

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年7月2日(02.07.2020)



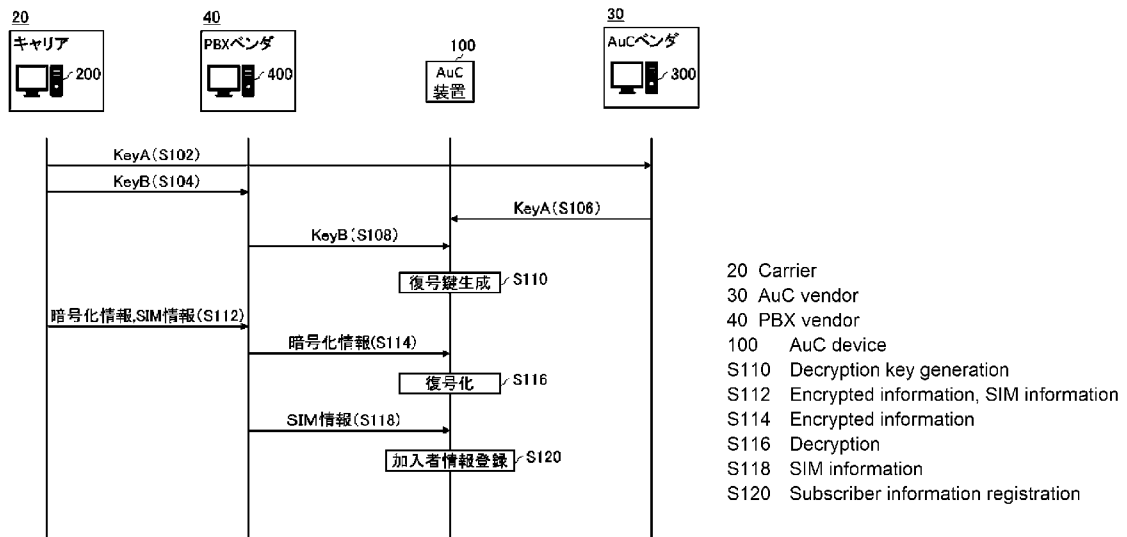
(10) 国際公開番号

WO 2020/136857 A1

- (51) 国際特許分類:
H04W 12/04 (2009.01) *H04L 9/32* (2006.01)
H04L 9/08 (2006.01) *H04W 12/06* (2009.01)
- (21) 国際出願番号: PCT/JP2018/048402
- (22) 国際出願日: 2018年12月28日(28.12.2018)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人: ビー・ビー・バックボーン株式会社(BB BACKBONE CORPORATION) [JP/JP]; 〒1057304 東京都港区東新橋1丁目9番1号 Tokyo (JP). ソフトバンク株式会社(SOFTBANK CORP.) [JP/JP]; 〒1057317 東京都港区東新橋一丁目9番1号 Tokyo (JP).
- (72) 発明者: 佐田 昌博(SADA Masahiro); 〒1057304 東京都港区東新橋一丁目9番1号 Tokyo (JP). 滝井 孝則(TAKII Takanori); 〒1057304 東京都港区東新橋一丁目9番1号 Tokyo (JP). 櫻井 忠良(SAKURAI Tadayoshi); 〒1057304 東京都港区東新橋一丁目9番1号 Tokyo (JP). 白川 洋平(SHIRAKAWA Yohei); 〒1057304 東京都港区東新橋一丁目9番1号 Tokyo (JP). 三平 大輔(MIHIRA Daisuke); 〒1057304 東京都港区東新橋一丁目9番1号 Tokyo (JP). 菅 司(KAN Tsukasa); 〒1057304 東京都港区東新橋一丁目9番1号 Tokyo (JP).
- (74) 代理人: 龍華国際特許業務法人(RYUKA IP LAW FIRM); 〒1631522 東京都新宿区西新宿1-6-1 新宿エルタワー22階 Tokyo (JP).

