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

特許第4671776号
(P4671776)

(45)発行日　平成23年4月20日(2011.4.20)　(24)登録日　平成23年1月28日(2011.1.28)

(51)Int.Cl.　　F I
H04W 12/02 (2009.01)　　H04Q 7/00 181
H04L 9/36 (2006.01)　　H04L 9/00 685

請求項の数 5　(全 10 頁)

(21)出願番号　特願2005-175779 (P2005-175779)
(22)出願日　平成17年6月15日 (2005.6.15)
(65)公開番号　特開2006-352490 (P2006-352490A)
(43)公開日　平成18年12月28日 (2006.12.28)
審査請求日　平成20年5月29日 (2008.5.29)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(73)特許権者　503220750
ドコモ・テクノロジ株式会社
東京都港区赤坂二丁目４番５号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　原田　篤
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　石井　美波
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

最終頁に続く

(54)【発明の名称】秘匿処理装置及び秘匿処理方法

(57)【特許請求の範囲】
【請求項１】
移動通信システムのＭＡＣレイヤで秘匿処理を行う秘匿処理装置であって、
ハイパーフレーム番号及びシステムフレーム番号から構成される秘匿シーケンス番号を用いてマスクを作成する手段と、
前記マスクとトランスポートブロックを論理演算することで、暗号化されたトランスポートブロックを出力する秘匿手段と
を有し、前記秘匿手段は、複数のパケットデータユニットを含む前記トランスポートブロックを単位として、前記秘匿処理を行う、秘匿処理装置。
【請求項２】
前記システムフレーム番号は、基地局が固有に有するシーケンス番号であって、共通チャネルで移動局に通知される、請求項１記載の秘匿処理装置。
【請求項３】
所定の暗号化アルゴリズムの入力に秘匿シーケンス番号、論理チャネルの識別子及びマスク長を含む情報が与えられ、前記マスクが前記暗号化アルゴリズムに従って導出される、請求項１記載の秘匿処理装置。
【請求項４】
論理演算が排他的論理和演算である、請求項１記載の秘匿処理装置。
【請求項５】
移動通信システムのＭＡＣレイヤで秘匿処理を行う秘匿処理方法であって、

ハイパーフレーム番号及びシステムフレーム番号から構成される秘匿シーケンス番号を用いてマスクを作成するステップと、
前記マスクとトランスポートブロックを論理演算することで、暗号化されたトランスポートブロックを出力するステップと
を有し、前記トランスポートブロックを出力するステップにおいて、複数のパケットデータユニットを含む前記トランスポートブロックを単位として、前記秘匿処理を行う、秘匿処理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、移動通信システムの秘匿処理を行う装置及び方法に関する。

【背景技術】

【０００２】

ＩＭＴ－２０００システムのような移動通信システムでは伝送されるデータに秘匿処理が施される。ＩＭＴ－２０００システムにおける無線区間の秘匿処理の概要については、非特許文献１に記載されている。

【０００３】

従来の秘匿処理方式では、図１に示すように、秘匿処理が無線リンク制御（ＲＬＣ：Ｒａｄｉｏ Ｌｉｎｋ Ｃｏｎｔｒｏｌ）サブレイヤおよび媒体アクセス制御（ＭＡＣ：Ｍｅｄｉｕｍ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）サブレイヤに分散して配置されている。秘匿処理を行うプロトコルレイヤは無線ベアラ（ＲＢ）に適用されるＲＬＣプロトコルの動作モードに応じて定められている。例えば音声通信で用いられるトランスペアレントモード（ＴＭ：Ｔｒａｎｓｐａｒｅｎｔ Ｍｏｄｅ）の場合にはＭＡＣ層で秘匿処理が行われ、パケット通信や制御信号の送信に用いられる非確認モード（ＵＭ：Ｕｎａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ Ｍｏｄｅ）および確認モード（ＡＭ：Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ Ｍｏｄｅ）の場合にはＲＬＣ層で秘匿処理が行われる。また、秘匿の強度を高めるために、秘匿処理のパラメータとして、暗号鍵（ＣＫ：Ｃｉｐｈｅｒｉｎｇ Ｋｅｙ）の他に、秘匿処理を行うユニット毎に付与される秘匿シーケンス番号（カウント）“ＣＯＵＮＴ”や無線ベアラＩＤ“ＢＥＡＲＥＲ”等が組み合わせられている。

