致信号ＭＴＨに応じて、鍵作成部１６０からの秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。
【０１６４】
一方、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、データ比較部１７２は、不一致信号ＮＭＴＨを生成して送信処理部１２０及び鍵一致化部１９０へ出力する。送信処理部１２０は、不一致信号ＮＭＴＨをアンテナ部１３０を介して無線装置３０へ送信する。そして、無線装置３０は、無線装置１０において秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたことを検知する。
【０１６５】
これにより、無線装置１０における鍵一致の確認が終了する（ステップＳ４１）。
【０１６６】
無線装置３０においても、無線装置１０と同じ動作によって鍵一致の確認が行なわれる（ステップＳ４２）。
【０１６７】
ステップＳ４１において、秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたとき、無線装置１０において、鍵一致化部１９０の擬似シンドローム作成部１９１は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受ける。そして、擬似シンドローム作成部１９１は、不一致信号ＮＭＴＨに応じて、鍵作成部１６０から受けた秘密鍵Ｋｓ１のビットパターンx_1を検出し、その検出したビットパターンx_1のシンドローム$s1 = x_1 H^T$を演算する。
【０１６８】
擬似シンドローム作成部１９１は、演算したシンドローム$s1 = x_1 H^T$を不一致ビット検出部１９２へ出力し、ビットパターンx_1を鍵不一致訂正部１９３へ出力する。
【０１６９】

一方、無線装置３０は、ステップＳ１１において無線装置１０から不一致信号ＮＭＴＨを受信し、その受信した不一致信号ＮＭＴＨに応じて、シンドロームｓ２＝ｘ$_2$Ｈ^{T}を演算して無線装置１０へ送信する。

【０１７０】

無線装置１０のアンテナ部１３０は、無線装置３０からシンドロームｓ２＝ｘ$_2$Ｈ^{T}を受信して受信処理部１４０へ出力する。受信処理部１４０は、シンドロームｓ２＝ｘ$_2$Ｈ^{T}に対して所定の処理を施し、シンドロームｓ２＝ｘ$_2$Ｈ^{T}を鍵一致化部１９０へ出力する。

【０１７１】

鍵一致化部１９０の不一致ビット検出部１９２は、受信処理部１４０から無線装置３０において作成されたシンドロームｓ２＝ｘ$_2$Ｈ^{T}を受ける。そして、不一致ビット検出部１９２は、無線装置１０で作成されたシンドロームｓ１＝ｘ$_1$Ｈ^{T}と無線装置３０において作成されたシンドロームｓ２＝ｘ$_2$Ｈ^{T}との差分ｓ＝ｓ１－ｓ２を演算する。

【０１７２】

その後、不一致ビット検出部１９２は、ｓ≠０であることを確認し、鍵不一致のビットパターンｅ＝ｘ$_1$－ｘ$_2$をｓ＝ｅＨ^{T}に基づいて演算し、その演算した鍵不一致のビットパターンｅを鍵不一致訂正部１９３へ出力する。

【０１７３】

鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からのビットパターンｘ$_1$と、不一致ビット検出部１９２からの鍵不一致のビットパターンｅとに基づいて、無線装置３０において作成された秘密鍵Ｋｓ２のビットパターンｘ$_2$＝ｘ$_1$－ｅを演算する。

【０１７４】

そして、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における鍵一致確認の動作と同じ動作によって、一致化された鍵ｘ$_2$＝ｘ$_1$－ｅの一致を確認する。

【０１７５】

これにより、鍵不一致対策が終了する（ステップＳ４３）。

【０１７６】

無線装置３０においても、無線装置１０と同じ動作によって鍵不一致対策が行なわれる（ステップＳ４４）。

【０１７７】

ステップＳ１１において、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することが確認されたとき、またはステップＳ４３において鍵不一致対策がなされたとき、暗号部２００は、鍵記憶部１８０から秘密鍵Ｋｓ１を読出して送信データを暗号化し、暗号化した送信データを送信処理部１２０へ出力する。そして、送信処理部１２０は、暗号化された送信データに変調等を施し、アンテナ部１３０を介して暗号化された送信データを無線装置３０へ送信する。

【０１７８】

また、アンテナ部１３０は、暗号化された送信データを無線装置３０から受信し、その受信した暗号化された送信データを受信処理部１４０へ出力する。受信処理部１４０は、暗号化された送信データに所定の処理を施し、暗号化された送信データを復号部２１０へ出力する。

