

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5038366号  
(P5038366)

(45) 発行日 平成24年10月3日 (2012. 10. 3)

(24) 登録日 平成24年7月13日 (2012. 7. 13)

(51) Int. Cl.		F I			
<b>HO 4 W</b>	<b>12/04</b>	<b>(2009. 01)</b>	<b>HO 4 Q</b>	<b>7/00</b>	<b>1 8 2</b>
<b>HO 4 W</b>	<b>72/04</b>	<b>(2009. 01)</b>	<b>HO 4 Q</b>	<b>7/00</b>	<b>5 4 4</b>

請求項の数 12 (全 12 頁)

(21) 出願番号	特願2009-168130 (P2009-168130)	(73) 特許権者	392026693
(22) 出願日	平成21年7月16日 (2009. 7. 16)		株式会社エヌ・ティ・ティ・ドコモ
(65) 公開番号	特開2011-24037 (P2011-24037A)		東京都千代田区永田町二丁目 1 1 番 1 号
(43) 公開日	平成23年2月3日 (2011. 2. 3)	(74) 代理人	100083806
審査請求日	平成23年3月31日 (2011. 3. 31)		弁理士 三好 秀和
早期審査対象出願		(74) 代理人	100100712
			弁理士 岩▲崎▼ 幸邦
		(74) 代理人	100095500
			弁理士 伊藤 正和
		(74) 代理人	100101247
			弁理士 高橋 俊一
		(74) 代理人	100117064
			弁理士 伊藤 市太郎

最終頁に続く

(54) 【発明の名称】 移動通信システム、移動局及び無線基地局

(57) 【特許請求の範囲】

【請求項 1】

移動局が、無線基地局との間で、複数の周波数キャリアを用いて通信を行うように構成されている移動通信システムであって、

前記移動局は、前記複数の周波数キャリアの全てに対して同じ鍵を適用して通信のセキュリティ処理を行うように構成されており、

前記移動局は、前記複数の周波数キャリアのいずれか 1 つの物理セル ID 及び周波数コードに基づいて、前記鍵を生成するように構成されていることを特徴とする移動通信システム。

【請求項 2】

前記複数の周波数キャリアの全てに対して同じセキュリティ処理のアルゴリズムが適用されることを特徴とする請求項 1 に記載の移動通信システム。

【請求項 3】

前記複数の周波数キャリアのいずれか 1 つは、前記無線基地局によって指定されるアンカーキャリアであることを特徴とする請求項 1 に記載の移動通信システム。

【請求項 4】

前記アンカーキャリアが、前記無線基地局によって変更される場合、前記移動局は、変更後の前記アンカーキャリアの物理セル ID 及び周波数コードに基づいて、前記鍵を生成するように構成されていることを特徴とする請求項 3 に記載の移動通信システム。

【請求項 5】

10

20

無線基地局との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている通信部を具備し、

前記通信部は、前記複数の周波数キャリアの全てに対して同じ鍵を適用して通信のセキュリティ処理を行うように構成されており、

前記複数の周波数キャリアのいずれか1つの物理セルID及び周波数コードに基づいて、前記鍵を生成するように構成されている鍵生成部を具備することを特徴とする移動局。

【請求項6】

前記通信部は、前記複数の周波数キャリアの全てに対して同じセキュリティ処理のアルゴリズムを用いるように構成されていることを特徴とする請求項5に記載の移動局。

【請求項7】

前記複数の周波数キャリアのいずれか1つは、前記無線基地局によって指定されるアンカーキャリアであることを特徴とする請求項5に記載の移動局。

【請求項8】

前記アンカーキャリアが、前記無線基地局によって変更される場合、前記鍵生成部は、変更後の前記アンカーキャリアの物理セルID及び周波数コードに基づいて、前記鍵を生成するように構成されていることを特徴とする請求項7に記載の移動局。

【請求項9】

移動局との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている通信部を具備し、

前記通信部は、前記複数の周波数キャリアの全てに対して同じ鍵を適用して通信のセキュリティ処理を行うように構成されており、

前記複数の周波数キャリアのいずれか1つの物理セルID及び周波数コードに基づいて、前記鍵を生成するように構成されている鍵生成部を具備することを特徴とする無線基地局。