(54) Title: AUTHENTICATION DEVICE, SYSTEM, AUTHENTICATION METHOD, AND PROGRAM

(54) 発明の名称: 認証装置、システム、認証方法及びプログラム



(57) Abstract: Provided is an authentication device comprising: a key information storage unit including a first storage area in which first decryption key information is stored in such a format that the first decryption key information cannot be referred to externally; and a second storage area for storing second decryption key information that has been input externally; a decryption key generation unit for generating a decryption key on the basis of the first decryption key information stored in the first storage area, and the second decryption key information stored in the second storage area; a

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

decryption unit for decrypting encrypted information by using the decryption key; and an authentication unit for receiving an authentication request of a portable terminal, and authenticating a SIM on the basis of SIM information of the SIM of the portable terminal included in the authentication request, and the information decrypted by the decryption unit.

(57) 要約: 第1復号鍵情報を外部から参照不可能な形式で記憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する鍵情報記憶部と、第1記憶領域に記憶されている第1復号鍵情報と、第2記憶領域に記憶された第2復号鍵情報とに基づいて復号鍵を生成する復号鍵生成部と、復号鍵を用いて、暗号化された情報を復号化する復号部と、携帯端末の認証要求を受け付け、認証要求に含まれる携帯端末のSIMのSIM情報と、復号部によって復号化された情報とに基づいて、SIMの認証を行う認証部とを備える認証装置を提供する。

明 細 書

発明の名称： 認証装置、システム、認証方法及びプログラム

技術分野

[0001] 本発明は、認証装置、システム、認証方法及びプログラムに関する。

背景技術

[0002] SIM (Subscriber Identity Module) に記憶された鍵情報と、HSS (Home Subscriber Server) 上に保存された鍵情報とを用いてSIMの認証を行う仕組みが知られていた（例えば、特許文献1 参照）。

〔先行技術文献〕

〔特許文献〕

〔特許文献1〕 特開2013-168035号公報

解決しようとする課題

[0003] SIMの情報が漏えいする可能性を低減可能な技術を提供することが望ましい。

一般的開示

[0004] 本発明の第1の態様によれば、認証装置が提供される。認証装置は、第1復号鍵情報を外部から参照不可能な形式で記憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する鍵情報記憶部を備えてよい。認証装置は、第1記憶領域に記憶されている第1復号鍵情報と、第2記憶領域に記憶された第2復号鍵情報とに基づいて復号鍵を生成する復号鍵生成部を備えてよい。認証装置は、復号鍵を用いて、暗号化された情報を復号化する復号部を備えてよい。認証装置は、携帯端末の認証要求を受け付け、認証要求に含まれる携帯端末のSIMのSIM情報と、復号部によって復号化された情報とに基づいて、SIMの認証を行う認証部を備えてよい。

[0005] 上記認証装置は、上記第2復号鍵情報を外部から受信して上記第2記憶領

域に記憶する第2復号鍵情報受信部を備えてよい。上記第2復号鍵情報受信部は、インターネットを介して送信された上記第2復号鍵情報を受信してよい。上記第1復号鍵情報は、上記第2復号鍵情報よりもデータ量が多くてよい。上記第1復号鍵情報は、上記第2復号鍵情報よりもデータ量が少なくてもよい。

[0006] 上記認証装置は、複数の加入者情報を記憶する加入者情報記憶部であって、上記複数の加入者情報のそれぞれは、加入者識別番号と、SIM毎に固有の鍵情報とを含む加入者情報記憶部を備えてよく、上記SIM情報は上記加入者識別番号を含んでよく、上記認証部は、上記SIM情報に含まれる加入者識別番号と、上記加入者情報記憶部に当該加入者識別番号と対応付けて記憶されている鍵情報と、上記復号部によって復号化された情報とに基づいて、上記SIMの認証を行ってよい。上記加入者識別番号は、IMSI (International Mobile Subscriber Identity) であってよく、上記鍵情報は、K値であってよい。