【０００４】

図２及び図３はＩＭＴ－２０００方式での無線区間における秘匿処理を示す。

【０００５】

図２はＲＬＣの動作モードがＴＭの場合のＲＢに適用される秘匿処理である。

【０００６】

秘匿処理はＭＡＣ－ＳＤＵ（サービスデータユニット）単位で行われる。この場合ＭＡＣエンティティにて実施される秘匿処理のパラメータとして、暗号鍵（ＣＫ）以外にコネクションフレーム番号（ＣＦＮ：Ｃｏｎｎｅｃｔｉｏｎ Ｆｒａｍｅ Ｎｕｍｂｅｒ）とハイパーフレーム番号（ＨＦＮ：Ｈｙｐｅｒ Ｆｒａｍｅ Ｎｕｍｂｅｒ）の組み合わせから生成される秘匿シーケンス番号（カウント）および論理チャネルの識別子（ベアラ）に加え、通信の伝送方向（上りリンク／下りリンクの違い）を示す識別子（ディレクション）“ＤＩＲＥＣＴＩＯＮ”が利用される。また、ＭＡＣエンティティで実施される秘匿処理では全ての論理チャネルに共通の秘匿シーケンスが設定される。

【０００７】

図３はＲＬＣの動作モードがＡＭおよびＵＭの場合のＲＢに適用される秘匿処理である。

秘匿処理はＲＬＣ－ＰＤＵ（パケットデータユニット）単位で行われる。この場合ＲＬＣエンティティにて実施される秘匿処理のパラメータとして、暗号鍵（ＣＫ）以外に、ＲＬＣプロトコルデータユニット（ＲＬＣ－ＰＤＵ）に付与されるシーケンス番号（ＳＮ）とハイパーフレーム番号（ＨＦＮ）の組み合わせから生成される秘匿シーケンス番号（カウント）および前記ＰＤＵが属する無線ベアラＩＤ（ベアラ）に加え、通信の伝送方向（上

りリンク／下りリンクの違い）を示す識別子（ディレクション）が利用される。また、ＲＬＣエンティティで実施される秘匿処理では各論理チャネル毎に個別の秘匿シーケンス（カウント）が設定される。

【非特許文献１】３ＧＰＰ　ＴＳ３３．１０２，６．６章
【非特許文献２】３ＧＰＰ　ＴＲ２５．８５８，９．１章
【非特許文献３】３ＧＰＰ　ＴＲ２５．９１３、６．１章

【発明の開示】

【発明が解決しようとする課題】

【０００８】

一般に秘匿処理は処理遅延を抑えつつ、高い強度の秘匿処理を実現することが望ましく、さらに装置構成の簡素化の観点から、トラヒックやチャネル、無線ベアラの種別やＲＬＣの動作モードによらず統一的な手法で提供できることが望ましい。また、秘匿強度を高めるためには複雑な秘匿アルゴリズムを用いる必要がある。このため、処理負荷の観点からは単位時間、例えば、送信時間間隔（ＴＴＩ：Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｔｉｍｅ　Ｉｎｔｅｒｖａｌ）あたりに秘匿処理を施すべき処理単位（プロトコルユニット数（ＰＵ数））の少ない方が、すなわち、ＰＵは出来るだけペイロードサイズが大きい方が望ましい。

【０００９】

また、従来のＩＭＴ－２０００システムにおいて、ＲＬＣ－ＰＤＵもしくはＭＡＣ－ＳＤＵのＰＤＵサイズは４０バイト程度の一定長である。このため従来の秘匿処理では、例えばＨＳＤＰＡ（非特許文献２参照。）やＥｖｏｌｖｅｄ　ＵＴＲＡＮ（非特許文献３参照。）等の新技術の導入による無線ベアラ伝送速度の広帯域化に伴い、単位時間当たりに秘匿処理を行うＰＵ数が増加し、処理負荷が増大することが考えられる。例えば、１００Ｍｂｐｓの無線伝送速度が想定される場合には、ＴＴＩ長をＨＳＤＰＡと同じ２ｍｓｅｃとすると、ＴＴＩ当たりに約２５０００ｂｙｔｅｓの情報伝送が可能になる。従って、仮にＨＳＤＰＡと同じＰＤＵサイズ（４２バイト）およびＴＴＩ長が仮定されると、Ｅｖｏｌｖｅｄ　ＵＴＲＡＮ　で規定されている最大伝送速度（１００Ｍｂｐｓ）の場合、ＴＴＩ＝２ｍｓｅｃあたりに約６００個のＲＬＣ－ＰＤＵに対する秘匿処理が必要となる。これは現在のＨＳＤＰＡの最大伝送速度１４．４Ｍｂｐｓとの比より、従来に比較して約７倍の処理数となり処理負荷が増大してしまうことが考えられる。