【０１７９】

復号部２１０は、受信処理部１４０からの暗号化された送信データを復号して受信データを取得する。

【０１８０】

これにより、秘密鍵Ｋｓ１による暗号・復号が終了する（ステップＳ４５）。

【０１８１】

無線装置３０においても、無線装置１０と同じ動作によって秘密鍵Ｋｓ２による暗号・復号が行なわれる（ステップＳ４６）。そして、一連の動作が終了する。

【０１８２】
上述したステップＳ３３，Ｓ３４に示す動作は、無線装置３０において受信信号プロファイルＲＳＳＩ１を生成するための電波を無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ送信し、かつ、無線装置３０において電波の強度Ｉ１ｋを検出する動作であり、ステップＳ３５，Ｓ３６に示す動作は、無線装置１０において受信信号プロファイルＲＳＳＩ２を生成するための電波を無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、かつ、無線装置１０において電波の強度Ｉ２ｋを検出する動作である。そして、所定の信号を構成する電波の無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０への送信及び所定の信号を構成する電波の無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１への送信は、アレーアンテナ２０の指向性を１つの指向性に設定して交互に行なわれる。つまり、所定の信号を構成する電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間で時分割復信（ＴＤＤ）等により送受信される。

【０１８３】
従って、アレーアンテナ２０の指向性を１つの指向性に設定して無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ所定の信号を構成する電波を送信し、無線装置３０において電波の強度Ｉ１ｋを検出した直後に、同じ所定の信号を構成する電波を無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、無線装置１０において電波の強度Ｉ２ｋを検出することができる。その結果、無線装置１０，３０間において同じ伝送路特性を確保して所定の信号を構成する電波を無線装置１０，３０間で送受信でき、電波の可逆性により電波の強度Ｉ１１～Ｉ１ｎをそれぞれ電波の強度Ｉ２１～Ｉ２ｎに一致させることができる。そして、無線装置１０において作成される秘密鍵Ｋｓ１を無線装置３０において作成される秘密鍵Ｋｓ２に容易に一致させることができる。

【０１８４】
また、所定の信号を構成する電波は、無線装置１０，３０間で時分割復信（ＴＤＤ）等により送受信されるので、電波の干渉を抑制して１つのアレーアンテナ２０を介して所定の信号を構成する電波を無線装置１０，３０間で送受信できる。

【０１８５】
更に、鍵確認用データＤＣＦＭ１～４は、秘密鍵Ｋｓ１，Ｋｓ２に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データＤＣＦＭ１～４が盗聴されても秘密鍵Ｋｓ１，Ｋｓ２が解読される危険性を極めて低くできる。

【０１８６】
更に、シンドロームｓ１，ｓ２は、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンを示す鍵x_1，x_2に検査行列Ｈの転置行列H^Tを乗算して得られるので、シンドロームｓ１，ｓ２が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

【０１８７】
なお、無線装置１０，３０間で通信を行なう動作は、実際には、ＣＰＵによって行なわれ、無線装置１０に搭載されたＣＰＵは、図２１に示す各ステップＳ３３，Ｓ３６，Ｓ４０，Ｓ４１，Ｓ４３，Ｓ４５を備えるプログラムをＲＯＭから読出し、無線装置３０に搭載されたＣＰＵは、図２１に示す各ステップＳ３１，Ｓ３２，Ｓ３４，Ｓ３５，Ｓ３７，Ｓ３８，Ｓ３９，Ｓ４２，Ｓ４４，Ｓ４６を備えるプログラムをＲＯＭから読出し、無線装置１０，３０に搭載された２つのＣＰＵは、その読出したプログラムを実行して図２１に示すフローチャートに従って無線装置１０，３０間で通信を行なう。

【０１８８】
従って、ＲＯＭは、無線装置１０，３０間で通信を行なう動作をコンピュータ（ＣＰＵ）に実行させるためのプログラムを記録したコンピュータ（ＣＰＵ）読取り可能な記録媒体に相当する。

【０１８９】

そして、図２１に示す各ステップを備えるプログラムは、アレーアンテナ２０の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置１０，３０間における通信をコンピュータ（ＣＰＵ）に実行させるプログラムである。

【０１９０】

上記においては、電気的に指向性を切換え可能なアレーアンテナ２０を無線装置３０のみに装着すると説明したが、この発明においては、アレーアンテナ２０は、無線装置１０及び３０の両方に装着されてもよい。

【０１９１】

即ち、この発明においては、アレーアンテナ２０は、２つの無線装置１０，３０のうち、少なくとも一方の無線装置に装着されていればよい。

【０１９２】

また、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、無線装置１０，３０間の通信環境に応じて決定されてもよい。即ち、無線装置１０，３０間の通信環境が盗聴し易い環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、無線装置１０，３０間の通信環境が盗聴しにくい環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

【０１９３】

更に、定期的に秘密鍵Ｋｓ１，Ｋｓ２の鍵長を変えるようにしてもよい。

【０１９４】

更に、無線装置１０，３０間で送受信する情報の機密性に応じて秘密鍵Ｋｓ１、Ｋｓ２の鍵長を変えるようにしてもよい。即ち、情報の機密性が高いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、情報の機密性が低いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

【０１９５】

そして、この鍵長は、アレーアンテナ２０の指向性を変化させる個数、即ち、制御電圧ＣＬＶ１～ＣＬＶｎの個数により制御される。秘密鍵Ｋｓ１，Ｋｓ２は、検出された電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数からなるビットパターンを有し、電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数は、アレーアンテナ２０の指向性を変化させる個数に等しいからである。つまり、制御電圧ＣＬＶ１～ＣＬＶｎの個数により秘密鍵Ｋｓ１，Ｋｓ２の鍵長を制御できる。