【請求項10】

前記通信部は、前記複数の周波数キャリアの全てに対して同じセキュリティ処理のアルゴリズムを用いるように構成されていることを特徴とする請求項9に記載の無線基地局。

【請求項11】

前記複数の周波数キャリアのいずれか1つは、前記無線基地局によって指定されるアンカーキャリアであることを特徴とする請求項9に記載の無線基地局。

【請求項12】

前記アンカーキャリアが、変更される場合、前記鍵生成部は、変更後の前記アンカーキャリアの物理セルID及び周波数コードに基づいて、前記鍵を生成するように構成されていることを特徴とする請求項11に記載の無線基地局。

【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、移動局及び無線基地局に関する。

【背景技術】

【0002】

LTE (Long Term Evolution) 方式の後継の通信方式であるLTE-Advanced方式の移動通信システムでは、移動局UEが、無線基地局eNBとの間で、複数の周波数キャリアを同時に用いて通信を行う「Carrier Aggregation」と呼ばれる技術が利用可能である。

【0003】

「Carrier Aggregation」を構成する周波数キャリアは、「Component Carrier」と呼ばれる。

【0004】

各「Component Carrier」は、独立したLTE方式のセルとして機能する場合もある。すなわち、異なる周波数キャリアを用いるLTE方式のセルを「Com

10

20

30

40

50

ponent Carrier」として、「Carrier Aggregation」を行うことも可能である。

【0005】

よって、LTE-Advanced方式では、「Carrier Aggregation」によって、異なる周波数キャリアを用いる複数のLTE方式のセルを同時に利用して通信することができる。

【0006】

ここで、LTE方式では、無線セキュリティ処理に用いる鍵K<sub>eNB</sub>は、通信中セルの「PCI (Physical Cell Identity、物理セルID)」及び「E-ARFCN (E-UTRA Absolute Radio Frequency Channel Number、周波数コード)」の両方に依存する。

10

【0007】

これは、鍵K<sub>eNB</sub>を生成する際に、PCI及びE-ARFCNをパラメータとした鍵生成関数KDF (Key Derivation Function) を用いるためである。

【0008】

また、かかる鍵K<sub>eNB</sub>は、移動局UE毎に異なる親鍵K<sub>ASME</sub>から生成される。したがって、LTE方式では、かかる鍵K<sub>eNB</sub>は、セル固有 (cell specific) かつ移動局UE固有 (UE specific) となる。

20

【先行技術文献】

【非特許文献】

【0009】

【非特許文献1】3GPP TS 33.401

【非特許文献2】3GPP TS 36.331

【発明の概要】

【発明が解決しようとする課題】

【0010】

しかしながら、かかるLTE-Advanced方式の移動通信システムでは、「Carrier Aggregation」における無線セキュリティ処理について規定されていないという問題点があった。

30

【0011】

そこで、本発明は、上述の課題に鑑みてなされたものであり、「Carrier Aggregation」における無線セキュリティ処理を適切に実現することができる移動通信システム、移動局及び無線基地局を提供することを目的とする。

【課題を解決するための手段】

【0012】

本発明の第1の特徴は、移動通信システムであって、移動局が、無線基地局との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている移動通信システムであって、前記移動局は、前記複数の周波数キャリアの各々に対して同一の鍵を適用して通信を行うように構成されていることを要旨とする。

40

【0013】

本発明の第2の特徴は、移動局であって、無線基地局との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている通信部を具備し、前記通信部は、前記複数の周波数キャリアの各々に対して同一の鍵を適用して通信のセキュリティ処理を行うように構成されていることを要旨とする。

【0014】

本発明の第3の特徴は、無線基地局であって、移動局との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている通信部を具備し、前記通信部は、前記複数の周波数キャリアの各々に対して同一の鍵を適用して通信のセキュリティ処理を行うように構成されていることを要旨とする。

50

## 【発明の効果】

## 【0015】

以上説明したように、本発明によれば、「Carrier Aggregation」における無線セキュリティ処理を適切に実現することができる移動通信システム、移動局及び無線基地局を提供することができる。

## 【図面の簡単な説明】

## 【0016】

【図1】本発明の第1の実施形態に係る移動通信システムの全体構成図である。

【図2】本発明の第1の実施形態に係る移動通信システムのプロトコルスタック図である。

10

【図3】本発明の第1の実施形態に係る移動通信システムにおいて3個のPDCP-SDUが送信される場合の例について説明するための図である。

【図4】本発明の第1の実施形態に係る移動局の機能ブロック図である。

【図5】本発明の第1の実施形態に係る無線基地局の機能ブロック図である。

【図6】本発明の第1の実施形態に係る移動通信システムの動作を示すシーケンス図である。

## 【発明を実施するための形態】

## 【0017】

(本発明の第1の実施形態に係る移動通信システム)