【００１０】

更に、秘匿パラメータとして用いられているシーケンス番号は送受信で同期されている必要がある。ＨＦＮはネットワーク側（ＲＮＣ）と移動局のコネクションの設定時に同期された後、秘匿性を維持するために、シーケンス番号（ＳＮもしくはＣＦＮ）の周期毎に送信側、受信側双方で独立にカウントアップされる。このため、シーケンス番号の１周期分以上のＰＤＵが連続して失われた場合（ロスとなった場合）に、送受信側のＨＦＮの同期が外れるという問題がある。図４は、ＳＮの周期が４であり、ＨＦＮの周期が８である場合（秘匿シーケンス番号の周期は８ｘ４＝３２）の例を示す。送信側のＨＦＮは逐次カウントアップされるが、受信側で４つ以上のＰＤＵが連続してロスとなった場合には、受信側のＨＦＮが１周期分送れてカウントアップされ、ＨＦＮの同期が外れてしまう。より具体的には、ＲＬＣ－ＵＭではシーケンス番号（ＳＮ）の桁数は７ビットであるので、１２７個のＲＬＣ－ＰＤＵのロスが発生すると秘匿同期外れが発生する。

【００１１】

本発明は、上記問題点の少なくとも１つに対処するためになされたものであり、その課題は秘匿の処理遅延及び秘匿の同期外れの頻度を少なくとも軽減する秘匿処理装置及び秘匿処理方法を提供することである。

【課題を解決するための手段】

【００１２】

一実施例による秘匿処理装置は、
移動通信システムのＭＡＣレイヤで秘匿処理を行う秘匿処理装置であって、

ハイパーフレーム番号及びシステムフレーム番号から構成される秘匿シーケンス番号を用いてマスクを作成する手段と、
前記マスクとトランスポートブロックを論理演算することで、暗号化されたトランスポートブロックを出力する秘匿手段と
を有し、前記秘匿手段は、複数のパケットデータユニットを含む前記トランスポートブロックを単位として、前記秘匿処理を行う、秘匿処理装置である。

【発明の効果】
【００１３】
本発明によれば、移動通信システムにおける秘匿処理の遅延及び秘匿の同期外れの頻度が少なくとも軽減できる。
【発明を実施するための最良の形態】
【００１４】
本発明の一形態によるＭＡＣ秘匿サブレイヤはトランスポートブロック（ＴＢ）を単位として秘匿処理を行う。トランスポートブロックは、単位時間（ＴＴＩ）当たりのＭＡＣ層から物理層へのデータの転送単位である。秘匿シーケンス番号としてハイパーフレーム番号（ＨＦＮ）及びシステムフレーム番号（ＳＦＮ）が利用され、これによりＲＬＣの全てのモードで統一的な秘匿シーケンス番号の使用が可能になる。秘匿シーケンス番号としてＨＦＮとＳＦＮを組み合わせることにより、ＨＦＮの同期外れが回避される。
【００１５】
秘匿処理部がＭＡＣサブレイヤに統合されることで、移動機構成の簡素化を実現することができる。従来は個々のＲＬＣ－ＰＤＵ毎に秘匿処理が繰り返えされていたが、本発明の一形態では、ＭＡＣ層のＰＤＵ毎に秘匿処理がまとめて行われ、それにより処理負荷及び処理遅延を減らすことができる。ＲＬＣモードによらず、統一したシーケンス番号を利用することで秘匿処理システムの簡素化を図ることができる。また、システムフレーム番号を利用することで、秘匿パラメータの同期外れの確率を低減することができる。
【実施例１】
【００１６】
以下の実施例では下りリンク伝送を想定して説明が行われるが、上りリンク伝送の場合にも本発明が適用可能であることは明らかである。
【００１７】
図５は本発明の一実施例によるＭＡＣ秘匿サブレイヤを含む送信側ＭＡＣサブレイヤの構成例を示す。送信側ＭＡＣサブレイヤは論理チャネル（ＬＣＨ：Ｌｏｇｉｃａｌ Ｃｈａｎｎｅｌ）多重部、優先度識別部、優先度別キュー、スケジューリング部、ＭＡＣ秘匿サブレイヤ、送信側ＨＡＲＱ部から構成される。論理チャネル多重部は、上位レイヤから転送されてくる複数の異なる論理チャネルの多重化処理を行い、後段の優先度識別部にデータを転送する。優先度識別部は、例えば上位レイヤからのシグナリング情報に基づき、論理チャネル多重部において多重化された複数のデータフローに対し、フロー間の送信優先度の順位付けを行い、データをそれぞれの優先度キューに振り分ける。優先度別キューは転送されたデータのバッファリングを行い、スケジューリング部からの指示に基づき、送信タイミングが割り当てられる。優先度別キューは、送信タイミングが割り当てられると、レイヤ１に割り当てられた無線リソースの量に応じてキューから上位レイヤからのＰＤＵデータを取り出してトランスポートブロック（ＴＢ）を構成し、ＭＡＣ秘匿サブレイヤに対しデータの転送を行う。ＭＡＣ秘匿サブレイヤは、データに対し秘匿処理を実施し、送信側ＨＡＲＱ部にデータを転送する。ＨＡＲＱ部は、データの送達管理を行い、無線区間でのデータ伝送の誤りの有無に応じて送信データの再送を行う。
【００１８】
図６に本発明におけるＭＡＣ秘匿サブレイヤを含む受信側ＭＡＣサブレイヤの構成例を示す。受信側ＭＡＣサブレイヤは論理チャネル分離部、ＭＡＣリオーダリング部（Ｒｅｏｒｄｅｒｉｎｇ）部、ＭＡＣ秘匿サブレイヤ、受信側ＨＡＲＱ部から構成される。受信側

