(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4644487号
(P4644487)
(45)発行日　平成23年3月2日(2011.3.2)　(24)登録日　平成22年12月10日(2010.12.10)

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

請求項の数 9　(全 10 頁)

| | |
|---|---|
| (21)出願番号 | 特願2004-525600 (P2004-525600) |
| (86)(22)出願日 | 平成15年6月27日 (2003.6.27) |
| (65)公表番号 | 特表2005-534260 (P2005-534260A) |
| (43)公表日 | 平成17年11月10日 (2005.11.10) |
| (86)国際出願番号 | PCT/IB2003/002932 |
| (87)国際公開番号 | WO2004/014037 |
| (87)国際公開日 | 平成16年2月12日 (2004.2.12) |
| 審査請求日 | 平成18年6月26日 (2006.6.26) |
| (31)優先権主張番号 | 02078076.3 |
| (32)優先日 | 平成14年7月26日 (2002.7.26) |
| (33)優先権主張国 | 欧州特許庁 (EP) |

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100114753
弁理士　宮崎　昭彦
(74)代理人　100122769
弁理士　笛田　秀仙

最終頁に続く

(54)【発明の名称】安全な認証型距離測定法

(57)【特許請求の範囲】
【請求項１】
第１通信装置に記憶されたマルチメディアデータが第２通信装置によってアクセスされるべきかを決定する方法であって、前記第１通信装置と前記第２通信装置との間の距離測定を実行するステップを有する方法において、前記第１通信装置及び前記第２通信装置は、前記距離測定の実行に用いられる共通秘密を共有し、前記共通秘密は、前記距離測定を実行する前に、前記第２通信装置が事前規定された一連の準拠規則に準拠するかを確認することによって、前記第１通信装置からの前記第２通信装置に関しての認証確認を実行するステップ、及び、前記第２通信装置が準拠する場合、前記共通秘密を共有するステップにより共有され、
当該方法はさらに、前記認証確認及び前記距離測定後に、前記第１通信装置から前記第２通信装置へと前記マルチメディアデータを送信するためのセキュア認証済チャネル（SAC）の生成に前記共通秘密を使用するステップを有することを特徴とする方法。
【請求項２】
請求項１に記載の方法であって、前記距離測定が、
－第１時間ｔ１において第１信号を前記第１通信装置から前記第２通信装置へ伝送するステップであって、前記第２通信装置が、前記第１信号を受信するように構成されたステップと、
－前記受信された第１信号を前記共通秘密に従い修正することにより第２信号を生成し、前記第２信号を前記第１通信装置へ伝送するステップと、

