(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-136439
(P2010-136439A)
(43)公開日　平成22年6月17日(2010.6.17)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 12/08	(2009.01)	H04Q	7/00	184	5J104
H04W 36/08	(2009.01)	H04Q	7/00	306	5K067
H04L 9/14	(2006.01)	H04L	9/00	641	

審査請求 未請求　請求項の数 1　OL　（全 20 頁）

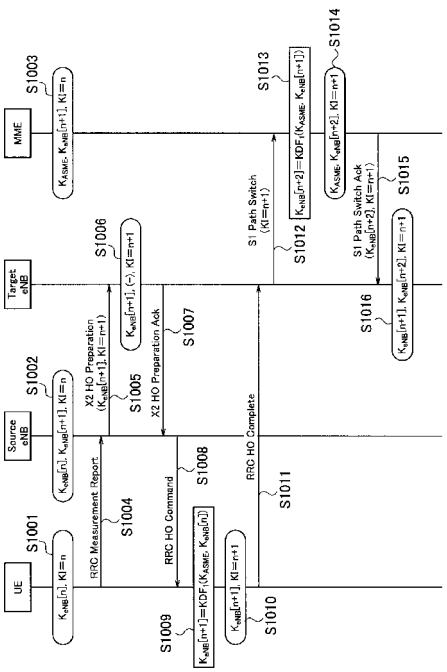
(21)出願番号　特願2010-32602(P2010-32602)
(22)出願日　平成22年2月17日(2010.2.17)
(62)分割の表示　特願2008-162617(P2008-162617)の分割
原出願日　平成20年6月20日(2008.6.20)

(71)出願人　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)【要約】
【課題】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。
【解決手段】本発明に係る移動通信方法は、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移動通信方法であって、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）は、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$K_{eNB【n+1】}$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$K_{eNB【n+2】}$の両方を取得する。
【選択図】図４



【特許請求の範囲】
【請求項１】
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特徴とする移動通信方法。
【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。
【先行技術文献】
【非特許文献】

【０００９】
【非特許文献１】３ＧＰＰ　ＴＳ３３．４０１　ｖ８．０．０
【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、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。
【００１１】
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。
【００１２】
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。
【００１３】
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。
【００１４】
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】
【００１５】
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】
【００１６】
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。
【図面の簡単な説明】
【００１７】
【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。
【発明を実施するための形態】
【００１８】
（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。
【００１９】
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。
【００２０】
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。
【００２１】
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。
【００２２】
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。
【００２３】
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。
【００２４】
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。
【００２５】
$K_{eNB[0]}=KDF_0(K_{ASME}, NAS\ SN)$
$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$，（$n \geqq 0$）
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。
【００２６】
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。

【００２７】
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。
【００２８】
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。
【００２９】
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）。
【００３０】
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　Ｃｏｎｎｅｃｔｉｏｎ　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。
【００３１】
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。
【００３２】
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。
【００３３】
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。
【００３４】
$K_{eNB[0]} = KDF_0(K_{ASME}, NAS\ SN)$
$K_{eNB[1]} = KDF_1(K_{ASME}, K_{eNB[0]})$
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】
$K_{eNB[0]} = KDF_0(K_{ASME}, NAS\ SN)$
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。
【００３８】
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）。

【００３９】

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。

【００４０】

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。

【００４１】

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

【００４２】

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。

【００４３】

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。

【００４４】

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。

【００４５】

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。

【００４６】

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）。

【００４７】

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。

【００４８】

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。

【００４９】

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。

【００５０】
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。
【００５１】
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。
【００５２】
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。
【００５３】
$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$
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。
【００５４】
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。
【００５５】
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。
【００５６】
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。
【００５７】
$K_{eNB[n+2]}=KDF_1(K_{ASME}, K_{eNB[n+1]})$
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。
【００５８】
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。
【００５９】
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。
【００６０】
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。
【００６１】
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）。
【００６２】
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。