ＨＡＲＱ部は下位レイヤから転送されるデータの復号結果を基に送信側ＨＡＲＱ部に再送要求を行い、データが正しく受信できた時点で復号データをＭＡＣ秘匿サブレイヤに転送する。ＭＡＣ秘匿サブレイヤは、受け取ったデータに対し秘匿解除処理を実施し、ＭＡＣリオーダリング部にデータを転送する。ＭＡＣリオーダリング部は、到着データの順序一貫性を保つためにバッファリングを行い、順序の保証されたデータを論理チャネル分離部に報告する。論理チャネル分離部は送信側で多重された論理チャネルを分離し、それぞれの論理チャネル毎に上位レイヤへデータを転送する。

【００１９】

ＭＡＣ秘匿サブレイヤには秘匿処理に用いるパラメータとして秘匿シーケンス番号（ＳＦＮ）および優先度キューＩＤ（ＢＥＡＲＥＲ）が通知される。受信側ＭＡＣ秘匿サブレイヤへの秘匿パラメータ通知は、例えば共通制御チャネルを用いてスケジューリング割り当て情報として該当ＴＢの送信タイミング（即ちＳＦＮ）を通知する方法等が考えられる。伝送方向（ＤＩＲＥＣＴＩＯＮ）は既知であるため通知不要である。

【００２０】

図５，６に示される本実施例によるＭＡＣサブレイヤは、図１０に示されるように機能する。即ち、送信側のＭＡＣサブレイヤはシステムフレーム番号（ＳＦＮ）を利用して論理チャネルを暗号化して物理レイヤに与える。また、受信側のＭＡＣサブレイヤはシステムフレーム番号（ＳＦＮ）に基づいて暗号化を解除し、上位レイヤに報告する。

【００２１】

図７は秘匿処理単位の一例を示す。この例では同一優先度を有する複数の異なる論理チャネルに属する複数のＰＤＵが一つのトランスポートブロックに多重されて単位時間（ＴＴＩ）毎に下位レイヤに転送される。従来の方法では個々のＰＤＵに対して秘匿処理が行われていた。これに対して本実施例では論理チャネル多重部で多重された複数のＰＤＵが秘匿処理の一単位とされる。この単位はプロトコルユニット（ＰＵ）と呼ばれてもよい。複数のＰＤＵがまとめて暗号化されることで、単位時間（ＴＴＩ）あたりに処理すべきＰＵ数を減らすことが出来、処理負荷・遅延の低減を実現できる。