図1乃至図3を参照して、本発明の第1の実施形態に係る移動通信システムについて説明する。

20

## 【0018】

本実施形態に係る移動通信システムは、LTE-Advanced方式の移動通信システムであって、かかる移動通信システムにおいて、移動局UEは、無線基地局eNBとの間で、複数の周波数キャリアを同時に用いて通信を行うことができる、すなわち、「Carrier Aggregation」を利用可能である。

## 【0019】

本実施形態では、図1に示すように、移動局UEは、「PCI(Physical Cell ID)=1」によって特定されるセル#1における周波数キャリアF1と、「PCI=2」によって特定されるセル#2における周波数キャリアF2と、「PCI=3」によって特定されるセル#3における周波数キャリアF3とを同時に用いて通信を行うことができる。

30

## 【0020】

ここで、セル#1乃至セル#3は、全て無線基地局eNB配下のセルであるものとする。なお、セル#1乃至セル#3は、それぞれ独立したLTE方式のセルであってもよい。

## 【0021】

図2に示すように、本実施形態に係る移動通信システムにおいて、移動局UE及び無線基地局eNBは、物理(PHY)レイヤ機能と、MAC(Media Access Control)レイヤ機能と、RLC(Radio Link Control)レイヤ機能と、PDCP(Packet Data Convergence Protocol)レイヤ機能とを具備している。

40

## 【0022】

PDCPレイヤ機能は、移動局UEと無線基地局eNBとの間の通信における無線セキュリティ処理を行うように構成されている。

## 【0023】

また、RLCレイヤ機能は、RLCレイヤにおける再送制御を行うように構成されており、MACレイヤ機能は、HARQ再送制御を行うように構成されている。

## 【0024】

図3に、3個のPDCP-SDU#1~#3が送信される場合の例について示す。

## 【0025】

50

図3に示すように、第1に、PDCPレイヤ機能は、U-planeのPDCP-SDU #1~#3に対して、秘匿(Ciphering)処理を施して、PDCP-PDU #1~#3を生成して、RLCレイヤ機能に渡す。

【0026】

一方、PDCPレイヤ機能は、C-planeのPDCP-SDU #1~#3に対して、秘匿(Ciphering)処理を施すことに加えて、改竄保護(Integrity Protection)処理用のMAC-Iを付与して、PDCP-PDU #1~#3を生成して、RLCレイヤ機能に渡す。

【0027】

第2に、RLCレイヤ機能は、スケジューラによって指定されたTBS(Transmission Block Size)のRLC-PDU #1~#4を生成するように、セグメント処理(Segmentation)又は連結処理(Concatenation)を施し、RLCヘッダを付与する。

10

【0028】

なお、RLCレイヤ機能は、AMモードで起動している場合、RLCレイヤにおける再送制御を行う。

【0029】

第3に、RLCレイヤ機能は、生成したRLC-PDU #1~#4を、MACレイヤ機能に渡す。

【0030】

20

第4に、MACレイヤ機能は、RLC-PDU #1~#4に対してMACヘッダを付与して、MAC-PDU #1~#4を生成し、HARQ再送制御を用いて、物理レイヤ機能に対して送信する。

【0031】

図4に示すように、移動局UEは、取得部11と、鍵生成部12と、通信部13とを具備している。

【0032】

取得部11は、無線基地局eNBから、かかる無線基地局eNB配下の各セルを特定するための「PCI」及び各セルで用いられている周波数キャリアを特定するための「E-ARFCN(E-UTRA Absolute Radio Frequency Channel Number)」を取得するように構成されている。

30

【0033】

鍵生成部12は、取得部11によって取得された「PCI」及び「E-ARFCN」に基づいて、鍵KeNBを生成するように構成されている。

【0034】

例えば、鍵生成部12は、鍵生成関数KDF(PCI, E-ARFCN)によって、鍵KeNBを生成するように構成されていてもよい。

【0035】

ここで、鍵KeNBは、PDCPレイヤ機能における無線セキュリティ処理で用いられる鍵(K<sub>UPEnc</sub>、K<sub>RRCEnc</sub>、K<sub>RRCint</sub>)を生成するための鍵である。