【００６３】
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。
【００６４】
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。
【００６５】
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。
【００６６】
$K_{eNB[n+2]}=KDF_1(K_{ASME}, K_{eNB[n+1]})$
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。
【００６７】
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。
【００６８】
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。
【００６９】
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。
【００７０】
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。
【００７１】
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。
【００７２】
$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$
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。
【００７３】
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_Cip}

$_{h}$、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。

【００７４】

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。

【００７５】

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。

【００７６】

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。

【００７７】

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。

【００７８】

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。

【００７９】

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。

【００８０】

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）。

【００８１】

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。

【００８２】

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。

【００８３】

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。

【００８４】

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

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。

【００８５】

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。

【００８６】

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。

【００８７】

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。

【００８８】

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。

【００８９】

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

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。

【００９０】

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）。

【００９１】

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。

【００９２】

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。

【００９３】

（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。

【００９４】

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。

【００９５】

（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。

【００９６】

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。

【００９７】

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。

【００９８】

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。

【００９９】

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

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

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。

【０１００】

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。

【０１０１】

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。

【０１０２】

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。

【０１０３】

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。

【０１０４】

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。

【０１０５】

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

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

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。

【０１０６】

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。

【０１０７】

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。

【０１０８】

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。

【０１０９】

（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。

【０１１０】

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。

【０１１１】

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。

【０１１２】

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。

【０１１３】

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

$K_{eNB[n][m+1]}=KDF_2(K_{eNB[n][m]})$，（$m \geqq 0$）

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。

【０１１４】

$K_{eNB[0]}=KDF_0(K_{ASME}$，ＮＡＳ　ＳＮ）

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

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。

【０１１５】

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。

【０１１６】

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）。

【０１１７】

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。

【０１１８】

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。

【０１１９】

ステップＳ６００６及びＳ６００７において、ハンドオーバ先無線基地局（Ｔａｒｇｅ

ｔ　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。

【０１２０】

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。

【０１２１】

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。

【０１２２】

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。

【０１２３】

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

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

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。

【０１２４】

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。

【０１２５】

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。

【０１２６】

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）。

【０１２７】

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。

【０１２８】

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。

【０１２９】

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。

【０１３０】

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

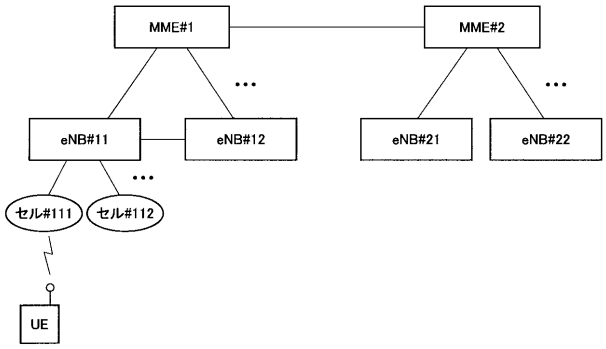
この段階で、ハンドオーバ先無線基地局（Ｔａｒｇｅｔ　ｅＮＢ）は、$K_{eNB[n+1]}$、$K_{eNB[n+2]}$、$K_{eNB[n+1][0]}$、「ＫＩ（＝ｎ＋１）」、「ＲＣ（＝０）」を記憶しているものとする（ステップＳ７０１５）。無線基地局ｅＮＢは、$K_{eNB[n+1][0]}$に基づき、K_{RRC_IP}、K_{RRC_Ciph}、K_{UP_Ciph}を算出し、その後のＡＳ通信に適用する。

【０１３１】
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。
【０１３２】
$K_{eNB[n+1]}=KDF_1(K_{ASME}, K_{eNB[n]})$
$K_{eNB[n+1][0]}=K_{eNB[n+1]}$
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。
【０１３３】
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。
【０１３４】
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。
【０１３５】
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）。
【０１３６】
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。
【０１３７】
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。
【０１３８】
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。
【０１３９】
$K_{eNB[n][m+1]}=KDF_2(K_{eNB[n][m]})$
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。
【０１４０】
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。
【０１４１】
$K_{eNB[n][m+1]}=KDF_2(K_{eNB[n][m]})$
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。
【０１４２】
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。