【０１９６】

このように、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、電気的に指向性を切換え可能なアレーアンテナ２０の指向性を変化させる個数によって決定される。

【０１９７】

更に、上記においては、２つの無線装置間において秘密鍵を生成する場合、即ち、１つの無線装置が１つの無線装置と通信する場合について説明したが、この発明は、これに限らず、１つの無線装置が複数の無線装置と通信する場合についても適用される。この場合、１つの無線装置は、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変えて秘密鍵を生成する。１つの無線装置は、アレーアンテナ２０の指向性の切換パターンを１つに固定して複数の無線装置との間で秘密鍵を生成することも可能であるが（複数の無線装置の設置場所によって１つの無線装置との伝送路が異なるので、通信の相手毎に異なる秘密鍵を生成できる）、盗聴を効果的に抑制するには、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変えて秘密鍵を生成するのが好ましい。

【０１９８】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【産業上の利用可能性】

【０１９９】

この発明は、秘密鍵の盗聴を抑制可能な無線通信システムに適用される。また、この発明は、２つの秘密鍵の相関値が最小になるように無線通信システムにおいて用いられる秘密鍵の作成をコンピュータに実行させるためのプログラムに適用される。

【図面の簡単な説明】

【０２００】

【図１】この発明の実施の形態による無線通信システムの概略図である。

【図２】図１に示す一方の無線装置の内部構成を示す概略ブロック図である。

【図３】図１に示す他方の無線装置の概略ブロック図である。

【図４】図３に示す指向性設定部の概略ブロック図である。

【図５】図１に示す盗聴装置の概略ブロック図である。

【図６】図２及び図３に示す鍵一致確認部の概略ブロック図である。

【図７】図２及び図３に示す鍵一致化部の概略ブロック図である。

【図８】受信信号プロファイルＲＳＳＩの概念図である。

【図９】図８に示すパターンＰ１～Ｐｎを決定するための制御電圧パターンと受信信号プロファイルを示す図である。

【図１０】２つの秘密鍵の相関値を演算する概念図である。

【図１１】盗聴装置において作成される秘密鍵との相関値が最小である秘密鍵を無線装置において作成するためのアレーアンテナの指向性パターンを決定する動作を説明するためのフローチャートである。

【図１２】シミュレーションに用いた無線装置及び盗聴装置の平面配置図である。

【図１３】無線装置における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ１と盗聴装置における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ３とを示す図である。

【図１４】無線装置のアレーアンテナから出射されるビームパターンである。

【図１５】ランダムビームが用いられたときの無線装置及び盗聴装置における受信信号プロファイルを示す図である。

【図１６】マルチビームのパターンである。

【図１７】図１６に示すマルチビームを用いた場合の無線装置及び盗聴装置における受信信号プロファイルを示す図である。

【図１８】シミュレーションに用いた無線装置及び盗聴装置の他の平面配置図である。

【図１９】図１８に示す配置位置において、無線装置における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ１と盗聴装置における受信信号プロファイルＲＳＳＩ及び秘密鍵Ｋｓ３とを示す図である。

【図２０】無線装置において作成された秘密鍵Ｋｓ１と盗聴装置において作成された秘密鍵Ｋｓ３とを示す図である。

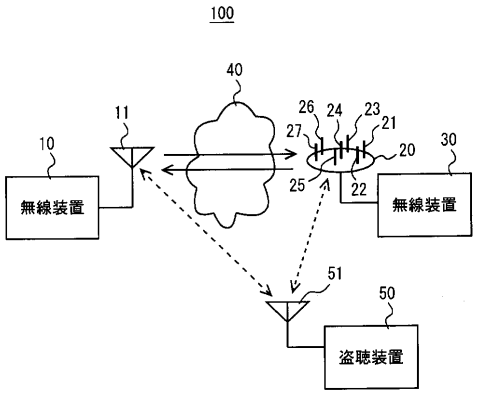
【図２１】図１に示す２つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