[0007] 本発明の第2の態様によれば、上記認証装置と、上記認証装置を管理する管理装置とを備えるシステムが提供される。上記管理装置は、上記第1復号鍵情報を外部から受信する第1復号鍵情報受信部を備えてよく、上記記憶制御部は、上記第1復号鍵情報受信部が受信した上記第1復号鍵情報を上記第1記憶領域に記憶させてよい。

[0008] 本発明の第3の態様によれば、認証方法が提供される。認証方法は、第1復号鍵情報を外部から参照不可能な形式で記憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する鍵情報記憶部を有する認証装置により実行されてよい。認証方法は、第1記憶領域に記憶されている第1復号鍵情報と、第2記憶領域に記憶された第2復号鍵情報とに基づいて復号鍵を生成する復号鍵生成段階を備えてよい。認証方法は、復号鍵を用いて、暗号化された情報を復号化する復号段階を備えてよい。認証方法は、携帯端末の認証要求を受け付け、認証要求に含まれる携帯端末のSIMのSIM情報と、復号部によって復号化された情報とに基づ

づいて、S I Mの認証を行う認証段階を備えてよい。

[0009] 本発明の第4の態様によれば、プログラムが提供される。プログラムは、第1復号鍵情報を外部から参照不可能な形式で記憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する鍵情報記憶部を有するコンピュータに、第1記憶領域に記憶されている第1復号鍵情報と、第2記憶領域に記憶された第2復号鍵情報とに基づいて復号鍵を生成する復号鍵生成段階を実行させてよい。プログラムは、上記コンピュータに、復号鍵を用いて、暗号化された情報を復号化する復号段階を実行させてよい。プログラムは、上記コンピュータに、携帯端末の認証要求を受け付け、認証要求に含まれる携帯端末のS I MのS I M情報と、復号部によって復号化された情報とに基づいて、S I Mの認証を行う認証段階を実行させてよい。

[0010] なお、上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではない。また、これらの特徴群のサブコンビネーションもまた、発明となりうる。

図面の簡単な説明

[0011] [図1]本実施形態に係るA u C (A u t h e n t i c a t i o n C e n t r e) 装置100を用いることによって実現されるサービスを説明するための説明図である。

[図2]本実施形態に係るA u C装置100を用いることによって実現されるサービスの流れの一例を概略的に示す。

[図3]A u C装置100の機能構成の一例を概略的に示す。

[図4]鍵情報記憶部102の構成の一例を概略的に示す。

[図5]A u C装置100による処理の流れの一例を概略的に示す。

[図6]復号鍵610、復号鍵620及び復号鍵630の一例を概略的に示す。

[図7]復号鍵610、復号鍵620及び復号鍵630の他の一例を概略的に示す。

[図8]A u Cベンダ装置300の機能構成の一例を概略的に示す。

[図9] A u C 装置 1 0 0 として機能するコンピュータ 1 2 0 0 のハードウェア構成の一例を概略的に示す。

発明を実施するための形態

[0012] 以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は請求の範囲にかかる発明を限定するものではない。また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

[0013] 図 1 は、本実施形態に係る A u C 装置 1 0 0 を用いることによって実現されるサービスを説明するための説明図である。A u C 装置 1 0 0 は、認証装置の一例である。本サービスは、企業 5 0 等の内部で移動体通信ネットワークを構成できるような仕組みを提供する。

[0014] ここでは、通信事業者であるキャリア 2 0 が、移動体通信ネットワークにおけるいわゆるコアネットワークを P B X (P r i v a t e B r a n c h e X c h a n g e r) ベンダ 4 0 に提供し、P B X ベンダ 4 0 が、コアネットワークを企業 5 0 に提供することによってサービスが実現される場合を例に挙げて説明する。企業 5 0 内の携帯端末 5 2 は、当該サービスによって、企業 5 0 内のコアネットワークを介して、無線通信を実行することができる。