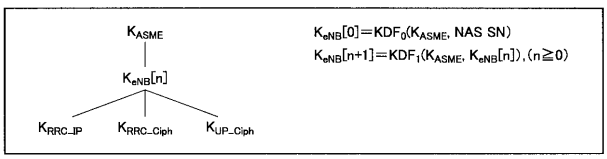
【０１４３】
本実施例により、Ｉｎｔｒａ-ｅＮＢハンドオーバ手順における「Ｐａｔｈ　Ｓｗｉｔｃｈ」を省くことができる。
【０１４４】
以上、図９乃至図１１に示したように、パラメータ「ＲＣ」による無線基地局でのK_{eNB}の更新を導入することで、交換局ＭＭＥへの問い合わせを省きつつ、K_{eNB}を更新できる。
【０１４５】
なお、図９乃至図１１の手順において、「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」では、パラメータ「ＲＣ」を省いてもよい。
【０１４６】
パラメータ「ＲＣ」を「ＲＲＣ　ＨＯ　Ｃｏｍｍａｎｄ（ハンドオーバ指示信号）」に含めずに省いた場合、パラメータ「ＫＩ」がインク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。
【０１４７】
「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。
【０１４８】
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。
【０１４９】
（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。
【０１５０】
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。
【０１５１】
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。
【０１５２】
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】
【０１５３】