【符号の説明】

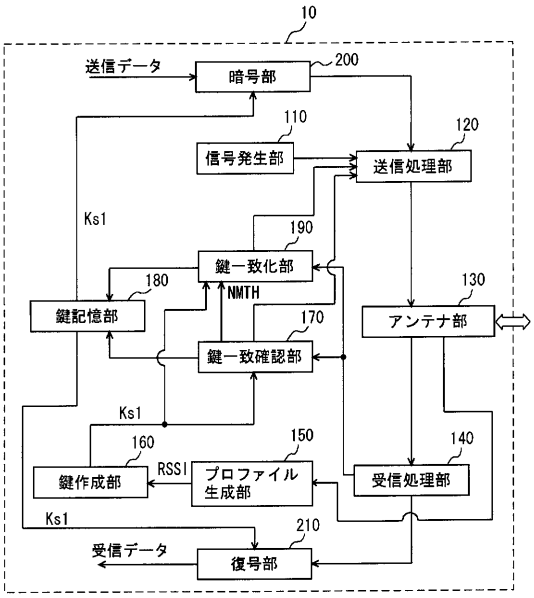
【０２０１】

１０，３０　無線装置、１１，５１　アンテナ、２０　アレーアンテナ、２１～２７　アンテナ素子、４０　中間物、５０　盗聴装置、６０，７０　秘密鍵、８０　部屋、８１　壁、１００　無線通信システム、１１０　信号発生部、１２０　送信処理部、１３０，２２０，３１０　アンテナ部、１４０　受信処理部、１５０，３２０　プロファイル生成部、１６０，３３０　鍵作成部、１７０　鍵一致確認部、１７１，１９４　データ発生部、１７２，１９５　データ比較部、１７３，１９６　結果処理部、１８０　鍵記憶部、１９０　鍵一致化部、１９１　擬似シンドローム作成部、１９２　不一致ビット検出部、１９３　鍵不一致訂正部、２００　暗号部、２１０　復号部、２３０　指向性設定部、２３１　制御電圧発生回路、２３２　バラクタダイオード、２４０　鍵受信部、２５０　鍵相関処理部、３４０　鍵送信部。

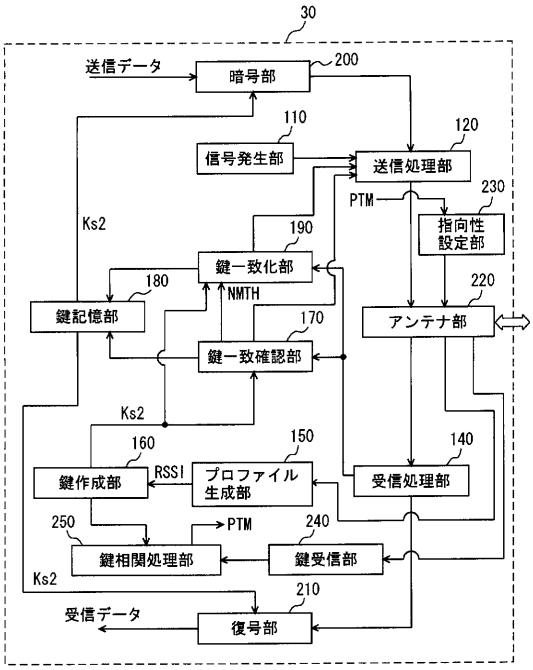
【図１】


100
40
11
10
無線装置
26
24
23
21
27
20
30
25
22
無線装置
51
50
盗聴装置

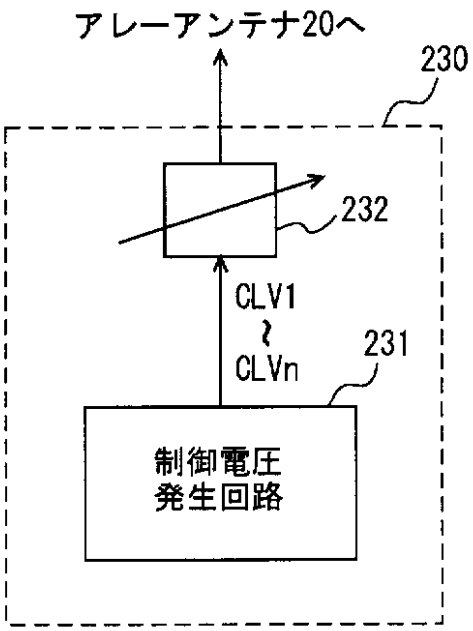
【図２】


10
送信データ
暗号部
200
110
信号発生部
120
送信処理部
Ks1
190
鍵一致化部
180
NMTH
130
鍵記憶部
170
アンテナ部
鍵一致確認部
Ks1
160
150
140
鍵作成部
RSSI
プロファイル生成部
受信処理部
Ks1
210
受信データ
復号部

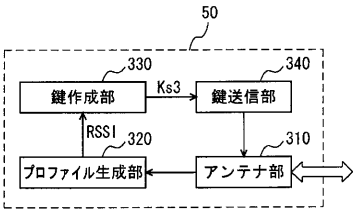
【図３】


30
送信データ
暗号部
200
110
信号発生部
120
送信処理部
PTM
230
指向性設定部
Ks2
190
鍵一致化部
180
NMTH
220
鍵記憶部
アンテナ部
170
鍵一致確認部
Ks2
160
150
140
鍵作成部
RSSI
プロファイル生成部
受信処理部
250
PTM
240
鍵相関処理部
鍵受信部
Ks2
210
受信データ
復号部