－第２時間ｔ２において前記第２信号を受信するステップと、
－前記第２信号が前記共通秘密に従い修正されたかを確認するステップと、
－前記第１通信装置と前記第２通信装置との間の距離をｔ１とｔ２との間の時間差に従い決定するステップと、
に従い実行される方法。
【請求項３】
前記第１信号が拡散スペクトル信号である、請求項２に記載の方法。
【請求項４】
請求項２に記載の方法であって、前記第２信号が前記共通秘密に従い修正されたかを確認するステップが、
－前記第１信号を前記共通秘密に従い修正することによって第３信号を生成するステップと、
－前記第３信号を前記受信された第２信号と比較するステップと、
によって実行される方法。
【請求項５】
請求項２に記載の方法であって、前記第１信号及び前記共通秘密がビットワードであり、前記第２信号が、当該ビットワードの間において排他的論理和演算を実行することによって生成される情報を有する方法。
【請求項６】
請求項１に記載の方法であって、前記認証確認は、前記第２装置の識別子が所期の識別子に準拠するかを確認するステップを更に有する方法。
【請求項７】
請求項１に記載の方法であって、前記共通秘密を共有するステップが、鍵転送プロトコル(key transport protocol)及び鍵合意プロトコル(key agreement protocol)のうちの一つを実行することを含む方法。
【請求項８】
第１通信装置に記憶されたマルチメディアデータが第２通信装置によってアクセスされるべきかを決定するように構成された第１通信装置であって、当該第１通信装置と前記第２通信装置との間の距離測定を実行する手段を有する第１通信装置において、前記第１通信装置が、前記第２通信装置にも記憶される共通秘密を記憶するメモリを有し、前記共通秘密は前記距離測定の実行に用いられ、前記第１通信装置は、前記距離測定を実行する前に、前記第２通信装置が事前規定された一連の準拠規則に準拠するかを確認することによって、前記第１通信装置からの前記第２通信装置に関しての認証確認を実行するステップ、及び、前記第２通信装置が準拠する場合、前記第２通信装置と前記共通秘密を共有するステップにより、前記共通秘密を共有するように構成され、前記第１通信装置はさらに、前記認証確認及び前記距離測定後に、前記第１通信装置から前記第２通信装置へと前記マルチメディアデータを送信するためのセキュア認証済チャネル（SAC）の生成に前記共通秘密を使用する第１通信装置。
【請求項９】
請求項８に記載の第１通信装置及び前記マルチメディアデータを再生するための手段を有する第２通信装置を有するシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、第１通信装置と第２通信装置との間の認証型距離測定を実行する第１通信装置のための方法に関する。本発明は、第１通信装置に記憶されたデータが、第２通信装置によってアクセスされるべきかを決定する方法にも関する。更に、本発明は、第２通信装置への認証型距離測定を実行するための通信装置に関する。本発明は、通信装置を有する、マルチメディア・コンテンツを再生するための機器にも関する。
【背景技術】

【０００２】
デジタル・メディアは、様々な種類のデータ情報に関しての人気の高いキャリアになっている。例えばコンピュータ・ソフトウェア及び音声情報は、光コンパクト・ディスク（ＣＤ）で広く入手可能であり、最近ではＤＶＤも流通シェアを増加させている。ＣＤ及びＤＶＤはデータ、ソフトウェア、画像及び音声のデジタル記録に関する共通の標準規格を利用する。記録可能なディスク及び固体メモリ等のその他の媒体は、ソフトウェア及びデータ流通市場において大幅に増加している。
【０００３】
デジタル形式のアナログ形式に比べて大幅に優れる品質は、前者に不正な複製作製及び海賊版作製を大幅にされ易くさせ、更にデジタル形式は複製をするのにより容易でありかつより早い。デジタル・データ・ストリームの複製は、圧縮型、無圧縮型、暗号型又は非暗号型であっても、データにおいて品質の何の明らかな損失も一般的に引き起こさない。したがって、デジタル複製は、多世代複製に関して実質的に無制限である。他方で、連続した複製毎にＳ／Ｎ比損失を伴うアナログ・データは、多世代及び大量複製に関して必然的に制限的である。
【０００４】
近年のデジタル形式の人気の到来は、多数の複製保護及びＤＲＭのシステム及び方法をもたらした。これらのシステム及び方法は、暗号化、透かし及び権利記載（例えばデータのアクセス及び複製のためのルール）等の技術を用いる。
【０００５】
デジタル・データの形のコンテンツを保護する一つの手段は、コンテンツが、
－受信装置が、準拠した装置であるとして認証された場合と、
－コンテンツの使用者が、このコンテンツを他の装置に転送（移動、複製）する権利を有する場合と、
にのみ転送されるということを保証することである。
【０００６】
コンテンツの転送が許可される場合、この転送は、コンテンツが有用な形式で違法に取り込まれ得ないことを確実にする暗号化手段で一般的に実行される。
【０００７】
装置認証及び暗号化コンテンツ転送を実行する技術は、利用可能であり、セキュア認証済チャンネル（ＳＡＣ）と呼ばれる。ＳＡＣ上に渡ってコンテンツを複製することを可能にされ得るが、コンテンツ業界は、インターネット上でのコンテンツ流通に関しかたくなである。これにより、インターネットすなわちイーサネットとうまく整合するインターフェース上でのコンテンツの転送に関し、コンテンツ業界の意見の不一致が生じる。
【０００８】
また、隣人を訪ねている使用者が、彼が所有する映画を隣人の大きなテレビ・スクリーンで鑑賞することは、可能であるべきである。一般的にコンテンツ所有者は、このことを許可しないであろうが、この映画のライセンス保持者（又はこのライセンス保持者が所有する装置）が、このテレビ・スクリーンの近くにあると証明され得る場合、容認され得る。
【０００９】
したがって、コンテンツが他の装置によってアクセスされる又は複製されるべきかを判断する場合に、認証型距離測定を含むことが可能であることは興味深い。
【００１０】
Stefan Brands 及び David Chaumによる記事、"Distance-Bounding protocols", Eurocrypt ’93 (1993), Pages 344-359において、距離束縛プロトコル(distance-bounding protocol)の公開鍵識別スキームとの統合が記述されている。そこでは、距離測定は、チャレンジ／レスポンス・ビットを使用し、及びコミットメント・プロトコル(commitment protocol)を使用した時間測定に基づき記述されている。これは、２つの装置がお互いにも認証しなければならない場合、認証装置準拠試験を可能にせず、有効ではない。