ＭＭＥ…交換局
ｅＮＢ…無線基地局
ＵＥ…移動局

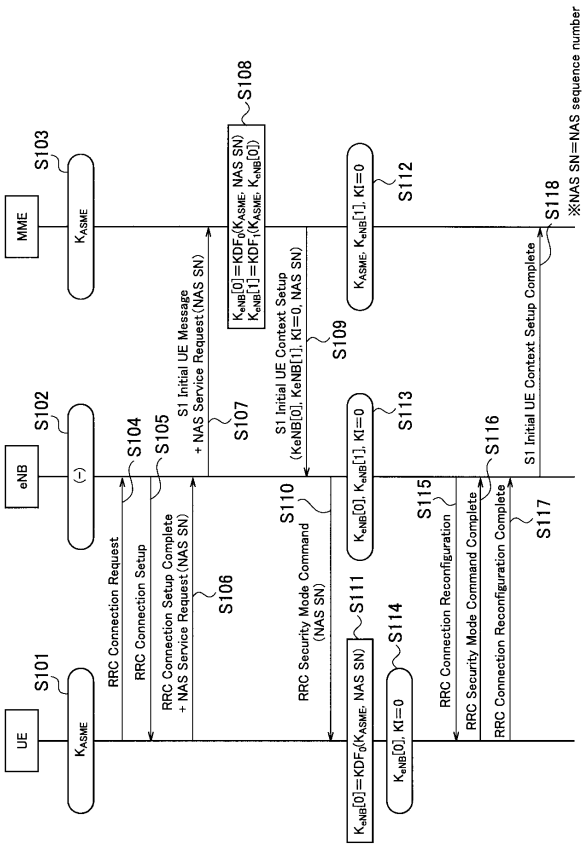
【図１】



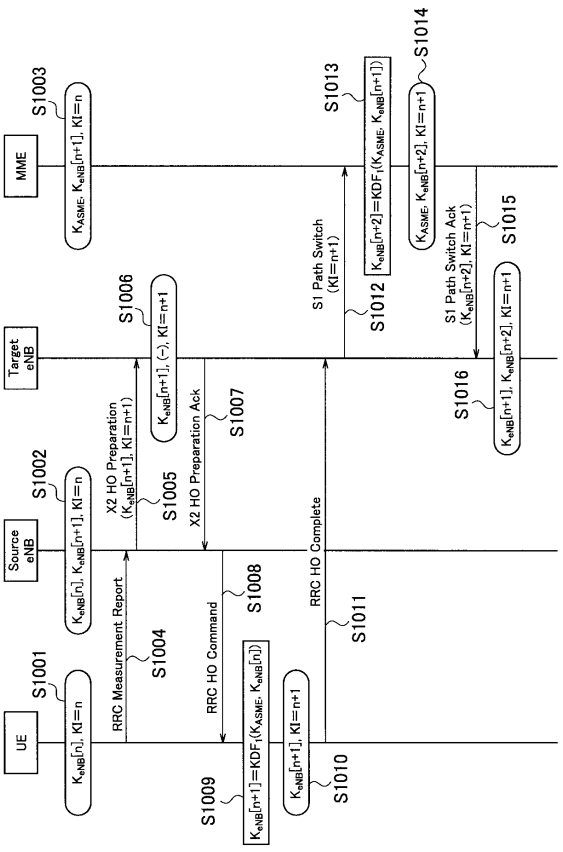
【図２】



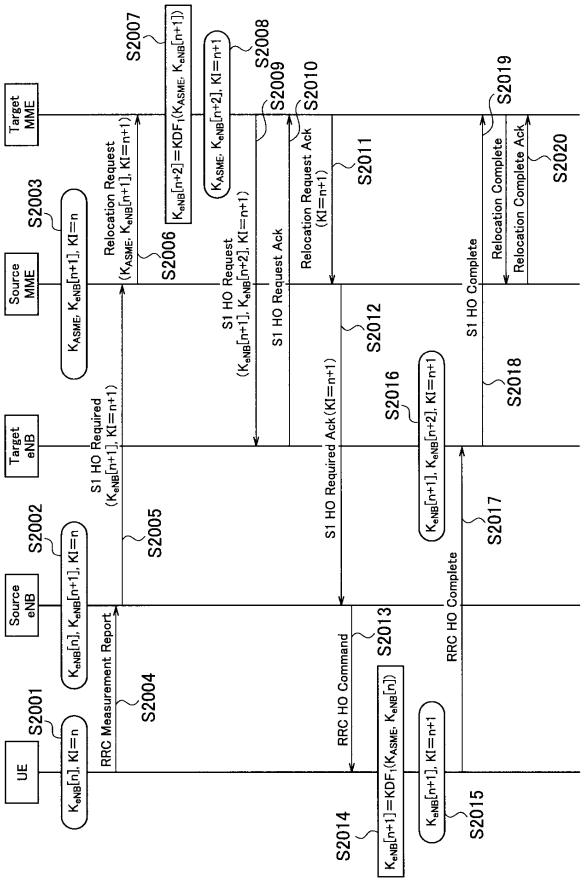
【図３】



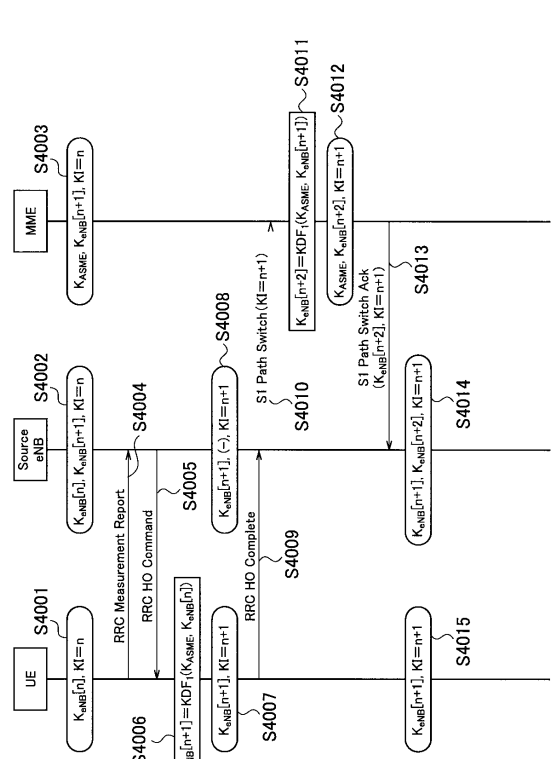
【図４】


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
S1 Path Switch Ack

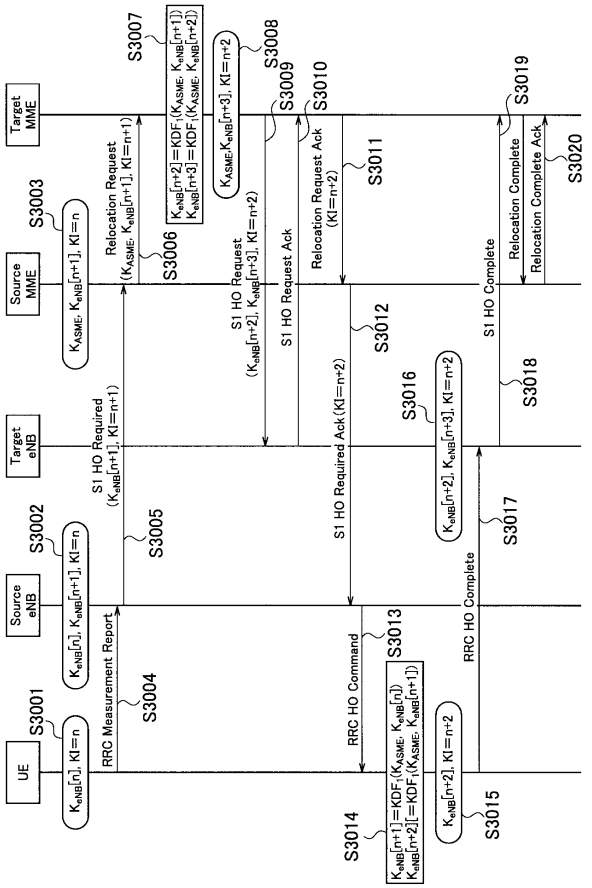
【図５】


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
S1 HO Required
Relocation Request
S1 HO Request
S1 HO Request Ack
Relocation Request Ack
S1 HO Required Ack