【００２２】

図８は本実施例によるＭＡＣ秘匿サブレイヤにおける秘匿処理を示す。ＭＡＣ秘匿サブレイヤに到着したＰＵ（トランスポートブロック）のビット系列と、秘匿アルゴリズムによって生成された秘匿マスク（Ｍａｓｋ）系列との演算処理（ＸＯＲ）を行うことで、秘匿されたＰＵ（Ｃｉｐｈｅｒｅｄトランスポートブロック）が生成され、図４に示す送信側ＨＡＲＱ部に転送される。秘匿アルゴリズムは秘匿マスク系列を生成するために暗号鍵（ＣＫ：Ｃｉｐｈｅｒｉｎｇ　Ｋｅｙ）および、秘匿シーケンス番号（カウント）“ＣＯＵＮＴ”、伝送の方向（ディレクション）“ＤＩＲＥＣＴＩＯＮ”、優先度キュー番号（ベアラ）“ＢＥＡＲＥＲ”をパラメータとして用いる。秘匿シーケンス番号（カウント）はＨＦＮとＳＦＮの結合で構成される。ＳＦＮは基地局が固有に有するシーケンス番号であり、共通チャネルを通じて基地局が管理する移動局に通知されており、基地局と移動局の間で同期されている。ＳＦＮはユーザのデータの有無に関わらず一定の時間周期でカウントアップされている。従って、基地局および移動局は、それぞれＳＦＮの周期に基づいてＨＦＮのカウントアップを行いさえすれば、たとえカウントアップがそれぞれ独立に行われたとしても、同期状態を維持できる。従って、個々のＰＤＵに付与されるシーケンス番号を用いる従来方式の場合に、１周期以上のパケットロスに起因して生じていた同期はずれの問題は回避できる（図９参照）。また、秘匿パラメータ（シーケンス番号）の不一致は再送によるトランスポートブロックの伝送遅延がＳＦＮの周期以上となる場合にのみ生じる。例えば、２ｍｓｅｃのＴＴＩ長で１２ビットのＳＦＮを用いた場合には$2\times10^{-3}\times2^{12}=8.192$秒以上の遅延が発生した場合に秘匿パラメータの不一致が発生するかもしれない。しかし、実際にはこのような大きな遅延が発生しないように回線品質や再送回数の設計を行うことができるので、実質的にはパラメータの不一致の生じる確率は従来技術に比較して顕著に低減される。

【００２３】

上記の実施例では下りリンク伝送の場合が説明された。しかし、本発明は下りリンク伝送の場合にのみ限定する必要は無く、移動機が送信側となる上りリンク伝送の場合の秘匿処理においても適用が可能なことは明らかである。

【図面の簡単な説明】

【００２４】

【図１】ＩＭＴ－２０００における秘匿処理を示す図である。

【図２】ＲＬＣ－ＴＭにおける秘匿処理を示す図である。

【図３】ＲＬＣ－ＵＭ及びＲＬＣ－ＡＭにおける秘匿処理を示す図である。

【図４】同期外れの説明図を示す。

【図５】ＭＡＣレイヤ秘匿の構成（送信側）を示す図である。

【図６】ＭＡＣレイヤ秘匿の構成（受信側）を示す図である。

【図７】本発明の秘匿処理単位を示す図である。

【図８】本発明の秘匿処理を示す図である。

【図９】本発明の効果を示す図である。

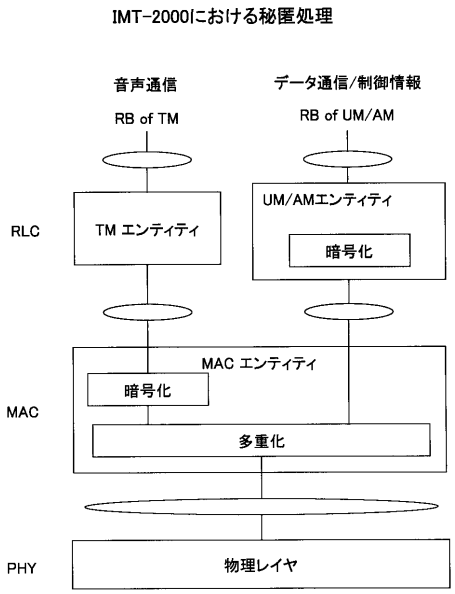
【図１０】本発明のＭＡＣ秘匿サブレイヤを示す図である。

【符号の説明】

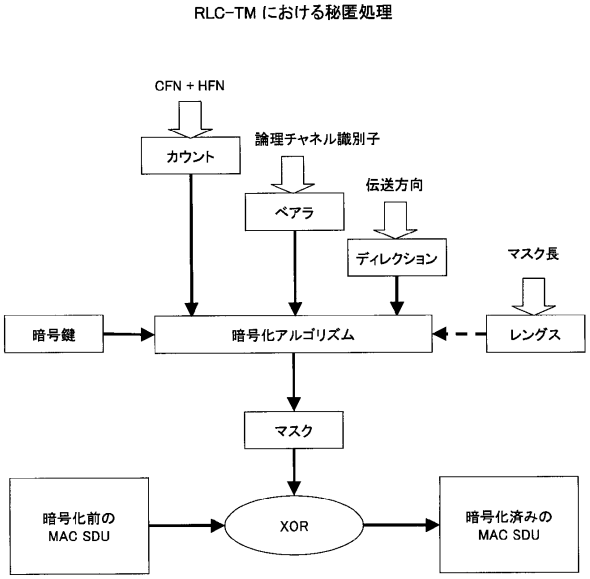
【００２５】

ＲＡＢ　無線アクセスベアラ
ＴＭ　透過型モード
ＵＭ　非確認型モード
ＡＭ　確認型モード
ＲＬＣ　無線リンクコントロール
ＭＡＣ　媒体アクセス制御
ＰＨＹ　物理レイヤ
ＣＦＮ　コネクションフレーム番号
ＨＦＮ　ハイパーフレーム番号
ＳＦＮ　システムフレーム番号
ＳＤＵ　サービスデータユニット
ＰＤＵ　プロトコルデータユニット
ＸＯＲ　排他的論理和
ＬＣＨ　論理チャネル
ＴｒＣＨ　トランスポートチャネル
ＨＡＲＱ　ハイブリッド自動再送要求