【発明の開示】
【発明が解決しようとする課題】
【００１１】
本発明の目的は、有限距離におけるコンテンツの安全な転送を実行する課題に対する解決法を得ることである。
【課題を解決するための手段】
【００１２】
このことは、第１通信装置が前記第１通信装置と第２通信装置との間の認証型距離測定を実行する方法によって達成され、前記第１通信装置及び前記第２通信装置は、共通秘密を共有し、前記共通秘密は、第１及び第２通信装置との間の距離測定を実行するのに用いられる。
【００１３】
前記共通秘密は距離測定を実行するために使用されているので、第１通信装置から第２通信装置への距離を測定する場合、測定されているのは正しい装置間の距離であることを保証され得る。
【００１４】
当該方法は、距離測定プロトコルを認証プロトコルと組み合わせる。これは、認証装置準拠試験を可能にし、有効である。というのも、安全なチャンネルが装置間の安全な通信を可能にさせることを何れにせよ必要とされ、距離測定が実行される前に、準拠性に関し装置が初めに試験され得るからである。
【００１５】
特定の実施例において、当該認証型距離測定は、次の、
－第１時間ｔ１において第１信号を前記第１通信装置から前記第２通信装置へ伝送するステップであって、前記第２通信装置が、前記第１信号を受信し、前記受信された第１信号を前記共通秘密に従い修正することにより第２信号を生成し、前記第２信号を前記第１装置へ伝送するように構成されたステップと、
－第２時間ｔ２において前記第２信号を受信するステップと、
－前記第２信号が、前記共通秘密に従い修正されたかを確認するステップと、
－前記第１と前記第２通信装置との間の距離をｔ１とｔ２との間の時間差に従い決定するステップと、
に従い実行される。
【００１６】
信号の伝送と受信との間の時間差を測定し、帰還信号が第２通信装置から実際に生じたかを決定するための、第１及び第２通信装置の間で共有された秘密を使用することによって距離を測定する場合に、（前記秘密を知らない）第３通信装置へこの距離が測定されないことを保証する安全な認証された手段で、この距離は測定される。信号を修正する共通秘密を使用することは、セキュアな認証型距離測定を実行する簡便な手段である。
【００１７】
特定の実施例において、第１信号は、拡散スペクトル信号である。それによって高解像度が得られ、悪伝送条件（例えば、多くの反射がある無線環境）に対処することが可能である。
【００１８】
他の実施例において、第２信号が共通秘密に従い修正されたかを確認するステップは、
－第１信号を共通秘密に従い修正することによって第３信号を生成するステップと、
－当該第３信号を、受信された第２信号と比較するステップと
によって実行される。
【００１９】
この方法は、確認ステップを実行するのに容易かつ簡便な手段であるが、第１通信装置及び第２通信装置の両方は、第１信号がどのように共通秘密を用いて修正されているかを知っていることが必要である。

