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

特許第4465015号
(P4465015)

(45)発行日　平成22年5月19日(2010.5.19)　(24)登録日　平成22年2月26日(2010.2.26)

(51)Int.Cl.　F I
H04W 12/04 (2009.01)　H04Q 7/00 182
H04W 36/14 (2009.01)　H04Q 7/00 309

請求項の数 14　(全 21 頁)

(21)出願番号　特願2008-162617(P2008-162617)
(22)出願日　平成20年6月20日(2008.6.20)
(65)公開番号　特開2010-4412(P2010-4412A)
(43)公開日　平成22年1月7日(2010.1.7)
審査請求日　平成21年6月15日(2009.6.15)

(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
(74)代理人　100083806
弁理士　三好　秀和
(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】移動通信方法

(57)【特許請求の範囲】
【請求項１】
無線基地局間インタフェースを用いて、移動局がハンドオーバ元無線基地局からハンドオーバ先無線基地局にハンドオーバする移動通信方法であって、
前記ハンドオーバ先無線基地局は、前記ハンドオーバ元無線基地局から、該ハンドオーバ先無線基地局と前記移動局との間の通信に用いられる所定鍵を生成するための第１鍵を取得する工程Ａと、
前記ハンドオーバ先無線基地局は、交換局から、次のハンドオーバ先無線基地局と前記移動局との間の通信に用いられる所定鍵を生成するための第２鍵を取得する工程Ｂとを有することを特徴とする移動通信方法。
【請求項２】
前記移動局が、前記ハンドオーバ元無線基地局からハンドオーバ指示信号を受信した際に、該ハンドオーバ元無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵を、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵に更新する工程Ｃを有することを特徴とする請求項１に記載の移動通信方法。
【請求項３】
前記工程Ｃにおいて、前記移動局は、前記ハンドオーバ指示信号に含まれるパラメータに基づいて、前記ハンドオーバ元無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵を、前記ハンドオーバ先無線基地局と該移動局との間の通信に用

いられる所定鍵を生成するための第１鍵に更新することを特徴とする請求項２に記載の移動通信方法。

【請求項４】

前記工程Ｃは、

前記ハンドオーバ指示信号に含まれるパラメータがインクリメントされている場合、前記移動局は、該パラメータに基づいて、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵を生成する工程Ｃ１と、

前記ハンドオーバ指示信号に含まれるパラメータがインクリメントされていない場合、前記移動局は、前記ハンドオーバ元無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵に基づいて、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵を生成する工程Ｃ２とを具備することを特徴とする請求項３に記載の移動通信方法。

【請求項５】

前記工程Ｃ１において、前記ハンドオーバ指示信号に含まれるパラメータがインクリメントされている場合、前記移動局は、該パラメータに基づいて、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第２鍵に更新し、更新された該第２鍵に基づいて、該ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵を生成することを特徴とする請求項４に記載の移動通信方法。

【請求項６】

前記パラメータは、ＫＩであることを特徴とする請求項４又は５に記載の移動通信方法。

【請求項７】

前記移動局が、受信した前記パラメータを記憶しておく工程Ｄを更に有することを特徴とする請求項３乃至６のいずれか一項に記載の移動通信方法。

【請求項８】

無線基地局間インタフェースを用いて、移動局がハンドオーバ元無線基地局からハンドオーバ先無線基地局にハンドオーバする際に該ハンドオーバ先無線基地局として機能する無線基地局であって、

前記ハンドオーバ元無線基地局から、前記ハンドオーバ先無線基地局と前記移動局との間の通信に用いられる所定鍵を生成するための第１鍵を取得するように構成されている第１取得部と、

交換局から、次のハンドオーバ先無線基地局と前記移動局との間の通信に用いられる所定鍵を生成するための第２鍵を取得するように構成されている第２取得部とを具備することを特徴とする無線基地局。

【請求項９】

ハンドオーバ元無線基地局からハンドオーバ先無線基地局にハンドオーバする移動局であって、

前記ハンドオーバ元無線基地局からのハンドオーバ指示信号を受信した際に、該ハンドオーバ元無線基地局と前記移動局との間の通信に用いられる所定鍵を生成するための第１鍵を、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵に更新するように構成されている鍵更新部を具備することを特徴とする移動局。

【請求項１０】

前記鍵更新部は、前記ハンドオーバ指示信号に含まれるパラメータに基づいて、前記ハンドオーバ元無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵を、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵に更新するように構成されていることを特徴とする請求項９に記載の移動局。

【請求項１１】

前記鍵更新部は、前記ハンドオーバ指示信号に含まれるパラメータがインクリメントされている場合、該パラメータに基づいて、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵を生成するように構成されており、

前記鍵更新部は、前記ハンドオーバ指示信号に含まれるパラメータがインクリメントされていない場合、前記ハンドオーバ元無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１鍵に基づいて、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１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１０に記載の移動局。

【請求項１２】

前記鍵更新部は、前記ハンドオーバ指示信号に含まれるパラメータがインクリメントされている場合、前記移動局は、該パラメータに基づいて、前記ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第２鍵に更新し、更新された該第２鍵に基づいて、該ハンドオーバ先無線基地局と該移動局との間の通信に用いられる所定鍵を生成するための第１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に記載の移動局。

【請求項１３】

前記パラメータは、ＫＩであることを特徴とする請求項１１又は１２に記載の移動局。

【請求項１４】

前記鍵更新部は、受信した前記パラメータを記憶しておくように構成されていることを特徴とする請求項１１乃至１３のいずれか一項に記載の移動局。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、所定鍵を用いて移動局と無線基地局との間の通信を行う移動通信方法に関する。

【背景技術】

【０００２】

従来、３ＧＰＰで規定されているＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）方式の移動通信システムでは、所定鍵を用いて、移動局ＵＥと無線基地局ｅＮＢとの間の通信を行うように構成されている。

【０００３】

所定鍵としては、例えば、移動局ＵＥと無線基地局ｅＮＢとの間（Ａｃｃｅｓｓ　Ｓｔｒａｔｕｍ、ＡＳ）のＣプレーンプロトコルであるＲＲＣプロトコルにおける「Ｃｉｐｈｅｒｉｎｇ」で用いられる鍵K_{RRC_Ciph}や、同ＲＲＣプロトコルにおける「Ｉｎｔｅｇｒｉｔｙ　Ｐｒｏｔｅｃｔｉｏｎ」で用いられる鍵K_{RRC_IP}や、移動局ＵＥと無線基地局ｅＮＢとの間（Ａｃｃｅｓｓ　Ｓｔｒａｔｕｍ、ＡＳ）のＵプレーンにおける「Ｃｉｐｈｅｒｉｎｇ」で用いられる鍵K_{UP_Ciph}等が挙げられる。なお、かかる所定鍵は、第１鍵K_{eNB}を用いて生成される。

【０００４】

かかる所定鍵や第１鍵K_{eNB}は、長時間同一のものを用いると、セキュリティ上システムが脆弱となり、好ましくない。そこで、ハンドオーバを行った際に、かかる所定鍵や第１鍵K_{eNB}を更新する手順が、３ＧＰＰにおいて考案されている。

【０００５】

ここで、図１２を参照して、移動局ＵＥのハンドオーバ手順において、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）が、所定鍵の生成に用いる第１鍵K_{eNB}＊＊を取得する動作について説明する。

【０００６】

図１２に示すように、第１に、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）が、記憶している第１鍵K_{eNB}と、パラメータ「Ｎｅｘｔ　Ｈｏｐ」と、ハンドオーバの種類を示すパラメータ「Ｈａｎｄｏｖｅｒ　Ｔｙｐｅ」と、ハンドオーバ先セルの識別情

報を示すパラメータ「Ｔａｒｇｅｔ　ＰＣＩ」とに基づいて、中間鍵K_{eNB}^{*}を生成する。

【０００７】

第２に、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）が、生成した中間鍵K_{eNB}^{*}を、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）に送信する。

【０００８】

第３に、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）が、受信した中間鍵K_{eNB}^{*}と、ハンドオーバ先セルによって割り当てられた「C-ＲＮＴＩ（Ｃｅｌｌ　Ｒａｄｉｏ　Ｎｅｔｗｏｒｋ　Ｔｅｍｐｏｒａｒｙ　ＩＤ）」とに基づいて、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）において所定鍵の生成に用いられる第１鍵K_{eNB}^{**}を生成する。