40

【0036】

K<sub>UPEnc</sub>は、U-planeの秘匿処理用の鍵であり、K<sub>RRCEnc</sub>は、C-planeの秘匿処理用の鍵であり、K<sub>RRCint</sub>は、C-planeの改竄保護処理用の鍵であり、これらは、いずれも鍵KeNBから生成される。

【0037】

なお、鍵生成部12は、「Carrier Aggregation」が用いられている場合、複数の周波数キャリアの全てに適用する1つの鍵KeNBを生成するように構成されている。

【0038】

また、鍵生成部12は、「Carrier Aggregation」が用いられてい

50

る場合、PDCPレイヤ機能における無線セキュリティ処理で用いられる鍵 ( $K_{UPenc}$ 、 $K_{RRCenc}$ 、 $K_{RRCint}$ ) についても、複数の周波数キャリアの全てに適用する一組の鍵 ( $K_{UPenc}$ 、 $K_{RRCenc}$ 、 $K_{RRCint}$ ) を生成するように構成されている。

【0039】

すなわち、鍵生成部12は、「Carrier Aggregation」が用いられている場合、複数の周波数キャリアのいずれか1つの「PCI」及び「E-ARFCN」に基づいて、具体的には、「Anchor Carrier」の「PCI」及び「E-ARFCN」に基づいて、かかる鍵  $K_{eNB}$  を生成するように構成されている。

【0040】

ここで、「Carrier Aggregation」を構成する複数の周波数キャリアの中から、「Anchor Carrier」が1つ決定される。

【0041】

例えば、「Anchor Carrier」は、「Connection Setup」時や、「Security Mode Command」時や、「Reconfiguration」時や、「Intra-RAT Handover」時や、「Inter-RAT Handover」時や、「Re-establishment」時等において、無線基地局  $eNB$  から移動局  $UE$  に対して設定される。

【0042】

或いは、「Anchor Carrier」は、移動局  $UE$  が  $RRC$  コネクションを最初に確立した周波数キャリアとして、定められてもよい。

【0043】

なお、鍵生成部12は、「Anchor Carrier」が変更になる場合、再度、変更後の「Anchor Carrier」の「PCI」及び「E-ARFCN」に基づいて、上述の鍵  $K_{eNB}$  を生成するように構成されていてもよい。

【0044】

「Anchor Carrier」が変更される場合、無線基地局  $eNB$  から、 $eNB$  内ハンドオーバ ( $intra-eNB handover$ ) が起動されてもよい。 $Intra-eNB handover$  が指示された場合、移動局  $UE$  は、「Anchor Carrier」を変更すると同時に、鍵  $K_{eNB}$  を更新し、 $LTE$  方式のハンドオーバと同様に、 $PHY$ 、 $MAC$ 、 $RLC$  の各レイヤのリセット処理を行ってもよい。

【0045】

通信部13は、上述の物理 ( $PHY$ ) レイヤ機能と  $MAC$  レイヤ機能と  $RLC$  レイヤ機能と  $PDCP$  レイヤ機能とによって構成されており、無線基地局  $eNB$  との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている。

【0046】

なお、 $PDCP$  レイヤにおいて使用される秘匿処理及び改竄保護処理のアルゴリズムについても、複数の周波数キャリアの各々において同一となるように構成されている。

【0047】

使用するアルゴリズムは、無線基地局  $eNB$  から、「Security Mode Command」時や、「Reconfiguration」時や、「Intra-RAT Handover」時や、「Inter-RAT Handover」時や、「Re-establishment」時等において、無線基地局  $eNB$  から移動局  $UE$  に対して設定される。

【0048】

図5に示すように、無線基地局  $eNB$  は、鍵生成部21と、通信部22とを具備している。ここで、鍵生成部21は、図4に示す鍵生成部12と同様の機能を具備し、通信部22は、図4に示す通信部13と同様の機能を具備する。

【0049】

以下、図6を参照して、本実施形態に係る移動通信システムの動作について説明する。

10

20

30

40

50

## 【0050】

図6に示すように、ステップS1001において、移動局UEは、無線基地局eNBに対して、セル#1との間で通信(RRC(Radio Resource Control)コネクション)の確立を要求するための「RRC Connection Request」を送信する。