【００２０】
特定の実施例において、第１信号及び共通秘密は、ビットワードであり、第２信号は、これらビットワードの間において排他的論理和演算を実行することによって生成される情報を有する。実行されるべきことは、非常に簡便な操作であり、当該操作を実行する場合、第１及び第２通信装置にほんの少しのリソースしか必要としない。
【００２１】
共通秘密が距離測定を実行する前に共有されている実施例において、この共有ステップは、
－第２通信装置が一群の事前規定された準拠規則に準拠するかを確認することによって、第１通信装置からの第２通信装置に関する認証確認を実行するステップと、
－第２通信装置が準拠する場合、前記秘密を第２通信装置へ伝送することによって前記共通秘密を共有するステップと、
によって実行される。
【００２２】
これは、秘密の共有を実施するのに安全な手段であり、準拠規則に準拠する装置のみが秘密を受信することが可能であることを保証する。更に、共有された秘密は、当該２つの装置の間においてＳＡＣチャンネルを生成するためにその後用いられ得る。当該秘密は、例えばＩＳＯ　１１７７０－３に記載の鍵配送機構（key transport mechanisms）を用いて共有され得る。代わりとして、鍵共有プロトコル(key agreement protocol)が用いられ得、例えば、このプロトコルも、ＩＳＯ　１１７７０－３に記載されている。
【００２３】
他の実施例において、認証確認は、第２装置の識別子が所期の識別子と準拠するかを確認するステップを有する。それにより、第２装置が確かにあるべき装置であるということを保証される。この同一性は、第２装置に記憶された証明を確認することにより得ることができる。
【００２４】
本発明は、第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定する方法に関し、当該方法は、第１通信装置と第２通信装置との間の距離測定を実施し、前記測定された距離が既定の距離区間の範囲内であるかを確認するステップを有し、ここでは、距離測定は、上記に従う認証型距離測定である。装置間におけるデータの共有に関連する認証型距離測定を用いることにより、コンテンツの不正配布は、低減され得る。
【００２５】
特定の実施例において、第１装置に記憶されたデータが第２装置によってアクセスされるべきであると決定される場合、第１装置に記憶されたデータは、第２装置に送信される。
【００２６】
本発明は、第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定する方法に関し、当該方法は、第３通信装置と第２通信装置との間のおける距離測定を実施し、前記測定された距離が既定の距離区間の範囲内であるかを確認するステップを有し、ここでは、距離測定は、上記に従う認証型距離測定である。この実施例において、距離は、第２通信装置とデータが記憶される第１通信装置との間の距離は測定されない。代わりに、距離は、第３通信装置がコンテンツの所有者の私的なものであり得るような、第３通信装置と第２通信装置との間において測定される。
【００２７】
本発明は、第２通信装置への認証型距離測定を実施する通信装置であり、当該通信装置が、共通秘密を第２通信装置と共有し、また当該通信装置が、前記共通秘密を用いて第２装置への距離を測定する手段を有するような通信装置にも関する。
【００２８】
特定の実施例において、当該装置は、

－第１時間ｔ１において第１信号を前記第２通信装置へ伝送する手段であって、前記第２通信装置が、前記第１信号を受信し、前記受信された第１信号を前記共通秘密に従い修正することにより第２信号を生成し、前記第２信号を伝送するように構成された手段と、
－第２時間ｔ２において前記第２信号を受信する手段と、
－前記第２信号が、前記共通秘密に従い修正されたかを確認する手段と、
－前記第１通信装置と前記第２通信装置の間の距離をｔ１とｔ２との間の時間差に従い決定する手段と、
を有する。