【非特許文献１】３ＧＰＰ　ＴＳ３３．４０１　ｖ８．０．０

【発明の開示】

【発明が解決しようとする課題】

【０００９】

しかしながら、上述のように、従来の移動通信システムのハンドオーバ手順では、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）及びハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）の双方で、複数のパラメータや関数を用いて、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）で用いられる第１鍵K_{eNB}^{**}を生成しなければならないという問題点があった。

【００１０】

特に、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）とハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）とで、異なるパラメータを用いたK_{eNB}変換関数（Ｋｅｙ　Ｄｅｒｉｖａｔｉｏｎ　Ｆｕｎｃｔｉｏｎ、ＫＤＦ）を用いなければならず、移動局ＵＥにおいても、これらのＫＤＦを装備する必要があり、複雑である問題があった。

【００１１】

また、ハンドオーバ先無線基地局のＰＣＩ（Ｐｈｙｓｉｃａｌ　Ｃｅｌｌ　ＩＤ）に応じて、K_{eNB}を更新する必要がある煩雑性があった。

【００１２】

更には、Ｃ－ＲＮＴＩに応じて、K_{eNB}を更新する必要があるため、C-ＲＮＴＩの変更割当を柔軟に行うことに制約があった。

【００１３】

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、簡素化された手順で、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）で用いられる第１鍵を生成することができる移動通信方法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】

【００１４】

本発明の第１の特徴は、所定鍵を用いて移動局と無線基地局との間の通信を行う移動通信方法であって、移動局のハンドオーバ手順において、ハンドオーバ先無線基地局は、該移動局との間の通信に用いられる所定鍵を生成するための第１鍵と、次のハンドオーバ先無線基地局と移動局との間の通信に用いられる所定鍵を生成するための第１鍵の両方を取得することを要旨とする。

【発明の効果】

【００１５】

以上説明したように、本発明によれば、簡素化された手順で、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）で用いられる第１鍵を生成することができる移動通信方法を提供することができる。

【発明を実施するための最良の形態】

【００１６】

（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６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。

【００１７】

本実施形態に係る移動通信システムは、ＬＴＥ方式が適用されている移動通信システムであって、図１に示すように、複数の交換局ＭＭＥ＃１、＃２…と、複数の無線基地局ｅＮＢ＃１１、＃１２、＃２１、＃２２…とを具備している。

【００１８】

例えば、移動局ＵＥは、無線基地局ｅＮＢ＃１１配下のセル＃１１１において、上述の所定鍵を用いて、無線基地局ｅＮＢ＃１１との間で通信を行うように構成されている。

【００１９】

また、移動局ＵＥのハンドオーバ手順において、ハンドオーバ先無線基地局（例えば、無線基地局ｅＮＢ＃１２）は、ハンドオーバ元無線基地局（例えば、無線基地局ｅＮＢ＃１１）によって生成される中間鍵$K_{eNB}{}^{*}$を用いることなく、移動局ＵＥとの間の通信に用いられる所定鍵を生成するための第１鍵K_{eNB}［ｎ＋１］、K_{eNB}［ｎ＋２］等を取得するように構成されている。

【００２０】

図２に、本実施形態に係る移動通信システムで用いられる鍵（すなわち、所定鍵の算出に用いられる鍵）の階層構造及び算出手順の一例について示す。

【００２１】

図２に示すように、ＲＲＣプロトコルにおける「Ｉｎｔｅｇｒｉｔｙ　Ｐｒｏｔｅｃｔｉｏｎ」で用いられる鍵K_{RRC_IP}、ＲＲＣプロトコルにおける「Ｃｉｐｈｅｒｉｎｇ」で用いられる鍵K_{RRC_Ciph}及びＡＳのＵプレーンにおける「Ｃｉｐｈｅｒｉｎｇ」で用いられる鍵K_{UP_Ciph}は、第１鍵$K_{eNB[n]}$を用いて生成される。

【００２２】

また、第１鍵$K_{eNB[n]}$は、親鍵K_{ASME}を用いて、下記の式によって算出される。

【００２３】

$K_{eNB[0]}=KDF_0(K_{ASME}, NAS\ SN)$

$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$，（$n \geqq 0$）

【００２４】

ここで、親鍵K_{ASME}は、移動局ＵＥ及び交換局ＭＭＥのみによって知られているものであり、無線基地局ｅＮＢによって知られてはならないものである。

【００２５】

また、ＮＡＳ　ＳＮは、移動局ＵＥと交換局ＭＭＥとの間（Ｎｏｎ　Ａｃｃｅｓｓ　Ｓｔｒａｔｕｍ、ＮＡＳ）のＣプレーンプロトコルであるＮＡＳプロトコルのシーケンス番号（Ｓｅｑｕｅｎｃｅ　Ｎｕｍｂｅｒ、ＳＮ）である。

【００２６】

以下、図３乃至図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。

【００２７】

第１に、図３を参照して、本実施形態に係る移動通信システムにおける初期設定手順（Ｉｎｉｔｉａｌ　Ｅｓｔａｂｌｉｓｈｍｅｎｔ　Ｐｒｏｃｅｄｕｒｅ）について説明する。

【００２８】

図３に示すように、初期設定手順の開始前の段階では、移動局ＵＥは、K_{ASME}を保持しており（ステップＳ１０１）、無線基地局ｅＮＢは、所定鍵の生成に用いる鍵について保持しておらず（ステップＳ１０２）、交換局ＭＭＥは、K_{ASME}を保持している（ステップＳ１０３）。

【００２９】

ステップＳ１０４において、移動局ＵＥは、無線基地局ｅＮＢに対して、「ＲＲＣ　Ｃ

onnection Request（RRC接続要求信号）」を送信し、ステップS105において、無線基地局eNBは、移動局UEに対して、「RRC Connection Setup（RRC接続設定信号）」を送信する。

【0030】

ステップS106において、移動局UEは、無線基地局eNBに対して、「RRC Connection Setup Complete（RRC接続設定完了信号）」と、「NAS SN（NASのシーケンス番号）」を含む「NAS Service Request（NASサービス要求信号）」とを送信する。

【0031】

ステップS107において、無線基地局eNBは、交換局MMEに対して、「S1 Initial UE Message」と、「NAS SN」を含む「NAS Service Request（NASサービス要求信号）」とを送信する。

【0032】

ステップS108において、交換局MMEは、下記の式によって、$K_{eNB[0]}$、$K_{eNB[1]}$を算出する。

【0033】

$K_{eNB[0]}=KDF_0(K_{ASME}, NAS\ SN)$

$K_{eNB[1]}=KDF_1(K_{ASME}, K_{eNB[0]})$

【0034】

ステップS109において、交換局MMEは、無線基地局eNBに対して、$K_{eNB[0]}$、$K_{eNB[1]}$、「NAS SN」を含む「S1 Initial UE Context Setup（初期UEコンテキスト設定信号）」を送信する。また、このメッセージに、「KI（＝0）」が含まれてもよいが、これは、必須ではない。

【0035】

ステップS110において、無線基地局eNBは、移動局UEに対して、「NAS SN」を含む「RRC Security Mode Command（RRCセキュリティモード指示信号）」を送信する。

【0036】

ステップS111において、移動局UEは、下記の式によって、$K_{eNB[0]}$を算出する。

【0037】

$K_{eNB[0]}=KDF_0(K_{ASME}, NAS\ SN)$

【0038】

また、移動局UEは、$K_{eNB[0]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のAS通信に適用する。

【0039】

この段階では、移動局UEは、$K_{eNB[0]}$、「KI（＝0）」を保持しており（ステップS114）、無線基地局eNBは、$K_{eNB[0]}$、$K_{eNB[1]}$、「KI（＝0）」を保持しており（ステップS113）、交換局MMEは、K_{ASME}、$K_{eNB[1]}$、「KI（＝0）」を保持している（ステップS112）。

【0040】

ステップS109の「S1 Initial UE Context Setup（初期UEコンテキスト設定信号）」に、「KI（＝0）」が含まれない場合は、無線基地局eNBは、かかるメッセージを受信したことで、自動的に「KI（＝0）」を初期化してもよい。