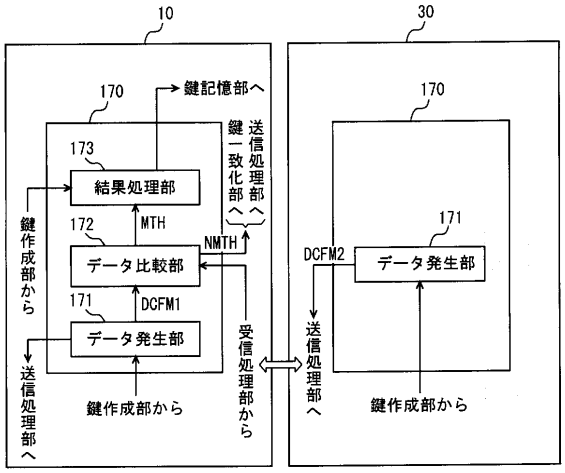
【図４】


アレーアンテナ20へ
230
232
CLV1
～
CLVn
231
制御電圧
発生回路

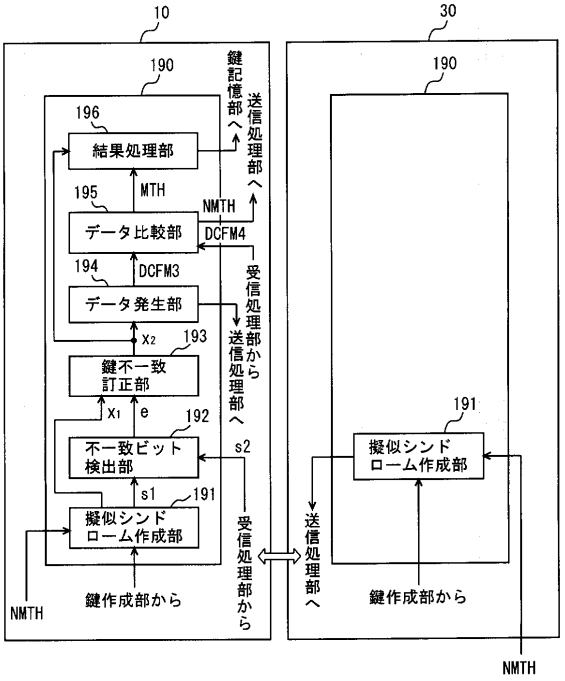
【図５】


50
330
340
鍵作成部
Ks3
鍵送信部
RSSI
320
310
プロファイル生成部
アンテナ部

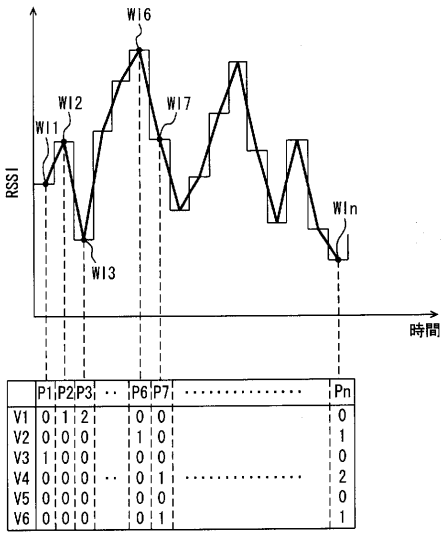
【図６】


10
30
170
鍵記憶部へ
送信処理部へ
鍵一致化部へ
173
結果処理部
172
MTH
データ比較部
NMTH
171
DCFM1
データ発生部
鍵作成部から
送信処理部へ
受信処理部から
DCFM2
データ発生部
鍵作成部から

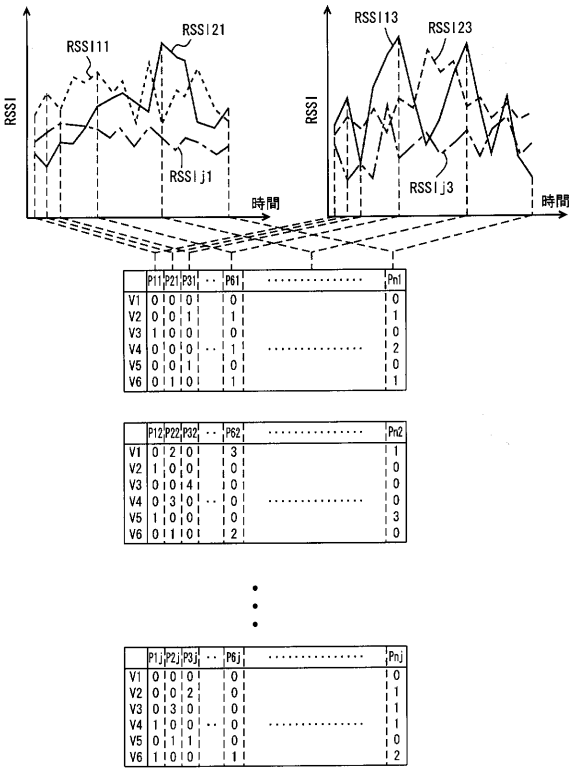
【図７】


10
30
190
196
結果処理部
195
MTH
データ比較部
NMTH
DCFM4
194
DCFM3
データ発生部
193
鍵不一致訂正部
192
不一致ビット検出部
191
擬似シンドローム作成部
鍵記憶部へ
送信処理部へ
受信処理部から
送信処理部へ
受信処理部から
鍵作成部から
NMTH
191
擬似シンドローム作成部
送信処理部へ
鍵作成部から
NMTH