## 【0051】

ステップS1002において、無線基地局eNBは、移動局UEに対して、ステップS1001において受信した「RRC Connection Request」に対する「RRC Connection Setup」を送信する。

## 【0052】

ステップS1003において、移動局UEは、無線基地局eNBに対して、「RRC Connection Setup Complete」を送信する。

## 【0053】

その結果、ステップS1004において、移動局UEと無線基地局eNBとの間で、周波数キャリアF1を用いたRRCコネクションが確立され、かかるRRCコネクションを介した通信が開始される。

## 【0054】

その後、ステップS1005において、無線基地局eNBは、移動局UEに対して、周波数キャリアF1を使って確立されたRRCコネクションに係る「RRC Connection Reconfiguration」を送信する。

## 【0055】

かかる「RRC Connection Reconfiguration」は、通信に用いる無線リソースとして、周波数キャリアF2を追加することを設定するものである。

## 【0056】

ステップS1006において、移動局UEは、無線基地局eNBに対して、「RRC Connection Reconfiguration Complete」を送信する。

## 【0057】

その結果、ステップS1007において、移動局UEと無線基地局eNBとの間で、周波数キャリアF1及び周波数キャリアF2を同時に用いた通信が開始される。

## 【0058】

同様に、他の周波数キャリアが追加され、3つ以上の周波数キャリアを同時に用いた通信を行うこともできる。また、通信中に一部の周波数キャリアを解放し、周波数キャリア数を変更することもできる。

## 【0059】

一般的に、LTE-Advanced方式の移動通信システムでは、HARQ再送制御において残留誤りが存在する場合、RLCレイヤにおける再送制御が行われる。

## 【0060】

ここで、RLCレイヤにおける再送では、初送時と異なる「Component Carrier」でRLC-PDUが再送される場合がある。

## 【0061】

しかし、RLC-PDUには、1個以上の秘匿処理後のPDCP-PDUが含まれている。したがって、LTE方式を踏襲して各周波数キャリアに依存した鍵KeNBを用いた場合、以下の点が懸念される。

## 【0062】

・ RLC-PDUを、初送時と異なる「Component Carrier」を用いて再送しようとした場合に、一旦、PDCPレイヤの秘匿を解除して、再送で用いられる「Component Carrier」に合わせた秘匿処理を再度行って、RLC-PDUを生成し直さなければならないことが想定される。

10

20

30

40

50

## 【 0 0 6 3 】

・ また、かかる L T E - A d v a n c e d 方式の移動通信システムでは、P D C P - P D U のセグメントごとに、異なる「C o m p o n e n t   C a r r i e r 」を用いたコネクションで送信する場合、受信側で、受信された P D C P - P D U のセグメントごとに秘匿処理に用いた鍵が異なることになり、P D C P - P D U の復号処理が極めて困難になることが想定される。

## 【 0 0 6 4 】

しかしながら、本実施形態に係る移動通信システムによれば、R R C コネクションを形成する複数の「C o m p o n e n t   C a r r i e r 」に対して1つの鍵 K e N B が用いられるため、上述の不具合を回避することができる。

10

## 【 0 0 6 5 】

以上に述べた本実施形態の特徴は、以下のように表現されていてもよい。

## 【 0 0 6 6 】

本実施形態の第1の特徴は、移動通信システムであって、移動局 U E が、無線基地局 e N B との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている移動通信システムであって、移動局 U E は、かかる周波数キャリアの全てに対して同じ鍵 K e N B を適用して通信のセキュリティ処理を行うように構成されていることを要旨とする。

## 【 0 0 6 7 】

本実施形態の第1の特徴において、移動局 U E は、「A n c h o r   C a r r i e r ( 複数の周波数キャリアのいずれか1つ ) 」の「P C I ( 物理セル I D ) 」及び「E - A R F C N ( 周波数コード ) 」に基づいて、かかる鍵 K e N B を生成するように構成されていてもよい。

20

## 【 0 0 6 8 】

本実施形態の第1の特徴において、上述の周波数キャリアの全てに対して同じセキュリティ処理 ( 秘匿処理及び改竄防止処理 ) のアルゴリズムを用いるように構成されていてもよい。

## 【 0 0 6 9 】

本実施形態の第1の特徴において、「A n c h o r   C a r r i e r ( アンカーキャリア ) 」は、前記無線基地局によって指定されてもよい。