【0041】

また、無線基地局eNBは、$K_{eNB[0]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のAS通信に適用する。

【0042】

ステップS115において、無線基地局eNBは、移動局UEに対して、「RRC C

ｏｎｎｅｃｔｉｏｎ Ｒｅｃｏｎｆｉｇｕｒａｔｉｏｎ（ＲＲＣ接続再構成信号）」を送信する。

【００４３】

ステップＳ１１６及びＳ１１７において、移動局ＵＥは、無線基地局ｅＮＢに対して、「ＲＲＣ Ｓｅｃｕｒｉｔｙ Ｍｏｄｅ Ｃｏｍｍａｎｄ Ｃｏｍｐｌｅｔｅ（ＲＲＣセキュリティモード指示完了信号）」及び「ＲＲＣ Ｃｏｎｎｅｃｔｉｏｎ Ｒｅｃｏｎｆｉｇｕｒａｔｉｏｎ Ｃｏｍｐｌｅｔｅ（ＲＲＣ接続再構成完了信号）」を送信する。

【００４４】

ステップＳ１１８において、無線基地局ｅＮＢは、交換局ＭＭＥに対して、「Ｓ１ Ｉｎｉｔｉａｌ ＵＥ Ｃｏｎｔｅｘｔ Ｓｅｔｕｐ Ｃｏｍｐｌｅｔｅ（初期ＵＥコンテキスト設定完了信号）」を送信する。

【００４５】

以上の手順により、移動局ＵＥ、無線基地局ｅＮＢ、交換局ＭＭＥにおいて、ＡＳにおける通信の保護（Ｉｎｔｅｇｒｉｔｙ Ｐｒｏｔｅｃｔｉｏｎ及びＣｉｐｈｅｒｉｎｇ）に必要な全ての鍵が揃う。

【００４６】

第２に、図４を参照して、本実施形態に係る移動通信システムにおけるＸ２ハンドオーバ手順（異無線基地局間ハンドオーバ手順）について説明する。

【００４７】

図４に示すように、Ｘ２ハンドオーバ手順の開始前の段階では、移動局ＵＥは、$K_{eNB[n]}$、「ＫＩ（＝ｎ）」を保持しており（ステップＳ１００１）、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ ｅＮＢ）は、$K_{eNB[n]}$、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持しており（ステップＳ１００２）、交換局ＭＭＥは、K_{ASME}、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持している（ステップＳ１００３）。

【００４８】

ステップＳ１００４において、移動局ＵＥは、所定条件が満たされた場合に、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ ｅＮＢ）に対して、「ＲＲＣ Ｍｅａｓｕｒｅｍｅｎｔ Ｒｅｐｏｒｔ（測定報告信号）」を送信する。

【００４９】

ステップＳ１００５において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ ｅＮＢ）は、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ ｅＮＢ）に対して、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を含む「Ｘ２ ＨＯ Ｐｒｅｐａｒａｔｉｏｎ（ハンドオーバ準備信号）」を送信する。

【００５０】

ハンドオーバ先無線基地局（Ｔａｒｇｅｔ ｅＮＢ）は、ステップＳ１００６において、受信した$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を記憶し、ステップＳ１００７において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ ｅＮＢ）に対して、「Ｘ２ ＨＯ Ｐｒｅｐａｒａｔｉｏｎ Ａｃｋ（ハンドオーバ準備応答信号）」を送信する。

【００５１】

また、無線基地局ｅＮＢは、$K_{eNB[n+1]}$ に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。

【００５２】

ステップＳ１００８において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ ｅＮＢ）は、移動局ＵＥに対して、「ＲＲＣ ＨＯ Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」を送信する。

【００５３】

移動局ＵＥは、ステップＳ１００９において、下記の式によって、$K_{eNB[n+1]}$を算出し、ステップＳ１０１０において、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を記憶する。

【００５４】

$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$

【００５５】

また、移動局Ｕｅは、$K_{eNB[n+1]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。

【００５６】

ステップＳ１０１１において、移動局ＵＥは、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）に対して、「ＲＲＣ　ＨＯ　Ｃｏｍｐｌｅｔｅ（ハンドオーバ完了信号）」を送信する。

【００５７】

ステップＳ１０１２において、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、交換局ＭＭＥに対して、「ＫＩ（＝ｎ＋１）」を含む「Ｓ１　Ｐａｔｈ　Ｓｗｉｔｃｈ（パススイッチ信号）」を送信する。

【００５８】

交換局ＭＭＥは、ステップＳ１０１３において、下記の式によって、$K_{eNB[n+2]}$を算出し、ステップＳ１０１４において、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を記憶する。

【００５９】

$K_{eNB[n+2]}=KDF_1(K_{ASME}, K_{eNB[n+1]})$

【００６０】

ステップＳ１０１５において、交換局ＭＭＥは、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）に対して、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を含む「Ｓ１　Ｐａｔｈ　Ｓｗｉｔｃｈ　Ａｃｋ（パススイッチ応答信号）」を送信する。

【００６１】

ステップＳ１０１６において、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、$K_{eNB[n+1]}$、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を記憶する。

【００６２】

以上の手順により、Ｘ２ハンドオーバ時に、K_{eNB}及び所定鍵が更新される。

【００６３】

第３に、図５を参照して、本実施形態に係る移動通信システムにおけるＳ１ハンドオーバ手順（異交換局間ハンドオーバ手順）について説明する。

【００６４】

図５に示すように、Ｓ１ハンドオーバ手順の開始前の段階では、移動局ＵＥは、$K_{eNB[n]}$、「ＫＩ（＝ｎ）」を保持しており（ステップＳ２００１）、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、$K_{eNB[n]}$、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持しており（ステップＳ２００２）、交換局ＭＭＥは、K_{ASME}、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持している（ステップＳ２００３）。

【００６５】

ステップＳ２００４において、移動局ＵＥは、所定条件が満たされた場合に、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「ＲＲＣ　Ｍｅａｓｕｒｅｍｅｎｔ　Ｒｅｐｏｒｔ（測定報告信号）」を送信する。

【００６６】

ステップＳ２００５において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、ハンドオーバ元交換局（Ｓｏｕｒｃｅ　ＭＭＥ）に対して、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を含む「Ｓ１　ＨＯ　Ｒｅｑｕｉｒｅｄ（ハンドオーバ要求受信信号）」を送信する。

【００６７】

ステップＳ２００６において、ハンドオーバ元交換局（Ｓｏｕｒｃｅ　ＭＭＥ）は、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）に対して、K_{ASME}、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を含む「Ｒｅｌｏｃａｔｉｏｎ　Ｒｅｑｕｅｓｔ（割り当て要求信号）」を送信する。

【００６８】
ステップＳ２００７において、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）は、下記の式によって、$K_{eNB[n+2]}$を算出し、ステップＳ２００８において、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を記憶する。
【００６９】
$K_{eNB[n+2]}=KDF_1(K_{ASME}, K_{eNB[n+1]})$
ステップＳ２００９において、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）は、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）に対して、$K_{eNB[n+1]}$、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を含む「Ｓ１　ＨＯ　Ｒｅｑｕｅｓｔ（ハンドオーバ要求信号）」を送信する。
【００７０】
ステップＳ２０１０において、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）に対して、「Ｓ１　ＨＯ　Ｒｅｑｕｅｓｔ　Ａｃｋ（ハンドオーバ要求応答信号）」を送信する。
【００７１】
ステップＳ２０１１において、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）は、ハンドオーバ元交換局（Ｓｏｕｒｃｅ　ＭＭＥ）に対して、「ＫＩ（＝ｎ＋１）」を含む「Ｒｅｌｏｃａｔｉｏｎ　Ｒｅｑｕｅｓｔ　Ａｃｋ（割り当て要求応答信号）」を送信する。
【００７２】
ステップＳ２０１２において、ハンドオーバ元交換局（Ｓｏｕｒｃｅ　ＭＭＥ）は、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「ＫＩ（＝ｎ＋１）」を含む「Ｓ１　ＨＯ　Ｒｅｑｕｉｒｅｄ　Ａｃｋ（ハンドオーバ要求受信応答信号）」を送信する。
【００７３】
ステップＳ２０１３において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、移動局ＵＥに対して、「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」を送信する。
【００７４】
移動局ＵＥは、ステップＳ２０１４において、下記の式によって、$K_{eNB[n+1]}$を算出し、ステップＳ２０１５において、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を記憶する。
【００７５】
$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$
【００７６】
また、移動局ＵＥは、$K_{eNB[n+1]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。
【００７７】
この段階で、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、$K_{eNB[n+1]}$、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を保持している（ステップＳ２０１６）。無線基地局ｅＮＢは、$K_{eNB[n+1]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。
【００７８】
ステップＳ２０１７において、移動局ＵＥは、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）に対して、「ＲＲＣ　ＨＯ　Ｃｏｍｐｌｅｔｅ（ハンドオーバ完了信号）」を送信する。
【００７９】
ステップＳ２０１８において、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）に対して、「Ｓ１　ＨＯ　Ｃｏｍｐｌｅｔｅ（ハンドオーバ完了信号）」を送信する。