RRC HO Command
S1 HO Complete
Relocation Complete
Relocation Complete Ack

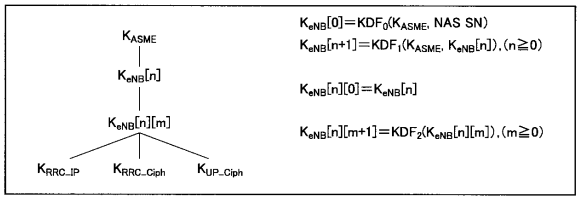
【図６】


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
S1 Path Switch Ack

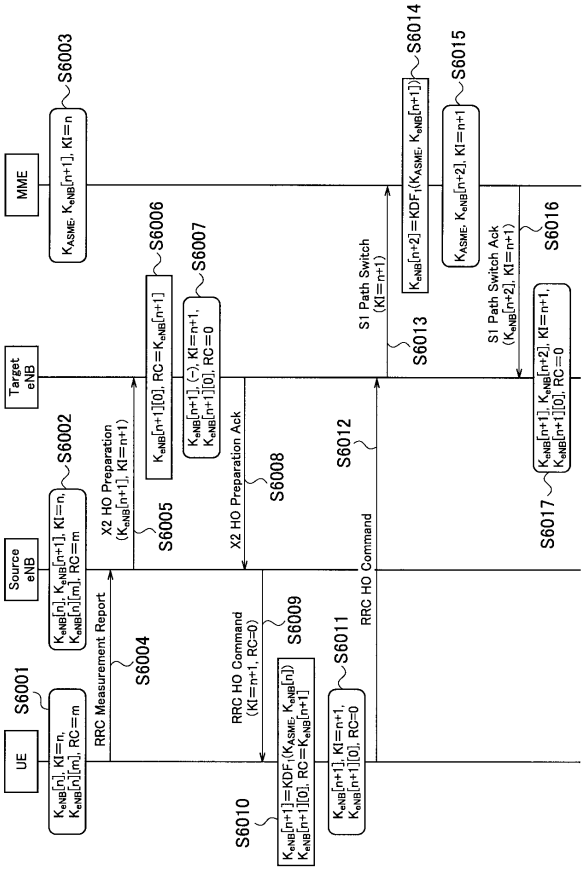
【図７】


UE
Source eNB
Source MME
Target eNB
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
S1 HO Required
Relocation Request
S1 HO Request
S1 HO Request Ack
Relocation Request Ack
S1 HO Required Ack
RRC HO Command
S1 HO Complete
Relocation Complete
Relocation Complete Ack