30

## 【 0 0 7 0 】

本実施形態の第1の特徴において、「A n c h o r   C a r r i e r 」が、無線基地局 e N B によって変更される場合、移動局 U E は、変更後の「A n c h o r   C a r r i e r 」の「P C I 」及び「E - A R F C N 」に基づいて、上述の鍵 K e N B を生成するように構成されていてもよい。

## 【 0 0 7 1 】

本実施形態の第2の特徴は、移動局 U E であって、無線基地局 e N B との間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている通信部 1 3 を具備し、通信部 1 3 は、かかる周波数キャリアの全てに対して同じ鍵 K e N B を適用して通信のセキュリティ処理を行うように構成されていることを要旨とする。

40

## 【 0 0 7 2 】

本実施形態の第2の特徴において、「A n c h o r   C a r r i e r 」の「P C I 」及び「E - A R F C N 」に基づいて、かかる鍵 K e N B を生成するように構成されている鍵生成部 1 2 を具備してもよい。

## 【 0 0 7 3 】

本実施形態の第2の特徴において、通信部 1 3 は、上述の周波数キャリアの全てに対して同じセキュリティ処理 ( 秘匿処理及び改竄防止処理 ) のアルゴリズムを用いるように構成されていてもよい。

## 【 0 0 7 4 】

本実施形態の第2の特徴において、「A n c h o r   C a r r i e r 」は、無線基地局

50



eNBによって指定されてもよい。

【0075】

本実施形態の第2の特徴において、「Anchor Carrier」が、無線基地局eNBによって変更される場合、鍵生成部12は、変更後の「Anchor Carrier」の「PCI」及び「E-ARFCN」に基づいて、上述の鍵KeNBを生成するように構成されていてもよい。

【0076】

本実施形態の第3の特徴は、無線基地局eNBであって、移動局UEとの間で、複数の周波数キャリアを同時に用いて通信を行うように構成されている通信部22を具備し、通信部22は、かかる周波数キャリアの全てに対して同じの鍵KeNBを適用して通信のセキュリティ処理を行うように構成されていることを要旨とする。

10

【0077】

本実施形態の第3の特徴において、「Anchor Carrier」の「PCI」及び「E-ARFCN」に基づいて、かかる鍵KeNBを生成するように構成されている鍵生成部21を具備してもよい。

【0078】

本実施形態の第3の特徴において、通信部22は、上述の周波数キャリアの全てに対して同じセキュリティ処理（秘匿処理及び改竄防止処理）のアルゴリズムを用いるように構成されていてもよい。

【0079】

20

本実施形態の第3の特徴において、「Anchor Carrier」が、変更される場合、鍵生成部21は、変更後の「Anchor Carrier」の「PCI」及び「E-ARFCN」に基づいて、上述の鍵KeNBを生成するように構成されていてもよい。

【0080】

なお、上述の無線基地局eNBや移動局UEの動作は、ハードウェアによって実施されてもよいし、プロセッサによって実行されるソフトウェアモジュールによって実施されてもよいし、両者の組み合わせによって実施されてもよい。

【0081】

ソフトウェアモジュールは、RAM(Random Access Memory)や、フラッシュメモリや、ROM(Read Only Memory)や、EPROM(Erasable Programmable ROM)や、EEPROM(Electronically Erasable and Programmable ROM)や、レジスタや、ハードディスクや、リムーバブルディスクや、CD-ROMといった任意形式の記憶媒体内に設けられていてもよい。

30

【0082】

かかる記憶媒体は、プロセッサが当該記憶媒体に情報を読み書きできるように、当該プロセッサに接続されている。また、かかる記憶媒体は、プロセッサに集積されていてもよい。また、かかる記憶媒体及びプロセッサは、ASIC内に設けられていてもよい。かかるASICは、無線基地局eNBや移動局UE内に設けられていてもよい。また、かかる記憶媒体及びプロセッサは、ディスクリットコンポーネントとして無線基地局eNBや移動局UE内に設けられていてもよい。

40

【0083】

以上、上述の実施形態を用いて本発明について詳細に説明したが、当業者にとっては、本発明が本明細書中に説明した実施形態に限定されるものではないということは明らかである。本発明は、特許請求の範囲の記載により定まる本発明の趣旨及び範囲を逸脱することなく修正及び変更態様として実施することができる。従って、本明細書の記載は、例示説明を目的とするものであり、本発明に対して何ら制限的な意味を有するものではない。