【００８０】
ステップＳ２０１９において、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）は、ハンドオーバ元交換局（Ｓｏｕｒｃｅ　ＭＭＥ）に対して、「Ｒｅｌｏｃａｔｉｏｎ　Ｃｏｍｐｌｅｔｅ（割り当て完了信号）」を送信し、ステップＳ２０２０において、ハンドオーバ元交換局（Ｓｏｕｒｃｅ　ＭＭＥ）は、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）に対して、「Ｒｅｌｏｃａｔｉｏｎ　Ｃｏｍｐｌｅｔｅ　Ａｃｋ（割り当て完了応答信号）」を送信する。
【００８１】
以上の手順により、Ｓ１ハンドオーバ時に、K_{eNB}及び所定鍵が更新される。
【００８２】
また、かかるＳ１ハンドオーバ手順において、移動局ＵＥが行う操作は、図２で示したＸ２ハンドオーバ手順における操作と同一である。移動局ＵＥは、同一処理に基づき、Ｘ２ハンドオーバ手順、Ｓ１ハンドオーバ手順の両方を行うことができる。すなわち、移動局ＵＥは、ハンドオーバ種別が「Ｘ２ハンドオーバ」であるか「Ｓ１ハンドオーバ」であるかについて意識する必要なく、ハンドオーバを実施することが可能である。
【００８３】
第４に、図６を参照して、本実施形態に係る移動通信システムにおけるＩｎｔｒａ-ｅＮＢハンドオーバ手順（無線基地局内ハンドオーバ手順）について説明する。
【００８４】
図６に示すように、Ｉｎｔｒａ-ｅＮＢハンドオーバ手順の開始前の段階では、移動局ＵＥは、$K_{eNB[n]}$、「ＫＩ（＝ｎ）」を保持しており（ステップＳ４００１）、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、$K_{eNB[n]}$、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持しており（ステップＳ４００２）、交換局ＭＭＥは、K_{ASME}、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持している（ステップＳ４００３）。
【００８５】
ステップＳ４００４において、移動局ＵＥは、所定条件が満たされた場合に、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「ＲＲＣ　Ｍｅａｓｕｒｅｍｅｎｔ　Ｒｅｐｏｒｔ（測定報告信号）」を送信する。
【００８６】
ステップＳ４００５において、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、移動局ＵＥに対して、「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」を送信する。
【００８７】
移動局ＵＥは、ステップＳ４００６において、下記の式によって、$K_{eNB[n+1]}$を算出し、ステップＳ４００７において、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を記憶する。
【００８８】
$$K_{eNB[n+1]} = KDF_1(K_{ASME}, K_{eNB[n]})$$
【００８９】
また、移動局ＵＥは、$K_{eNB[n+1]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。
【００９０】
この段階で、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を保持している（ステップＳ４００８）。無線基地局ｅＮＢは、$K_{eNB[n+1]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。
【００９１】
ステップＳ４００９において、移動局ＵＥは、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「ＲＲＣ　ＨＯ　Ｃｏｍｐｌｅｔｅ（ハンドオーバ完了信号）」を送信する。
【００９２】
ステップＳ４０１０において、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、交換局ＭＭＥ

に対して、「ＫＩ（＝ｎ＋１）」を含む「Ｓ１　Ｐａｔｈ　Ｓｗｉｔｃｈ（パススイッチ信号）」を送信する。

【００９３】

交換局ＭＭＥは、ステップＳ４０１１において、下記の式によって、$K_{eNB[n+2]}$を算出し、ステップＳ４０１２において、K_{ASME}、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を記憶する。

【００９４】

$K_{eNB[n+2]}=KDF_1(K_{ASME}, K_{eNB[n+1]})$

【００９５】

ステップＳ４０１３において、交換局ＭＭＥは、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を含む「Ｓ１　Ｐａｔｈ　Ｓｗｉｔｃｈ　Ａｃｋ（パススイッチ応答信号）」を送信する。

【００９６】

ステップＳ４０１４において、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、$K_{eNB[n+1]}$、$K_{eNB[n+2]}$、「ＫＩ（＝ｎ＋１）」を記憶する。この段階で、移動局ＵＥは、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を保持している（ステップＳ４０１５）。

【００９７】

以上の手順により、Ｉｎｔｒａ-ｅＮＢハンドオーバ時に、K_{eNB}及び所定鍵が更新される。

【００９８】

また、かかるＩｎｔｒａ-ｅＮＢハンドオーバ手順において、移動局ＵＥが行う操作は、図２で示したＸ２ハンドオーバ手順における操作並びに図３で示したＳ１ハンドオーバ手順における操作と同一である。移動局ＵＥは、同一処理に基づき、Ｘ２ハンドオーバ手順、Ｓ１ハンドオーバ手順、Ｉｎｔｒａ-ｅＮＢハンドオーバ手順の全てを行うことができる。すなわち、移動局ＵＥは、ハンドオーバ種別が「Ｘ２ハンドオーバ」、「Ｓ１ハンドオーバ」、「Ｉｎｔｒａ-ｅＮＢハンドオーバ」のいずれであるかを意識する必要なく、ハンドオーバを実施することが可能である。

【００９９】

（本発明の第１の実施形態に係る移動通信システムの作用・効果）

本発明の第１の実施形態に係る移動通信システムによれば、簡素化された手順で、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）で用いられる$K_{eNB[n+1]}$等を生成することができる。

【０１００】

また、本発明の第１の実施形態に係る移動通信システムによれば、ハンドオーバの種類（Ｘ２ハンドオーバ、Ｓ１ハンドオーバ、Ｉｎｔｒａ-ｅＮＢハンドオーバ）によらず、ハンドオーバ手順時の移動局ＵＥの動作を変更する必要がない。

【０１０１】

（本発明の第２の実施形態に係る移動通信システム）

図７を参照して、本発明の第２の実施形態に係る移動通信システムについて、上述の第１の実施形態に係る移動通信システムとの相違点に着目して説明する。

【０１０２】

具体的には、図７を参照して、本実施形態に係る移動通信システムにおけるＳ１ハンドオーバ手順（異交換局間ハンドオーバ手順）について説明する。

【０１０３】

図７に示すように、ステップＳ３００１乃至Ｓ３００６の動作は、図５に示すステップＳ２００１乃至Ｓ２００６の動作と同一である。

【０１０４】

ステップＳ３００７において、ハンドオーバ先交換局（Ｔａｒｇｅｔ　ＭＭＥ）は、下記の式によって、$K_{eNB[n+3]}$を算出し、ステップＳ３００８において、K_{eNB}

[n+3]、「KI（＝n＋2）」を記憶する。

【0105】

$K_{eNB[n+2]}=KDF_1(K_{ASME}, K_{eNB[n+1]})$

$K_{eNB[n+3]}=KDF_1(K_{ASME}, K_{eNB[n+2]})$

【0106】

ステップS3009において、ハンドオーバ先交換局（Target MME）は、ハンドオーバ先無線基地局（Target eNB）に対して、$K_{eNB[n+2]}$、$K_{eNB[n+3]}$、「KI（＝n＋2）」を含む「S1 HO Request（ハンドオーバ要求信号）」を送信する。