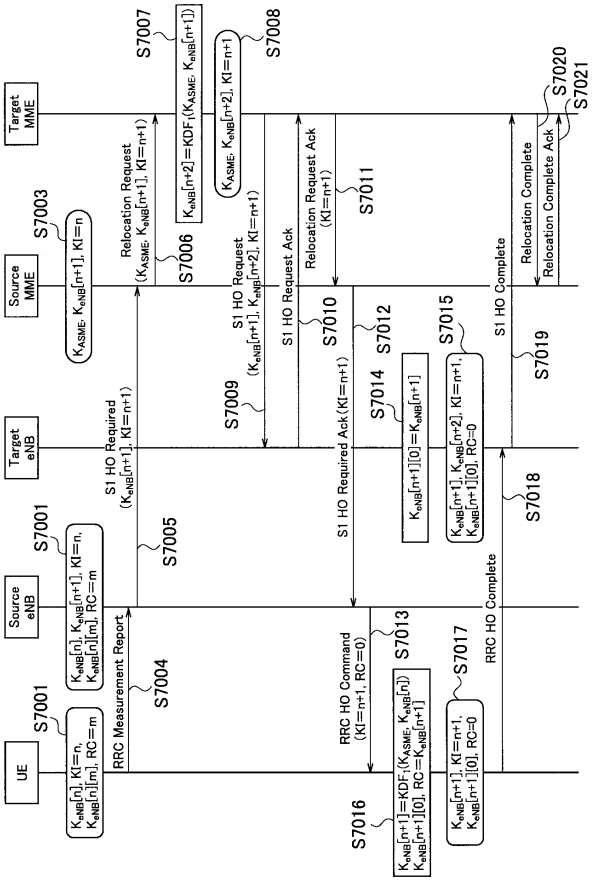
【図８】


K_ASME
K_eNB[n]
K_eNB[n][m]
K_RRC_IP
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)

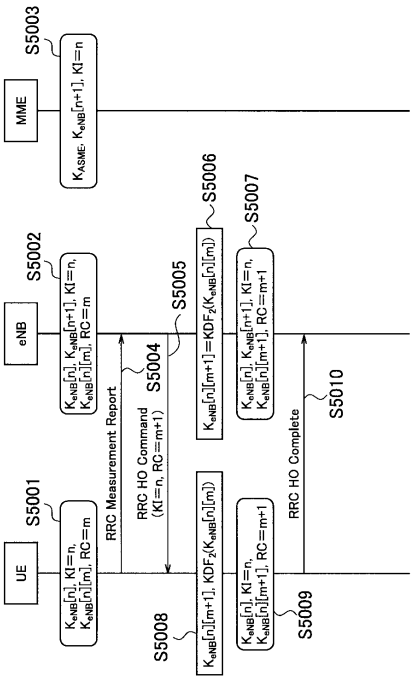
【図９】


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
S1 Path Switch Ack

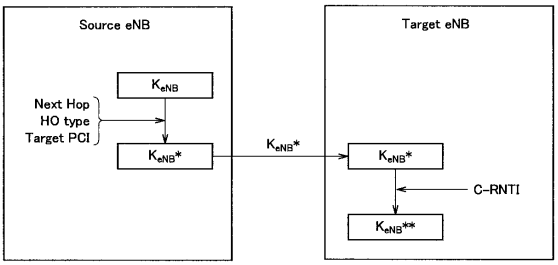
【図１０】


UE
Source eNB
Target eNB
Source MME
Target MME
S7001
S7002
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
RRC HO Command
S1 HO Required Ack
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
RRC HO Complete

【図１２】


Source eNB
Target eNB
K_{eNB}
Next Hop
HO type
Target PCI
K_{eNB}*
K_{eNB}*
K_{eNB}*
C-RNTI
K_{eNB}**

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

Ｆターム(参考) 5J104 AA16 AA34 EA04 EA15 JA03 NA02 NA37 PA01
5K067 AA35 BB02 EE02 EE10 HH36 JJ39