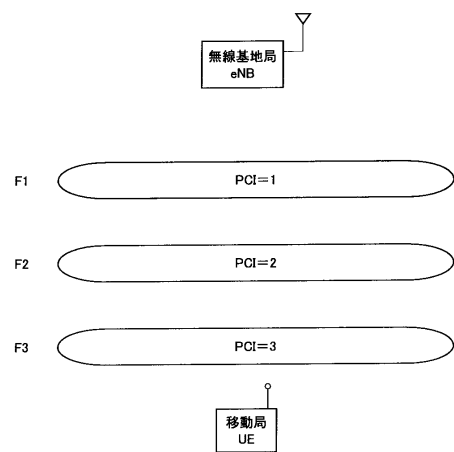
【符号の説明】

【0084】

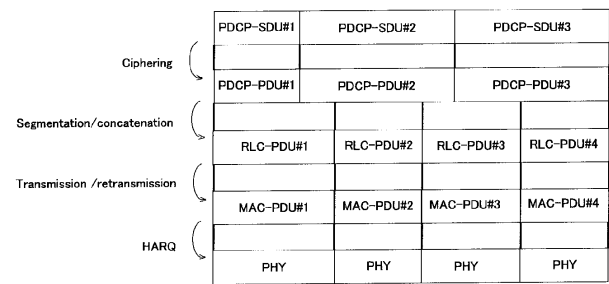
50

e N B ...無線基地局  
U E ...移動局  
1 1 ...取得部  
1 2、2 1 ...鍵生成部  
1 3、2 2 ...通信部

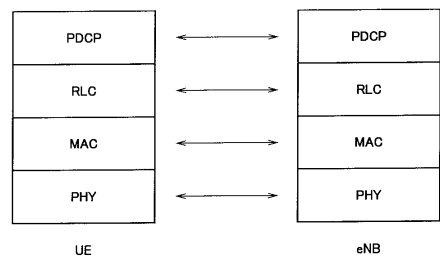
【図 1】



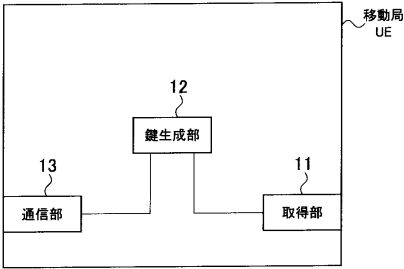
【図 3】



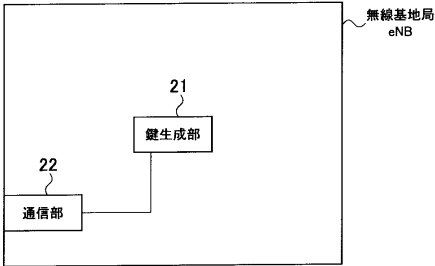
【図 2】



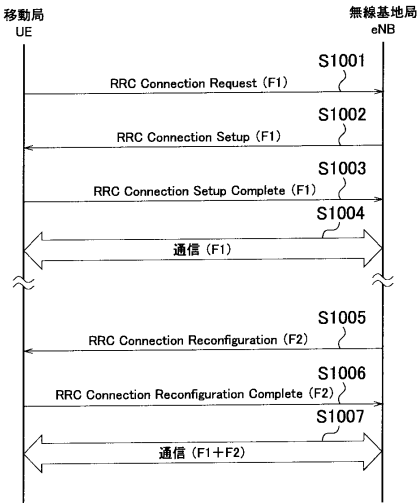
【図 4】



【図 5】



【図 6】



---

フロントページの続き

(72)発明者 岩村 幹生

東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

(72)発明者 ウリ アンダルマワンティ ハブサリ

東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

審査官 北川 純次

(56)参考文献 特開 2 0 0 6 - 3 5 2 2 2 5 ( J P , A )

特開 2 0 0 5 - 2 0 0 7 6 ( J P , A )

Fujitsu , Anchor component carrier , 3GPP TSG-RAN1 #57 R1-091966 , 2 0 0 9 年 5 月

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture; , 3GPP TS 33.

401 V9.0.0 , 2 0 0 9 年 6 月 , p.19-26,36-39,63

(58)調査した分野(Int.Cl. , D B 名)

H 0 4 B 7 / 2 4 - 7 / 2 6

H 0 4 W 4 / 0 0 - 9 9 / 0 0