【００２９】

本発明は、上記の通信装置を有する、マルチメディア・コンテンツを再生する機器にも関する。

【発明を実施するための最良の形態】

【００３０】

次において、本発明の好ましい実施例は、図を参考に説明される。

【００３１】

図１は、認証型距離測定がコンテンツ保護用に用いられている実施例を示す。円１０１の中心に、計算機１０３が配置される。前記計算機は、例えばハードディスク、ＤＶＤ又はＣＤに記憶されるビデオ又は音声であるマルチメディア・コンテンツのようなコンテンツを有する。当該計算機の所有者はこのコンテンツを所有するので、当該計算機は、この使用者に関してマルチメディア・コンテンツへアクセスすること及びマルチメディア・コンテンツを上演することを承認される。この使用者が、このコンテンツを例えばＳＡＣを介して他の装置に合法複製したい場合、その他の装置と計算機１０３との間の距離が測定され、円１０１内の装置１０５，１０７，１０９，１１１，１１３で示される、事前規定の距離の範囲内の装置のみが、コンテンツを受信することを許可される。この場合に、事前規定の距離より大きい、計算機１０１への距離を有する装置１１５，１１７，１１９は、コンテンツを受信することを許可されない。

【００３２】

この例において装置は計算機であるが、装置が距離測定を実行する通信装置を有する限り、装置は、例えばＤＶＤ駆動装置、ＣＤ駆動装置又はビデオでもあり得る。

【００３３】

データが記憶される計算機とその他の装置との間の距離が測定される必要のないような特定の例において、当該その他の装置は、第３装置、すなわち事前規定の距離の範囲内にあるコンテンツの所有者の私的なものである装置でもあり得る。

【００３４】

図２において、流れ図は、認証型距離測定を実行する通信装置を各々有する２つの装置２０１と２０３との間の認証型距離測定を実行する概略的な考え方を示す。この例において、第１装置２０１は、第２装置２０３が要求したコンテンツを有する。この認証型距離測定は、次のように行われる。ステップ２０５において、第１装置２０１は、第２装置２０３を認証する。このステップは、第２装置２０３が、準拠する装置であるかを確認するステップを有し得、第２装置２０３が確かに第１装置２０１へ特定された装置であるかを確認するステップも有し得る。その後ステップ２０７において、第１装置２０１は、秘密を第２装置２０３と交換し、このステップは、例えば、ランダムに生成されたビットワードを装置２０３へ伝送することによって実行され得る。当該秘密は、例えば、ＩＳＯ １１７７０等に記載の何らかの鍵管理プロトコルに従い安全に共有されなければならない。

【００３５】

その後ステップ２０９において、距離測定のための信号は、第２装置２０３へ伝送され、当該第２装置は、受信された信号を前記秘密に従い修正し、この修正された信号を第１装置へ再返送する。第１装置２０１は、出発信号と帰還信号との間の往復時間を測定し、帰還信号が前記交換された秘密に従い修正されたかを確認する。何らかの秘密に従う帰還信号の修正は、伝送システム及び距離測定に用いられる信号に最も依存しやすく、すなわ

ち（１３９４、イーサネット、ブルートゥース及びIEEE 802.11等のような）各々の通信システム関して特有である。

【００３６】

距離測定に用いられる信号は、通常のデータ・ビット信号であってもよく、データ通信用以外の特別信号が用いられてもよい。ある実施例において、拡散スペクトル信号が、高解像度を得ることができるように、及び悪伝送条件（例えば、多くの反射がある無線環境）に対処することができるように用いられる。

【００３７】

特定の例において、直接シーケンス拡散スペクトル信号が距離測定に関して用いられる。この信号は、秘密のビット（例えば、秘密は１２７ビットからなる）によって直接シーケンス・コードのチップを排他的論理和演算する（例えば、同様に１２７個のチップからなるコードを拡張する）ことにより修正され得る。排他的論理和演算と同様な他の数学的演算も用いられ得る。

【００３８】

認証２０５及び秘密の交換２０７は、いくつかの既知であるISO国際標準規格の、ＩＳＯ　９７９８及びＩＳＯ　１１７７０に記載のプロトコルを用いて実行され得る。例えば、第１装置２０１は、次の通信シナリオに従い第２装置２０３を認証することができる。