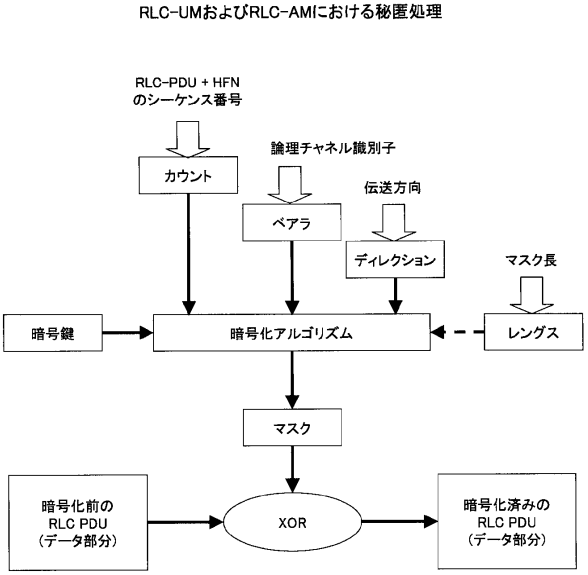
【図１】


IMT-2000における秘匿処理
音声通信
データ通信/制御情報
RB of TM
RB of UM/AM
RLC
TM エンティティ
UM/AMエンティティ
暗号化
MAC
MAC エンティティ
暗号化
多重化
PHY
物理レイヤ

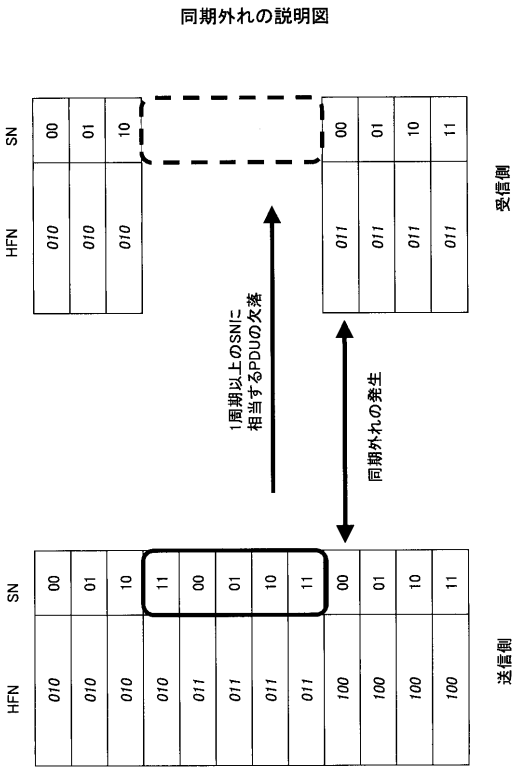
【図２】


RLC-TM における秘匿処理
CFN + HFN
カウント
論理チャネル識別子
ベアラ
伝送方向
ディレクション
マスク長
暗号鍵
暗号化アルゴリズム
レングス
マスク
暗号化前の
MAC SDU
XOR
暗号化済みの
MAC SDU