[0015] 携帯端末 5 2 は、例えば、スマートフォン等の携帯電話である。携帯端末 5 2 は、タブレット端末及び P C (P e r s o n a l C o m p u t e r) 等であってもよい。当該サービスを享受するのは、携帯端末 5 2 に限らない。例えば、企業 5 0 内のいわゆる I o T (I n t e r n e t o f T h i n g) 端末が、企業 5 0 内のコアネットワークを介して、無線通信を実行してもよい。

[0016] ここでは、移動体通信ネットワークが L T E (L o n g T e r m E v o l u t i o n) ネットワークである場合を主に例に挙げて説明する。コアネットワークは、1つの装置によって構成されてもよく、また、複数の装置によって構成されてもよい。

- [0017] コアネットワークが1つの装置によって構成される場合、当該装置は、HSS、MME (Mobility Management Entity)、PCRF (Policy and Charging Rule Function)、SGW (Serving Gateway)、及びPGW (Packet Data Network Gateway) として機能してよい。当該装置は、さらにIMS (IP Multimedia Subsystem) として機能してもよい。
- [0018] コアネットワークが複数の装置によって構成される場合、コアネットワークは、MMEの装置、HSSの装置、PCRFの装置、SGWの装置、及びPGWの装置から構成されてよい。コアネットワークは、これらの装置に加えてさらにIMSの装置から構成されてもよい。
- [0019] 本実施形態に係るAuC装置100は、AuCの機能を有する装置であり、コアネットワークが1つの装置によって構成される場合、AuC装置100は、当該1つの装置であってよい。すなわち、AuC装置100がコアネットワークとして機能してよい。コアネットワークが複数の装置によって構成される場合、AuC装置100は、コアネットワークを構成するHSSの装置であってよい。ここでは、AuC装置100がコアネットワークとして機能する場合を主に例に挙げて説明する。
- [0020] 移動体通信ネットワークでは、携帯端末52のSIMに記憶されている認証情報と、HSSに記憶されている認証情報とを用いて、携帯端末52のSIMの認証が行われる。キャリア20が提供するいわゆる一般的な移動体通信ネットワークにおいては、認証情報の生値がキャリア20によって厳重に管理されており、認証情報の生値が外部に漏れないことを前提としている。しかし、本実施形態におけるサービスの提供主体はPBXベンダ40であり、AuC装置100は企業50内に配置されるので、その前提は成り立たないことになる。認証情報が漏れいしてしまうと、企業50内で使用可能なクローンSIMが生成されて、企業50の無線通信サービスを不正規に利用されてしまい得る。

[0021] 本実施形態に係るサービスでは、認証用情報の漏えいを抑止する仕組みが提供される。本実施形態において、キャリア20は、暗号化された認証用情報を復号化するための復号鍵を第1復号鍵情報と第2復号鍵情報とに分割し、第1復号鍵情報をA u C装置100のベンダであるA u Cベンダ30に提供し、第2復号鍵情報をP B Xベンダ40に提供する。第1復号鍵情報及び第2復号鍵情報は、両方がそろって復号鍵を生成できる情報であり、いずれか一方のみでは復号鍵を生成することができない情報である。

[0022] キャリア20は、例えば、キャリア装置200を用いて、A u Cベンダ30のA u Cベンダ装置300に第1復号鍵情報を送信する。キャリア装置200は、例えば、ネットワーク80を介して、第1復号鍵情報をA u Cベンダ装置300に送信する。ネットワーク80は、例えば、インターネットを含む。

[0023] A u Cベンダ30は、第1復号鍵情報をA u C装置100に記憶させる。A u Cベンダ30は、例えば、A u Cベンダ装置300に、キャリア装置200から受信した第1復号鍵情報を、A u C装置100に記憶させる。A u Cベンダ装置300は、例えば、ネットワーク32を介して第1復号鍵情報をA u C装置100に送信し、記憶させる。ネットワーク32は、A u Cベンダ30が有するL A N (L o c a l A r e a N e t w o r k) 等であってよい。A u Cベンダ装置300は、A u C装置100に直接接続されてもよい。第1復号鍵情報を記憶したA u C装置100は、例えば、A u Cベンダ30からP B Xベンダ40に販売され、企業50内に配置される。