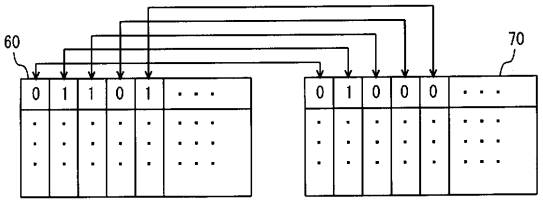
【図８】


WI6
WI2
WI7
WI1
WIn
WI3
RSSI
時間
P1 P2 P3 P6 P7 Pn
V1 0 1 2 0 0 0
V2 0 0 0 1 0 1
V3 1 0 0 0 0 0
V4 0 0 0 0 1 2
V5 0 0 0 0 0 0
V6 0 0 0 0 1 1

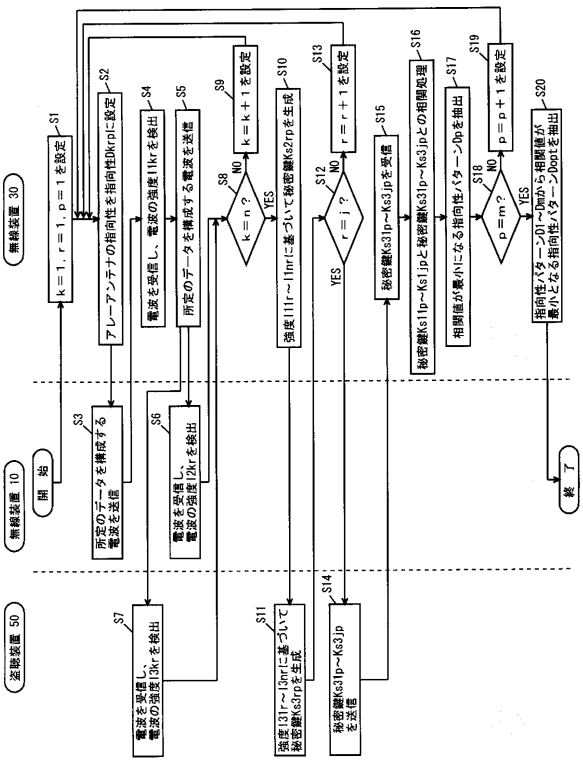
【図９】


RSSI
RSSI11
RSSI21
RSSIj1
時間
RSSI13
RSSI23
RSSIj3
時間
P11 P21 P31 P61 Pn1
V1 0 0 0 0 0
V2 0 0 1 1 1
V3 1 0 0 0 0
V4 0 0 0 1 2
V5 0 0 1 0 0
V6 0 1 1 0 1
P12 P22 P32 P62 Pn2
V1 0 2 0 3 1
V2 1 0 0 0 0
V3 0 0 4 0 0
V4 0 3 0 0 0
V5 1 0 0 0 3
V6 0 1 1 0 0
P1j P2j P3j P6j Pnj
V1 0 0 0 0 0
V2 0 0 2 0 1
V3 0 3 0 0 1
V4 1 0 0 0 1
V5 0 1 1 0 0
V6 1 0 0 1 2