第１装置　→　第２装置　：

【数１】

$$R_B||Text\ 1$$

ここで、$R_B$ はランダムな数である。

第２装置　→第１装置　：

【数２】

$$CertA||TokenAB$$

ここで、 CertA は Ａ の証明であり、

【数３】

$$TokenAB=R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)$$

$R_A$ は、ランダムな数であり、

識別子 B は、オプションであり、

$sS_A$ は、秘密鍵を用いて Ａ によって設定された符号である。

【００３９】

TokenABが、ＩＳＯ　１１７７０－３で定められるトークン(Token)で置き換えられる場合、同時に秘密鍵交換を行うことができる。このステップは、

【数４】

$$Text2:= eP_B(A||K||Text2)||Text3$$

であるようなText2を代入することにより用いられ得、

ここで、$eP_B$ は、公開鍵 B で暗号化され、

A は、A の識別子であり、

Kは、交換されるべき秘密である。

【００４０】

この場合、第２装置２０３が鍵を決定し（すなわち鍵制御を有し）、これは、鍵配送プ

ロトコルとも呼ばれるが、鍵共有プロトコルも用いられ得る。これは、第１装置が鍵を決定するような、反転され得る場合には望ましくないこともあり得る。ここで、秘密鍵は、図２におけるステップ２０７に従い交換された。再び、秘密鍵は、例えば、鍵配送プロトコル又は鍵共有プロトコルによって交換され得る。

【００４１】

距離が上述のような安全な認証手順で測定された後で、データは、ステップ２１１において第１装置及び第２装置の間で送信され得る。

【００４２】

図３は、認証型距離測定を実行するステップを更に詳細に示す。上述されるように、第１装置３０１及び第２装置３０２は、鍵を交換してあり、当該鍵は、第１装置のメモリ３０５及び第２装置のメモリ３０７に記憶される。距離測定を実行するために、信号は、伝送器３０９を介して第２装置へ伝送される。第２装置は、受信器３１１を介して該信号を受信し、３１３は、該信号をローカルに記憶された秘密を用いることにより修正を行う。前記信号は、第１装置３０１によって既知の規則に従い修正され、伝送器３１５を介して第１装置３０１へ返送される。第１装置３０１は、受信器３１７を介して前記修正された信号を受信し、３１９において、当該受信された修正信号は、ローカルに修正されていた信号と比較される。ローカルでの修正は、伝送器３０９で第２装置へ伝送される信号を用い、第２装置によって用いられる修正規則と同一のローカルに記憶された秘密を用いて信号を修正することにより、３２１において実行される。受信された修正信号とローカルに修正された信号とが同一である場合、受信された信号は、認証され、第１装置と第２装置との間の距離を決定するのに用いられ得る。この２つの信号が同一でない場合、受信された信号は、認証され得ず、したがって３２５で示されるように距離を測定するのに用いられることができない。３２３において、第１装置と第２装置との間の距離が計算される。このステップは、例えば、信号が第１装置から第２装置へ伝送器３０９によって伝送される時、及び受信器３１７が前記信号を第２装置から受信する時に、時間を測定することにより実行される。したがって、伝送時間と受信時間との間の時間差は、第１装置と第２装置との間の物理的距離を決定するのに用いられ得る。

【００４３】

図４において、認証型距離測定を実行するための通信装置が示される。装置４０１は、受信器４０３及び伝送器４１１を有する。当該装置は、通信バスを介してメモリ４１７に接続されるマイクロプロセッサ４１３を用いてソフトウェアを実行することによって実現され得る、上述のステップを実行する手段を更に有する。当該通信装置は、保護されたコンテンツにアクセスするために、DVD、計算機、CD、CDレコーダ、テレビ及びその他の装置のような装置の内部において配置され得る。