【0107】

ステップS3010において、ハンドオーバ先無線基地局（Target eNB）は、ハンドオーバ先交換局（Target MME）に対して、「S1 HO Request Ack（ハンドオーバ要求応答信号）」を送信する。

【0108】

ステップS3011において、ハンドオーバ先交換局（Target MME）は、ハンドオーバ元交換局（Source MME）に対して、「KI（＝n＋2）」を含む「Relocation Request Ack（割り当て要求応答信号）」を送信する。

【0109】

ステップS3012において、ハンドオーバ元交換局（Source MME）は、ハンドオーバ元無線基地局（Source eNB）に対して、「KI（＝n＋2）」を含む「S1 HO Required Ack（ハンドオーバ要求受信応答信号）」を送信する。

【0110】

ステップS3013において、ハンドオーバ元無線基地局（Source eNB）は、移動局UEに対して、「RRC HO Command（ハンドオーバ指示信号）」を送信する。本メッセージには、「KI（＝n＋2）」であることを示す情報が含まれてよい。

【0111】

移動局UEは、ステップS3014において、下記の式によって、$K_{eNB[n+2]}$を算出し、ステップS3015において、$K_{eNB[n+2]}$、「KI（＝n＋2）」を記憶する。

【0112】

$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$

$K_{eNB[n+2]}=KDF_1(K_{ASME}, K_{eNB[n+1]})$

【0113】

また、移動局UEは、$K_{eNB[n+2]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のAS通信に適用する。

【0114】

この段階で、ハンドオーバ先無線基地局（Target eNB）は、$K_{eNB[n+2]}$、$K_{eNB[n+3]}$、「KI（＝n＋2）」を保持している（ステップS3016）。無線基地局eNBは、$K_{eNB[n+2]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のAS通信に適用する。

【0115】

以下、ステップS3017乃至S3020の動作は、図5に示すステップS3017乃至S2020の動作と同一である。

【0116】

本手順により、ハンドオーバ先無線基地局（Target eNB）でAS通信に用いる所定鍵及びK_{eNB}を、ハンドオーバ元無線基地局（Source eNB）にて知りえなくなり、システムのセキュリティが向上する。

【０１１７】
（本発明の第３の実施形態に係る移動通信システム）
図８乃至図１１を参照して、本発明の第３の実施形態に係る移動通信システムについて、上述の第１の実施形態に係る移動通信システムとの相違点に着目して説明する。
【０１１８】
図８に、本実施形態に係る移動通信システムで用いられる鍵（すなわち、所定鍵の算出に用いられる鍵）の階層構造及び算出手順の一例について示す。
【０１１９】
図８に示すように、ＲＲＣプロトコルにおける「Ｉｎｔｅｇｒｉｔｙ　Ｐｒｏｔｅｃｔｉｏｎ」で用いられる鍵K_{RRC_IP}、ＲＲＣプロトコルにおける「Ｃｉｐｈｅｒｉｎｇ」で用いられる鍵K_{RRC_Ciph}及びＡＳのＵプレーンにおける「Ｃｉｐｈｅｒｉｎｇ」で用いられる鍵K_{UP_Ciph}は、$K_{eNB[n][m]}$を用いて生成される。
【０１２０】
また、$K_{eNB[n][m]}$は、$K_{eNB[n]}$を用いて、下記の式によって算出される。
【０１２１】
$K_{eNB[n][0]}=K_{eNB[n]}$
$K_{eNB[n][m+1]}=KDF_2(K_{eNB[n][m]})$，（$m \geqq 0$）
【０１２２】
さらに、$K_{eNB[n]}$は、K_{ASME}を用いて、下記の式によって算出される。
【０１２３】
$K_{eNB[0]}=KDF_0(K_{ASME}, NAS\ SN)$
$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$，（$n \geqq 0$）
【０１２４】
以下、図９乃至図１１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。
【０１２５】
第１に、図９を参照して、本実施形態に係る移動通信システムにおけるＸ２ハンドオーバ手順（異無線基地局間ハンドオーバ手順）について説明する。
【０１２６】
図９に示すように、Ｘ２ハンドオーバ手順の開始前の段階では、移動局ＵＥは、$K_{eNB[n]}$、$K_{eNB[n][m]}$、「ＫＩ（＝ｎ）」、「ＲＣ（＝ｍ）」を保持しており（ステップＳ６００１）、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、$K_{eNB[n]}$、$K_{eNB[n+1]}$、$K_{eNB[n][m]}$、「ＫＩ（＝ｎ）」、「ＲＣ（＝ｍ）」を保持しており（ステップＳ６００２）、交換局ＭＭＥは、K_{ASME}、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持している（ステップＳ６００３）。
【０１２７】
ステップＳ６００４において、移動局ＵＥは、所定条件が満たされた場合に、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「ＲＲＣ　Ｍｅａｓｕｒｅｍｅｎｔ　Ｒｅｐｏｒｔ（測定報告信号）」を送信する。
【０１２８】
ステップＳ６００５において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）に対して、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ＋１）」を含む「Ｘ２　ＨＯ　Ｐｒｅｐａｒａｔｉｏｎ（ハンドオーバ準備信号）」を送信する。
【０１２９】
ステップＳ６００６及びＳ６００７において、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、$K_{eNB[n+1]}$、$K_{eNB[n+1][0]}$、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝０）」を記憶する。ここで、$K_{eNB[n+1][0]}=K_{eNB[n+1]}$であるものとする。

【０１３０】
ステップＳ６００８において、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「Ｘ２　ＨＯ　Ｐｒｅｐａｒａｔｉｏｎ　Ａｃｋ（ハンドオーバ準備応答信号）」を送信する。
【０１３１】
ステップＳ６００９において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、移動局ＵＥに対して、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝０）」を含む「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」を送信する。
【０１３２】
移動局ＵＥは、ステップＳ６０１０において、下記の式によって、$K_{eNB[n+1]}$、$K_{eNB[n+1][0]}$を算出し、ステップＳ１０１０において、$K_{eNB[n+1]}$、$K_{eNB[n+1][0]}$、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝０）」を記憶する。
【０１３３】
$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$
$K_{eNB[n+1][0]}=K_{eNB[n+1]}$
【０１３４】
また、移動局ＵＥは、$K_{eNB[n+1][0]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。
【０１３５】
以下、ステップＳ６０１２乃至Ｓ６０１７の動作は、図４に示すステップＳＳ１０１１乃至Ｓ１０１６の動作と同一である。
【０１３６】
第２に、図１０を参照して、本実施形態に係る移動通信システムにおけるＳ１ハンドオーバ手順（異交換局間ハンドオーバ手順）について説明する。
【０１３７】
図１０に示すように、Ｓ１ハンドオーバ手順の開始前の段階では、移動局ＵＥは、$K_{eNB[n]}$、$K_{eNB[n][m]}$、「ＫＩ（＝ｎ）」、「ＲＣ（＝ｍ）」を保持しており（ステップＳ７００１）、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、$K_{eNB[n]}$、$K_{eNB[n+1]}$、$K_{eNB[n][m]}$、「ＫＩ（＝ｎ）」、「ＲＣ（＝ｍ）」を保持しており（ステップＳ７００２）、交換局ＭＭＥは、K_{ASME}、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持している（ステップＳ７００３）。
【０１３８】
以下、ステップＳ７００４乃至Ｓ７０１２の動作は、図５に示すステップＳ２００４乃至Ｓ２０１２の動作と同一である。
【０１３９】
ステップＳ７０１３において、ハンドオーバ元無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、移動局ＵＥに対して、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝０）」を含む「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」を送信する。
【０１４０】
ここで、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、ステップＳ７０１４において、下記の式によって、$K_{eNB[n+1][0]}$を算出して記憶する。
【０１４１】
$K_{eNB[n+1][0]}=K_{eNB[n+1]}$
【０１４２】
この段階で、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、$K_{eNB[n+1]}$、$K_{eNB[n+2]}$、$K_{eNB[n+1][0]}$、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝０）」を記憶しているものとする（ステップＳ７０１５）。無線基地局ｅＮＢは、$K_{eNB[n+1][0]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。
【０１４３】