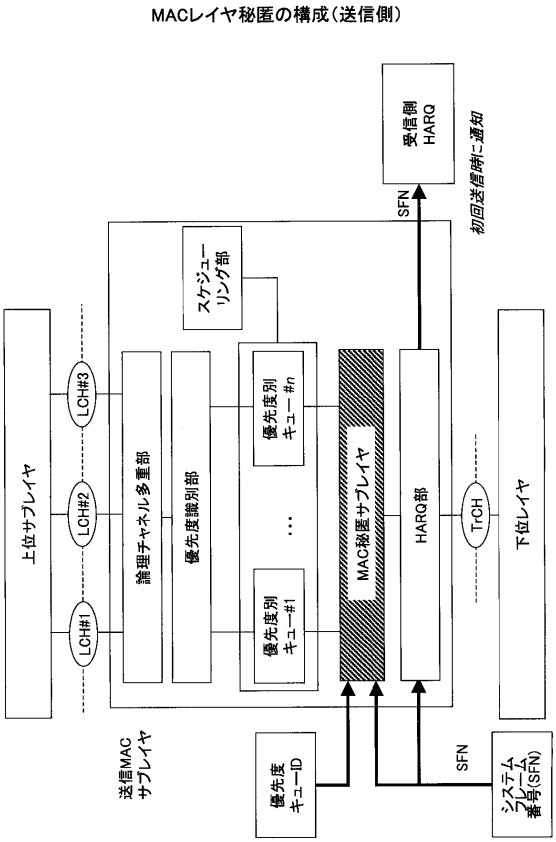
【図３】


RLC-UMおよびRLC-AMにおける秘匿処理
RLC-PDU + HFN
のシーケンス番号
カウント
論理チャネル識別子
ベアラ
伝送方向
ディレクション
マスク長
暗号鍵
暗号化アルゴリズム
レングス
マスク
暗号化前の
RLC PDU
（データ部分）
XOR
暗号化済みの
RLC PDU
（データ部分）

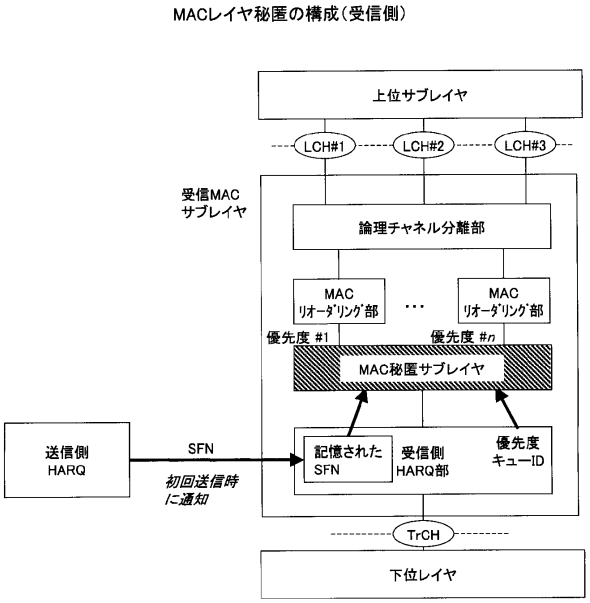
【図４】


同期外れの説明図
SN
HFN
00
01
10
11
010
011
100
受信側
送信側
1周期以上のSNに
相当するPDUの欠落
同期外れの発生

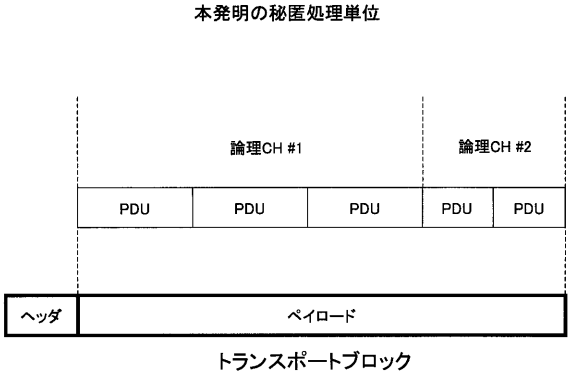
【図５】


MACレイヤ秘匿の構成（送信側）
受信側 HARQ
SFN
初回送信時に通知
スケジューリング部
上位サブレイヤ
LCH#3
LCH#2
LCH#1
論理チャネル多重部
優先度識別部
優先度別キュー #n
優先度別キュー #1
MAC秘匿サブレイヤ
HARQ部
TrCH
下位レイヤ
送信MACサブレイヤ
優先度キューID
SFN
システム番号(SFN)

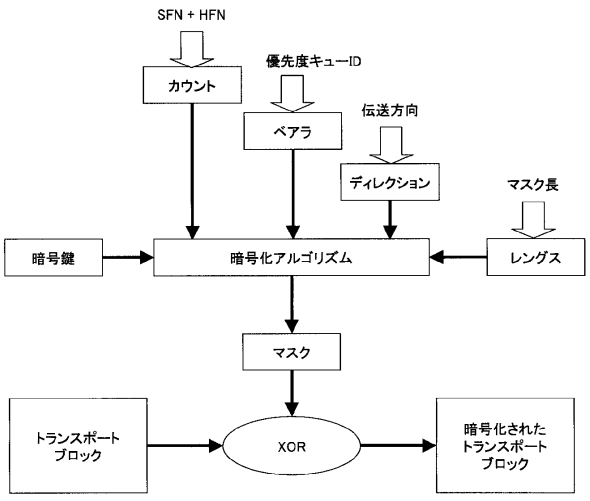
【図６】


MACレイヤ秘匿の構成（受信側）
上位サブレイヤ
LCH#1
LCH#2
LCH#3
受信MACサブレイヤ
論理チャネル分離部
MACリオーダリング部
MACリオーダリング部
優先度 #1
優先度 #n
MAC秘匿サブレイヤ
送信側 HARQ
SFN
初回送信時に通知
記憶されたSFN
受信側 HARQ部
優先度キューID
TrCH
下位レイヤ