【図面の簡単な説明】

【００４４】

【図１】図１は、コンテンツ保護に関して用いられる認証型距離測定を示す。

【図２】図２は、認証型距離測定を実行する方法を示す流れ図を示す。

【図３】図３は、図２で示される認証型距離測定を実行するステップを更に詳細に示す。

【図４】図４は、認証型距離測定を実行する通信装置を示す。

【図１】

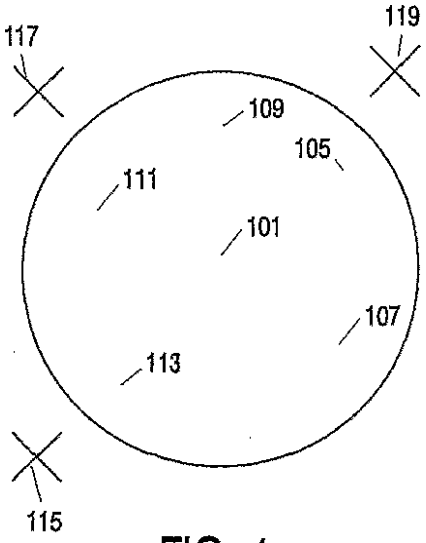



FIG. 1

【図２】

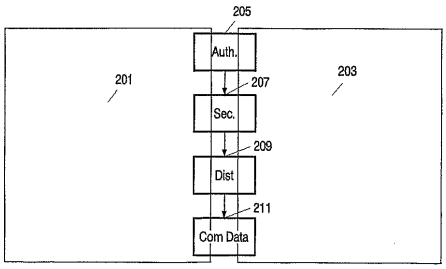
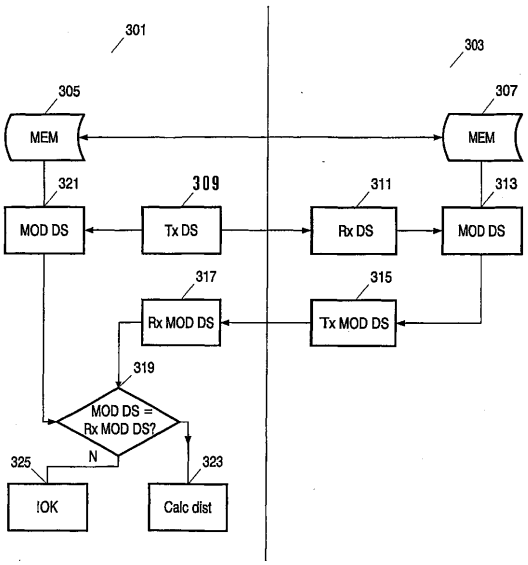



FIG. 2

【図３】




【図４】

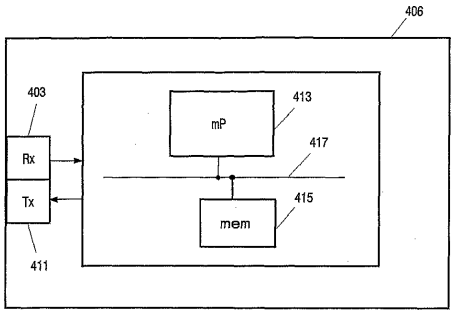



FIG. 4

フロントページの続き

(72)発明者　カンペルマン　フランシスカス　エル　エイ　ジェイ
オランダ国　５６５６　アーアー　アインドーフェン　プロフ　ホルストラーン　６

審査官　青木　重徳

(56)参考文献　特開平０９－１７０３６４（ＪＰ，Ａ）
特開２００１－２５７６７２（ＪＰ，Ａ）
特開平０６－０１９９４８（ＪＰ，Ａ）
国際公開第０２／０３３８８７（WO，Ａ１）
特開平０４－３０６７６０（ＪＰ，Ａ）
米国特許第０５１２６７４６（ＵＳ，Ａ）
特開２００１－３０８７４２（ＪＰ，Ａ）
特開２０００－１８１８６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/32