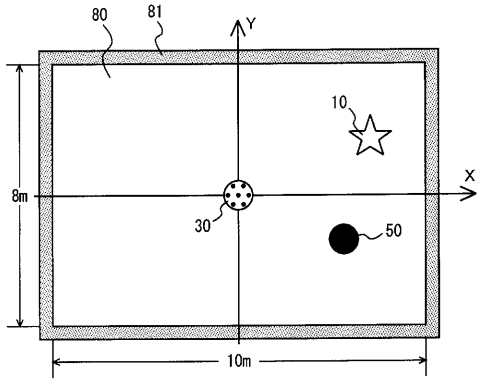
【図１０】



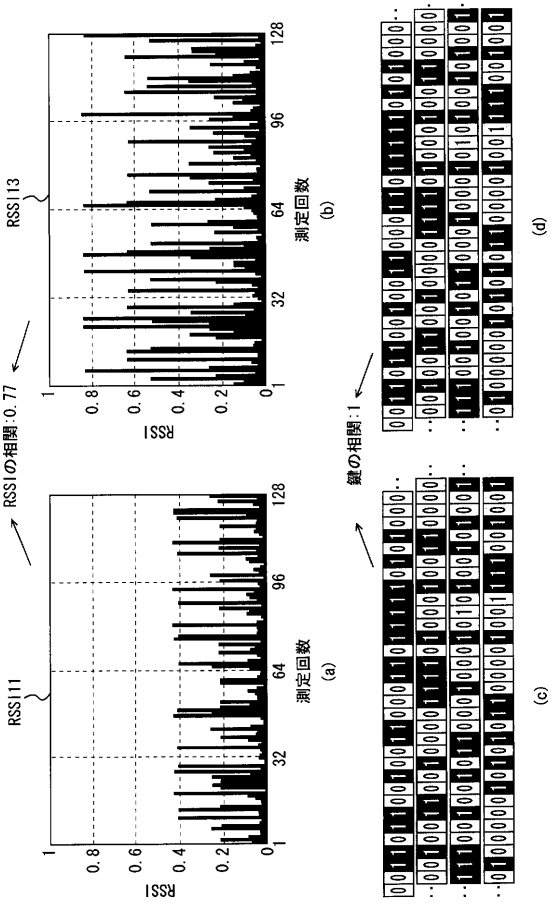
【図１１】



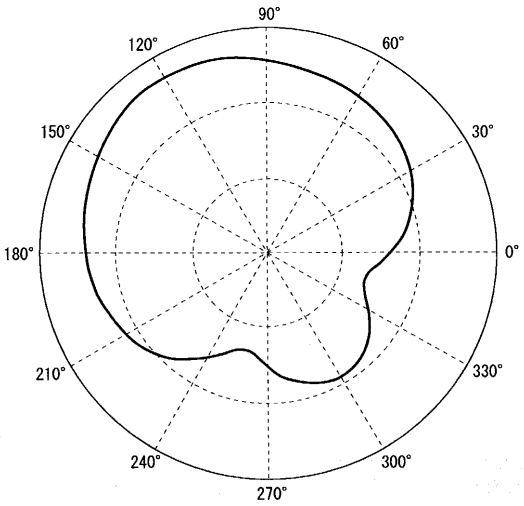
【図１２】



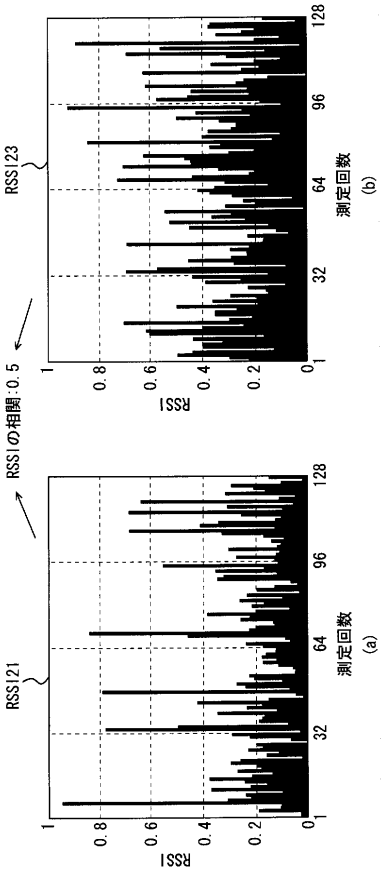
【図１３】



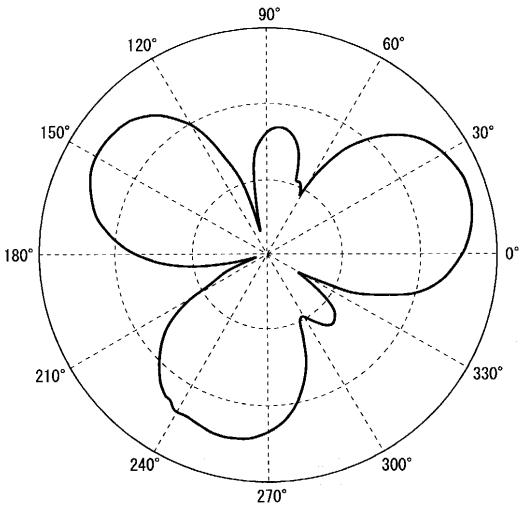
【図１４】



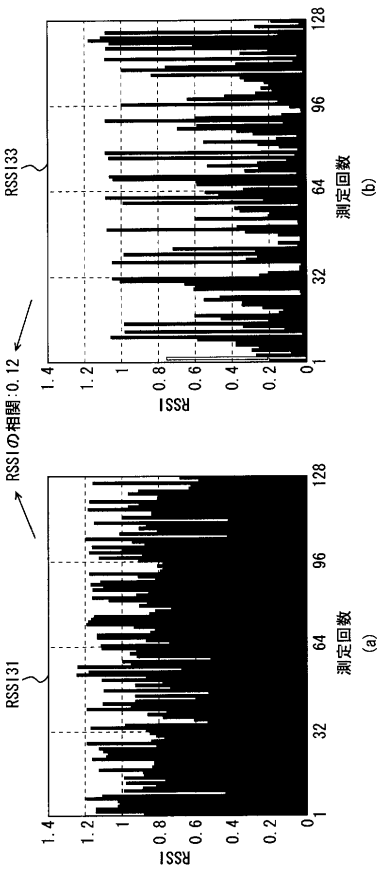
【図１５】



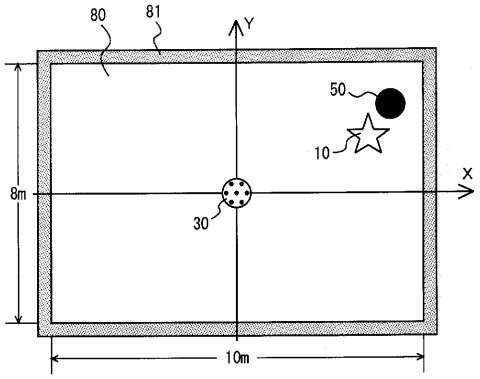
【図１６】



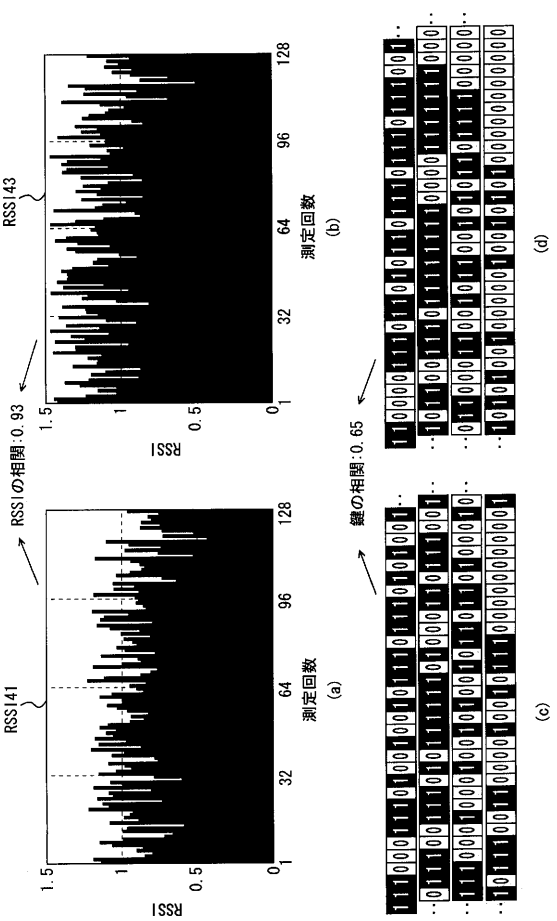
【図１７】



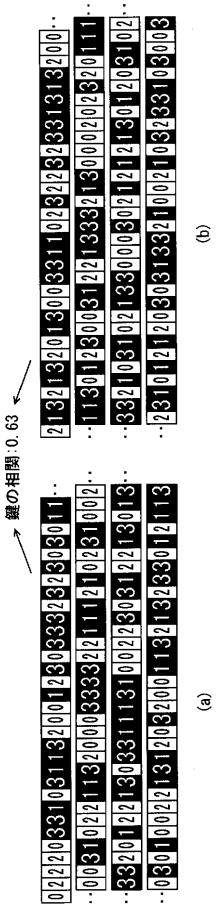
【図１８】



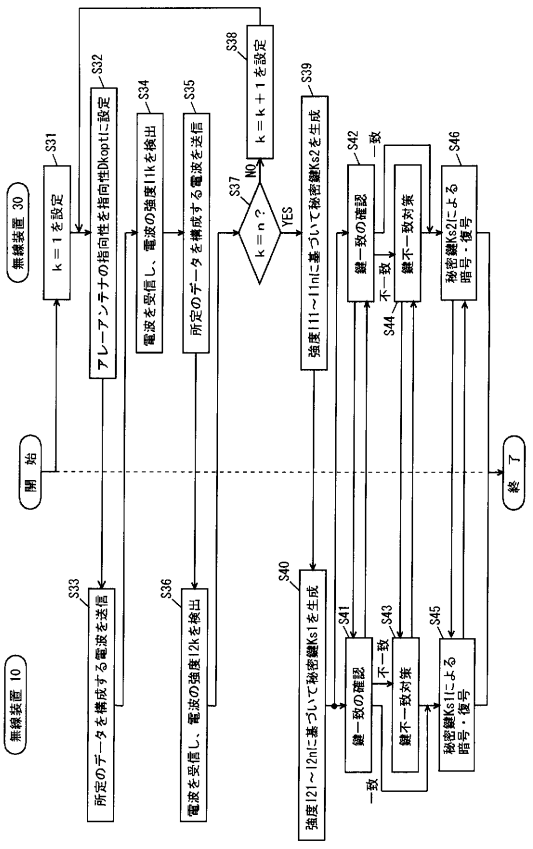
【図１９】



【図２０】



【図２１】



フロントページの続き

(72)発明者　北浦　明人
京都府京田辺市多々羅都谷１－３　同志社大学内
(72)発明者　大平　孝
京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内
(72)発明者　青野　智之
京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内
(72)発明者　俵　覚
京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内

審査官　中元　淳二

(56)参考文献　国際公開第０３／０７３６８９（WO，Ａ１）
M. Orihashi et al., Proposal of channel synthesized modulation for secured access on physical layer, Vehicular technology conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual, ２００３年　４月２２日, Vol.4, pp.2638-2642

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　８８／０２
Ｈ０４Ｌ　９／０８
Ｈ０４Ｗ　１２／０４