【図７】

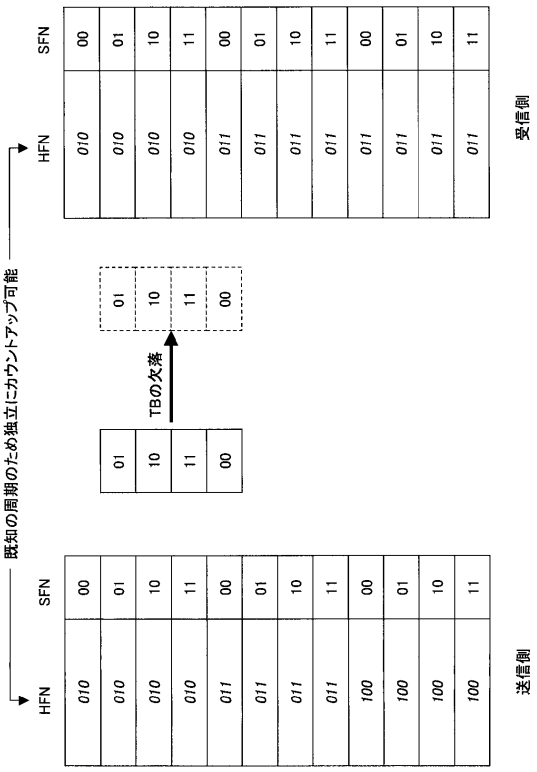

本発明の秘匿処理単位
論理CH #1
論理CH #2
PDU
PDU
PDU
PDU
PDU
ヘッダ
ペイロード
トランスポートブロック

【図８】


本発明の秘匿処理
SFN + HFN
カウント
優先度キューID
ベアラ
伝送方向
ディレクション
マスク長
暗号鍵
暗号化アルゴリズム
レングス
マスク
トランスポートブロック
XOR
暗号化されたトランスポートブロック

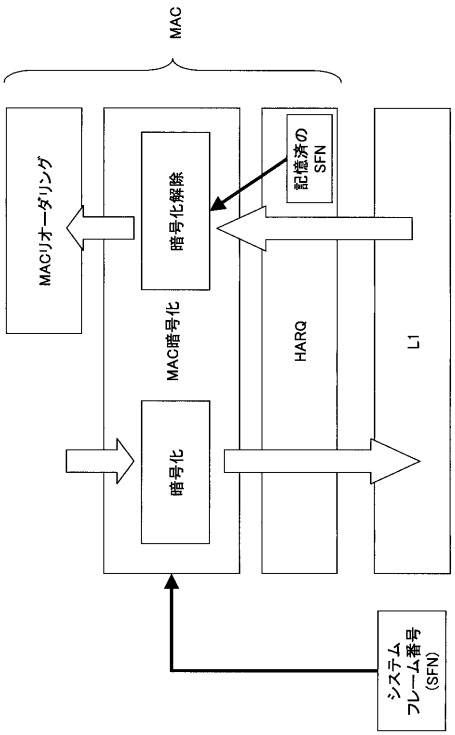
【図９】

本発明の効果



【図１０】

本発明のMAC秘匿サブレイヤ



フロントページの続き

(72)発明者　安部田　貞行
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　中村　武宏
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　鈴木　卓
東京都港区赤坂二丁目４番５号　ドコモ・テクノロジ株式会社内

審査官　浦口　幸宏

(56)参考文献　国際公開第２００５／０９１６６８（WO，Ａ１）
特表２００３－５２５５５６（ＪＰ，Ａ）
3GPP TS 25.402, 3rd Generation Partnership Project, ２００３年１２月, V6.0.0, p.11, ＵＲＬ, http://www.3gpp.org/ftp/Specs/archive/25_series/25.402/25402-600.zip

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　１／００－　５／００
Ｈ０４Ｂ　７／２４－　７／２６
Ｈ０４Ｋ　１／００－　３／００
Ｈ０４Ｌ　９／００－　９／３８
Ｈ０４Ｗ　４／００－９９／００