移動局ＵＥは、ステップＳ７０１６において、下記の式によって、$K_{eNB[n+1]}$、$K_{eNB[n+1][0]}$を算出し、ステップＳ７０１７において、$K_{eNB[n+1]}$、$K_{eNB[n+1][0]}$、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝０）」を記憶する。

【０１４４】

$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$

$K_{eNB[n+1][0]}=K_{eNB[n+1]}$

【０１４５】

また、移動局ＵＥは、$K_{eNB[n+1][0]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。

【０１４６】

以下、ステップＳ７０１８乃至Ｓ７０２１の動作は、図５に示すステップＳ２０１７乃至Ｓ２０２０の動作と同一である。

【０１４７】

第３に、図１１を参照して、本実施形態に係る移動通信システムにおけるＩｎｔｒａ-ｅＮＢハンドオーバ手順（無線基地局内ハンドオーバ手順）について説明する。

【０１４８】

図１１に示すように、Ｉｎｔｒａ-ｅＮＢハンドオーバ手順の開始前の段階では、移動局ＵＥは、$K_{eNB[n]}$、$K_{eNB[n][m]}$、「ＫＩ（＝ｎ）」、「ＲＣ（＝ｍ）」を保持しており（ステップＳ５００１）、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、$K_{eNB[n]}$、$K_{eNB[n+1]}$、$K_{eNB[n][m]}$、「ＫＩ（＝ｎ）」、「ＲＣ（＝ｍ）」を保持しており（ステップＳ５００２）、交換局ＭＭＥは、K_{ASME}、$K_{eNB[n+1]}$、「ＫＩ（＝ｎ）」を保持している（ステップＳ５００３）。

【０１４９】

ステップＳ５００４において、移動局ＵＥは、所定条件が満たされた場合に、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「ＲＲＣ　Ｍｅａｓｕｒｅｍｅｎｔ　Ｒｅｐｏｒｔ（測定報告信号）」を送信する。

【０１５０】

ステップＳ５００５において、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、移動局ＵＥに対して、「ＫＩ（＝ｎ）」、「ＲＣ（＝ｍ＋１）」を含む「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」を送信する。

【０１５１】

無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）は、ステップＳ５００６において、下記の式によって、$K_{eNB[n][m+1]}$を算出し、ステップＳ５００７において、$K_{eNB[n]}$、$K_{eNB[n+1]}$、$K_{eNB[n][m+1]}$、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝ｍ＋１）」を記憶する。

【０１５２】

$K_{eNB[n][m+1]}=KDF_2(K_{eNB[n][m]})$

【０１５３】

また、無線基地局ｅＮＢは、$K_{eNB[n][m+1]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。

【０１５４】

同様に、移動局ＵＥは、ステップＳ５００８において、下記の式によって、$K_{eNB[n][m+1]}$を算出し、ステップＳ５００９において、$K_{eNB[n]}$、$K_{eNB[n][m+1]}$、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝ｍ＋１）」を記憶する。

【０１５５】

$K_{eNB[n][m+1]}=KDF_2(K_{eNB[n][m]})$

【０１５６】

また、移動局ＵＥは、$K_{eNB[n][m+1]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。

【０１５７】

ステップＳ５０１０において、移動局ＵＥは、無線基地局（Ｓｏｕｒｃｅ　ｅＮＢ）に対して、「ＲＲＣ　ＨＯ　Ｃｏｍｐｌｅｔｅ（ハンドオーバ完了信号）」を送信する。

【０１５８】

本実施例により、Ｉｎｔｒａ-ｅＮＢハンドオーバ手順における「Ｐａｔｈ　Ｓｗｉｔｃｈ」を省くことができる。

【０１５９】

以上、図９乃至図１１に示したように、パラメータ「ＲＣ」による無線基地局でのK_{eNB}の更新を導入することで、交換局ＭＭＥへの問い合わせを省きつつ、K_{eNB}を更新できる。

【０１６０】

なお、図９乃至図１１の手順において、「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」では、パラメータ「ＲＣ」を省いてもよい。

【０１６１】

パラメータ「ＲＣ」を「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」に含めずに省いた場合、パラメータ「ＫＩ」がインクリメントされたか否かに基づき、「ＲＣ」をインクリメントすべきか否かを判定することができる。

【０１６２】

「ＫＩ」がインクリメントされた場合は、「ＲＣ」を「０」にリセットし、「ＫＩ」がインクリメントされなかった場合には、「ＲＣ」をインクリメントすればよい。

【０１６３】

或いは、パラメータ「ＲＣ」を「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」に含めずに省いた場合、移動局ＵＥは、「ＲＣ」の値を現在値のまま維持した場合と、現在値からインクリメントした場合と、「０」にリセットした場合の各場合を試行し、受信したメッセージに対する「Ｉｎｔｅｇｒｉｔｙ」をチェックすることで、どの場合が正しかったかを自律的に判定してもよい。

【０１６４】

（変更例）

なお、上述の交換局ＭＭＥや無線基地局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。

【０１６５】

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。

【０１６６】

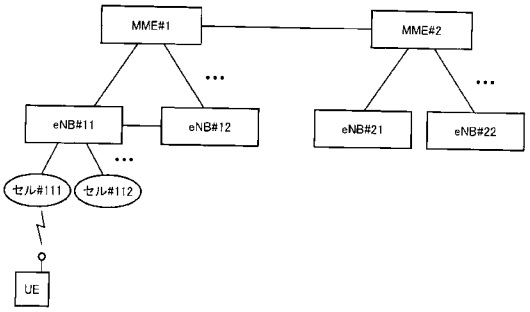
かかる記憶媒体は、プロセッサが当該記憶媒体に情報を読み書きできるように、当該プロセッサに接続されている。また、かかる記憶媒体は、プロセッサに集積されていてもよい。また、かかる記憶媒体及びプロセッサは、ＡＳＩＣ内に設けられていてもよい。かかるＡＳＩＣは、交換局ＭＭＥや無線基地局ｅＮＢや移動局ＵＥ内に設けられていてもよい。また、かかる記憶媒体及びプロセッサは、ディスクリートコンポーネントとして交換局ＭＭＥや無線基地局ｅＮＢや移動局ＵＥ内に設けられていてもよい。

【０１６７】

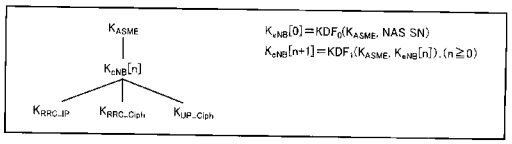
以上、上述の実施形態を用いて本発明について詳細に説明したが、当業者にとっては、本発明が本明細書中に説明した実施形態に限定されるものではないということは明らかである。本発明は、特許請求の範囲の記載により定まる本発明の趣旨及び範囲を逸脱することなく修正及び変更態様として実施することができる。従って、本明細書の記載は、例示説明を目的とするものであり、本発明に対して何ら制限的な意味を有するものではない。

【図面の簡単な説明】
【０１６８】
【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で用いられる鍵の階層構造及び算出手順の一例を示す図である。
【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ける初期設定手順を示すシーケンス図である。
【図４】本発明の第１の実施形態に係る移動通信システムにおけるＸ２ハンドオーバ手順を示すシーケンス図である。
【図５】本発明の第１の実施形態に係る移動通信システムにおけるＳ１ハンドオーバ手順を示すシーケンス図である。
【図６】本発明の第１の実施形態に係る移動通信システムにおけるＩｎｔｒａ-ｅＮＢハンドオーバ手順を示すシーケンス図である。
【図７】本発明の第２の実施形態に係る移動通信システムにおけるＳ１ハンドオーバ手順を示すシーケンス図である。
【図８】本発明の第３の実施形態に係る移動通信システムで用いられる鍵の階層構造及び算出手順の一例を示す図である。
【図９】本発明の第２の実施形態に係る移動通信システムにおけるＸ２ハンドオーバ手順を示すシーケンス図である。
【図１０】本発明の第３の実施形態に係る移動通信システムにおけるＳ１ハンドオーバ手順を示すシーケンス図である。
【図１１】本発明の第１の実施形態に係る移動通信システムにおけるＩｎｔｒａ-ｅＮＢハンドオーバ手順を示すシーケンス図である。
【図１２】従来技術に係る移動通信システムで用いられる鍵の算出手順の一例を示す図である。
【符号の説明】
【０１６９】
ＭＭＥ…交換局
ｅＮＢ…無線基地局
ＵＥ…移動局