[0024] キャリア20は、例えば、キャリア装置200を用いて、P B Xベンダ40のP B Xベンダ装置400に第2復号鍵情報を送信する。キャリア装置200は、例えば、ネットワーク80を介して、第2復号鍵情報をP B Xベンダ装置400に送信する。

[0025] P B Xベンダ40は、P B Xベンダ装置400を用いて、第2復号鍵情報をA u C装置100に送信する。P B Xベンダ装置400は、例えば、ネットワーク80を介して、第2復号鍵情報を企業50内に配置されたA u C装

置 1 0 0 に送信する。

[0026] A u C 装置 1 0 0 は、記憶している第 1 復号鍵情報と、P B X ベンダ装置 4 0 0 から受信した第 2 復号鍵情報とから、復号鍵を生成する。そして、A u C 装置 1 0 0 は、暗号化された認証用情報を受信した場合に、生成した復号鍵を用いて復号化することによって、認証用情報を取得する。

[0027] このように、復号鍵を 2 つの鍵情報に分割して、A u C ベンダ 3 0 及び P B X ベンダ 4 0 のそれぞれに送信する構成とすることにより、仮に一方の鍵情報が、A u C ベンダ 3 0 又は P B X ベンダ 4 0 内で漏えいしたり、ネットワーク 8 0 上で漏えいしたりした場合であっても、復号鍵を生成できないようにすることができる。これにより、復号鍵が漏えいし、暗号化された認証用情報が復号化されて漏えいしてしまうリスクを低減することができる。

[0028] なお、第 1 復号鍵情報を A u C 装置 1 0 0 に記憶させる方法として、さまざまな方法を採用し得る。例えば、A u C ベンダ装置 3 0 0 がキャリア装置 2 0 0 から受信した第 1 復号鍵情報を、A u C ベンダ 3 0 のオペレータが手作業で A u C 装置 1 0 0 に記憶させてもよい。また、例えば、A u C ベンダ 3 0 が、データを A u C 装置 1 0 0 に書き込み可能な仕組みをキャリア 2 0 に提供し、キャリア 2 0 が、当該仕組みを利用して、A u C 装置 1 0 0 に第 1 復号鍵情報を書き込んでもよい。

[0029] 図 2 は、本実施形態に係る A u C 装置 1 0 0 を用いることによって実現されるサービスの流れの一例を概略的に示す。ここでは、キャリア 2 0 が、S I M 認証に用いる第 1 の認証用情報を暗号化し、暗号化した第 1 の認証用情報を復号化するための復号鍵を 2 つに分割して K e y A 及び K e y B とした状態を開始状態として説明する。

[0030] なお、当該復号鍵は、第 1 の認証用情報を暗号化するための暗号鍵と同一であってよい。この場合、キャリア 2 0 は、第 1 の認証用情報用の鍵を用いて第 1 の認証用情報を暗号化し、第 1 の認証用情報用の鍵を 2 つに分割する。また、当該復号鍵は、第 1 の認証用情報を暗号化する暗号鍵と異なってもよい。この場合、キャリア 2 0 は、第 1 の認証用情報用の暗号鍵を用いて第

1 の認証用情報を暗号化し、第 1 の認証用情報用の暗号鍵とは異なる、第 1 の認証用情報用の復号鍵を 2 つに分割する。ここでは、暗号鍵と復号鍵とが同一である場合を主に例に挙げて説明する。

[0031] 第 1 の認証用情報は、例えば、S I M 認証を行うときに用いられる各種パラメータを含む。具体例として、第 1 の認証用情報は、3 G P P (3 r d Generation Partnership Project) において定義されている O P 、 c 、 r 等を含む。第 1 の認証用情報は、さらに、第 2 の認証用情報用の鍵を含んでよい。第 2 の認証用情報は、S I M 認証を行うときに用いられる。第 2 の認証用情報は、S I M 毎に固有の情報であってよい。具体例として、第 2 の認証用情報は、S I M 毎に固有の鍵情報である K 値である。第 2 の認証用情報用の鍵は、第 2 の認証用情報を暗号化及び復号化するための鍵であってよい。第 2 の認証用情報用の鍵を用いて暗号化された K 値を e K I と記載する場合がある。