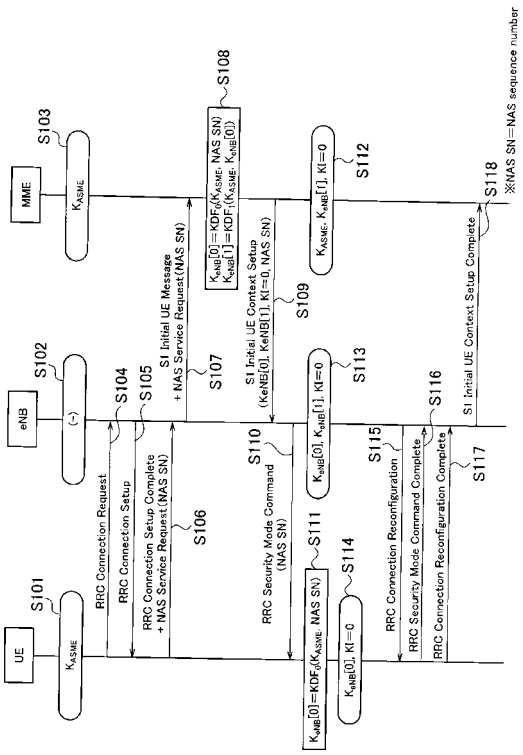
【図１】


MME#1
MME#2
eNB#11
eNB#12
eNB#21
eNB#22
セル#111
セル#112
UE

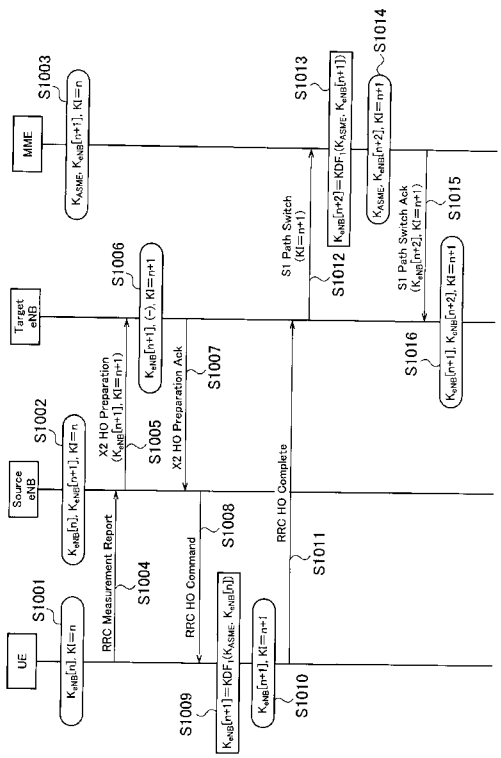
【図２】


K_ASME
K_eNB[n]
K_RRC_IP
K_RRC_Ciph
K_UP_Ciph
K_eNB[0]=KDF_0(K_ASME, NAS SN)
K_eNB[n+1]=KDF_1(K_ASME, K_eNB[n]), (n≧0)

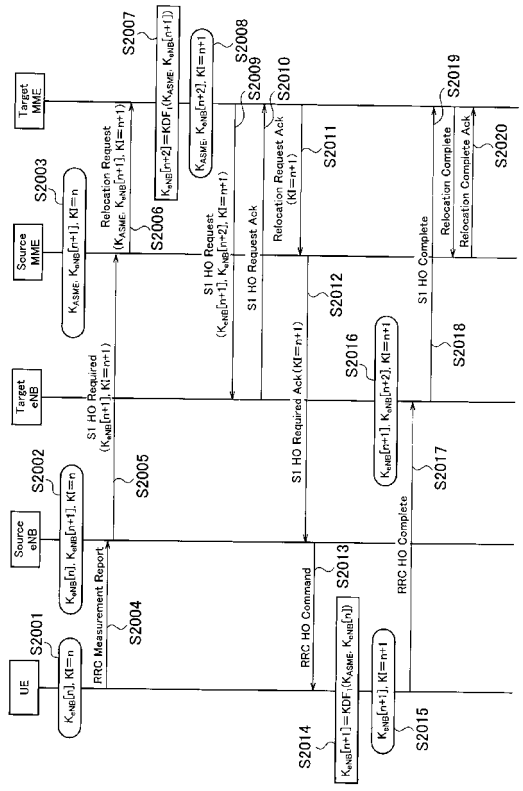
【図３】


UE
eNB
MME
S101
S102
S103
S104
S105
S106
S107
S108
S109
S110
S111
S112
S113
S114
S115
S116
S117
S118
※NAS SN=NAS sequence number
RRC Connection Request
RRC Connection Setup
RRC Connection Setup Complete + NAS Service Request(NAS SN)
S1 Initial UE Message + NAS Service Request(NAS SN)
S1 Initial UE Context Setup (KeNB[0], KeNB[1], KI=0, NAS SN)
RRC Security Mode Command (NAS SN)
RRC Connection Reconfiguration
RRC Security Mode Command Complete
RRC Connection Reconfiguration Complete
S1 Initial UE Context Setup Complete

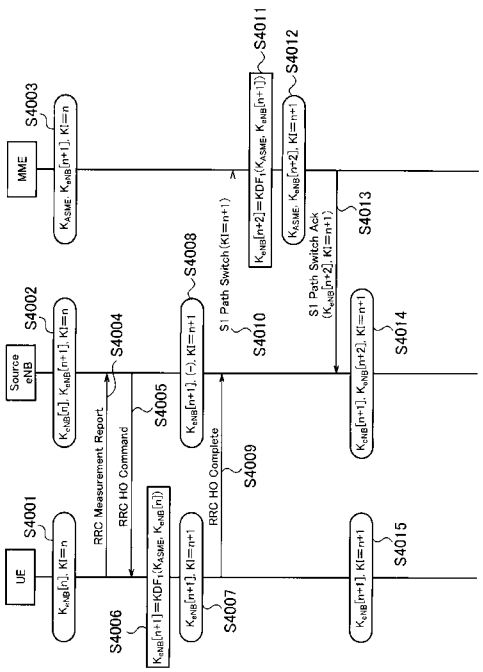
【図４】


UE
Source eNB
Target eNB
MME
S1001
S1002
S1003
S1004
S1005
S1006
S1007
S1008
S1009
S1010
S1011
S1012
S1013
S1014
S1015
S1016
RRC Measurement Report
X2 HO Preparation
X2 HO Preparation Ack
RRC HO Command
RRC HO Complete
S1 Path Switch (KI=n+1)
S1 Path Switch Ack (KI=n+1)

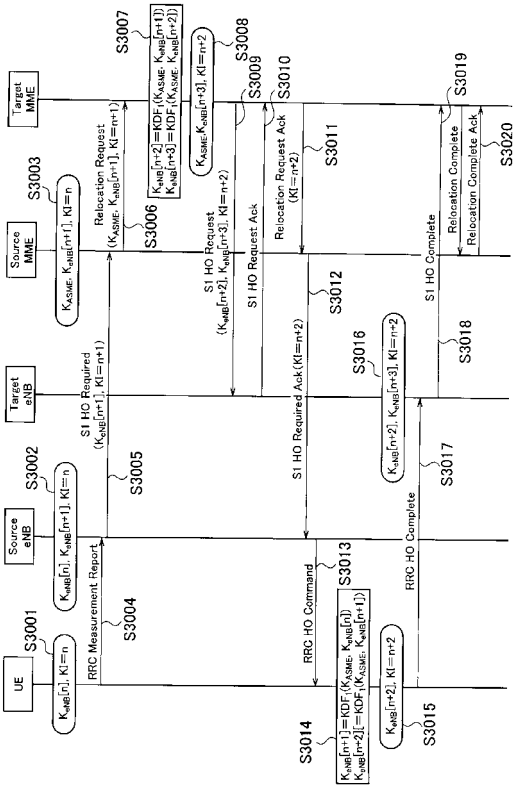
【図５】


UE
Source eNB
Source MME
Target eNB
Target MME
S2001
S2002
S2003
S2004
S2005
S2006
S2007
S2008
S2009
S2010
S2011
S2012
S2013
S2014
S2015
S2016
S2017
S2018
S2019
S2020
RRC Measurement Report
RRC HO Command
RRC HO Complete
S1 HO Required
S1 HO Request
S1 HO Request Ack
S1 HO Required Ack (KI=n+1)
S1 HO Complete
Relocation Request
Relocation Request Ack (KI=n+1)
Relocation Complete
Relocation Complete Ack

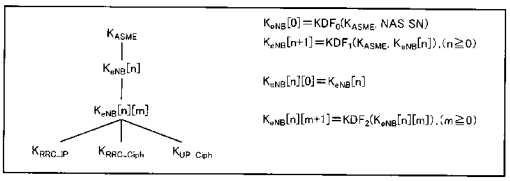
【図６】


UE
Source eNB
MME
S4001
S4002
S4003
S4004
S4005
S4006
S4007
S4008
S4009
S4010
S4011
S4012
S4013
S4014
S4015
RRC Measurement Report
RRC HO Command
RRC HO Complete
S1 Path Switch (KI=n+1)
S1 Path Switch Ack (KI=n+1)

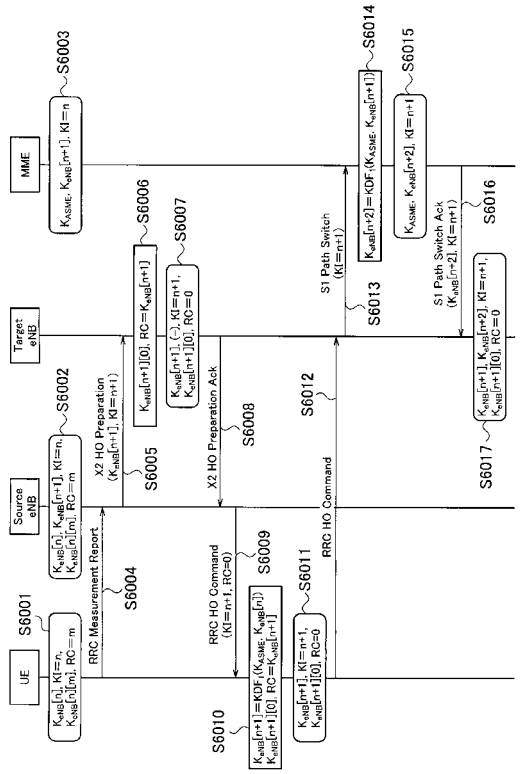
【図７】


UE
Source eNB
Target eNB
Source MME
Target MME
S3001
S3002
S3003
S3004
S3005
S3006
S3007
S3008
S3009
S3010
S3011
S3012
S3013
S3014
S3015
S3016
S3017
S3018
S3019
S3020
RRC Measurement Report
RRC HO Command
RRC HO Complete
S1 HO Required
S1 HO Required Ack
S1 HO Request
S1 HO Request Ack
Relocation Request
Relocation Request Ack
S1 HO Complete
Relocation Complete
Relocation Complete Ack

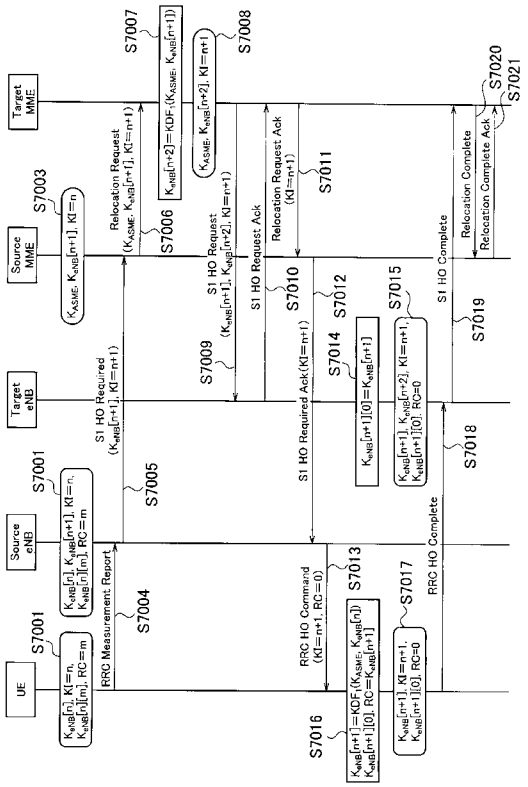
【図８】


K_ASME
K_eNB[n]
K_eNB[n][m]
K_RRC_UP
K_RRC_Ciph
K_UP Ciph
K_eNB[0]=KDF0(K_ASME, NAS SN)
K_eNB[n+1]=KDF1(K_ASME, K_eNB[n]),(n≧0)
K_eNB[n][0]=K_eNB[n]
K_eNB[n][m+1]=KDF2(K_eNB[n][m]),(m≧0)

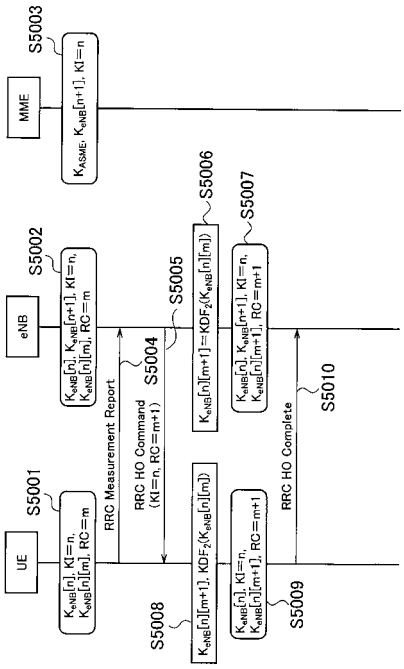
【図９】


UE
Source eNB
Target eNB
MME
S6001
S6002
S6003
S6004
S6005
S6006
S6007
S6008
S6009
S6010
S6011
S6012
S6013
S6014
S6015
S6016
S6017
RRC Measurement Report
X2 HO Preparation
X2 HO Preparation Ack
RRC HO Command
S1 Path Switch (KI=n+1)
S1 Path Switch Ack (KI=n+1)

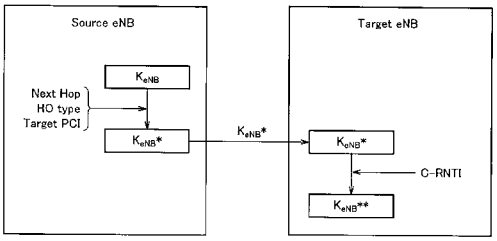
【図１０】


UE
Source eNB
Source MME
Target eNB
Target MME
S7001
S7003
S7004
S7005
S7006
S7007
S7008
S7009
S7010
S7011
S7012
S7013
S7014
S7015
S7016
S7017
S7018
S7019
S7020
S7021
RRC Measurement Report
S1 HO Required
Relocation Request
S1 HO Request
S1 HO Request Ack
Relocation Request Ack
S1 HO Required Ack(KI=n+1)
RRC HO Command
(KI=n+1, RC=0)
RRC HO Complete
S1 HO Complete
Relocation Complete
Relocation Complete Ack

【図１１】


UE
eNB
MME
S5001
S5002
S5003
S5004
S5005
S5006
S5007
S5008
S5009
S5010
RRC Measurement Report
RRC HO Command
(KI=n, RC=m+1)
RRC HO Complete

【図１２】


Source eNB
Target eNB
Next Hop
HO type
Target PCI
C-RNTI

フロントページの続き

(72)発明者　ウリ　Ａ．ハプサリ
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　岩村　幹生
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　アルフ　ツーゲンマイヤー
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

審査官　丹治　彰

(56)参考文献　特開２００８－０７２６９４（ＪＰ，Ａ）
特開２００７－１９４８４８（ＪＰ，Ａ）
特開２００７－２６７１２０（ＪＰ，Ａ）
Security architecture, 3GPP TS33.401 V8.0.0, ２００８年　6月, P. 26-31

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｑ７／００－７／３８
Ｈ０４Ｂ７／２４－７／２６