[0032] ステップ（ステップを S と省略して記載する場合がある。）102では、キャリア装置200が、K e y A を A u C ベンダ装置300に送信する。K e y A は、第 1 復号鍵情報の一例である。S 104では、キャリア装置200が、K e y B を P B X ベンダ装置400に送信する。K e y B は、第 2 復号鍵情報の一例である。

[0033] S 106では、A u C ベンダ装置300が、S 102において受信した K e y A を、外部から参照不可能な形式で A u C 装置100に記憶させる。S 108では、P B X ベンダ装置400が、S 104において受信した K e y B を、A u C 装置100に送信する。S 110では、A u C 装置100が、K e y A と K e y B とに基づいて復号鍵を生成する。

[0034] S 112では、キャリア20が、S I M ベンダによって製造された S I M を P B X ベンダ40に提供し、キャリア装置200が、第 1 の認証用情報を暗号化した暗号化情報と、e K I 及び I M S I を含む S I M 情報とを P B X ベンダ40に送信する。当該第 1 の認証用情報は、キャリア20が P B X ベンダ40に提供した S I M に記憶されているものであってよい。なお、ここ

でいう提供とは、貸与、譲渡、その他レンタルを内包する概念である。

[0035] キャリア 20 は、例えば、第 1 の認証用情報を SIM ベンダに通知して、第 1 の認証用情報を記憶した SIM を、SIM ベンダに製造させる。キャリア 20 は、外部に漏れることのない特定の方法で、第 1 の認証用情報を SIM ベンダに通知する。SIM ベンダは、外部から参照不可能な形式で第 1 の認証用情報を SIM に書き込む。

[0036] S114 では、PBX ベンダ装置 400 が、暗号化情報を AuC 装置 100 に送信する。S116 では、AuC 装置 100 が、S110 において生成した復号鍵を用いて、S114 において受信した暗号化情報を復号化する。

[0037] S118 では、PBX ベンダ装置 400 が、S112 において受信した SIM 情報を AuC 装置 100 に送信する。S120 では、AuC 装置 100 に、加入者情報を登録する。AuC 装置 100 は、S118 において受信した SIM 情報に含まれる eK1 を、S116 において復号化した認証用情報に含まれる第 2 の認証用情報用の鍵を用いて復号化することによって取得した K 値と、SIM 情報に含まれる IMSI とを対応付けて登録する。

[0038] 図 2 に示すサービスの流れは一例であって、各ステップの順番は異なってもよい。例えば、キャリア装置 200 が Key A 及び Key B を送信する順番は逆でもよい。また、例えば、キャリア装置 200 が暗号化情報及び SIM 情報を同時期に PBX ベンダ装置 400 に送信するのではなく、異なる時期に送信してもよい。また、例えば、AuC 装置 100 が暗号化情報と SIM 情報とを異なる時期に AuC 装置 100 に送信するのではなく、同時期に送信してもよい。

[0039] 図 3 は、AuC 装置 100 の機能構成の一例を概略的に示す。AuC 装置 100 は、鍵情報記憶部 102、復号鍵情報受信部 110、復号鍵生成部 112、暗号化情報受信部 114、復号部 116、加入者情報取得部 118、加入者情報記憶部 120、認証要求受信部 122、及び認証部 124 を備える。

[0040] 鍵情報記憶部 102 は、第 1 復号鍵情報を外部から参照不可能な形式で記

憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する。第1復号鍵情報の第1記憶領域への記憶は、例えば、A u Cベンダ装置300によって行われる。第1復号鍵情報の第1記憶領域への記憶は、A u Cベンダ30のオペレータによって行われてもよい。第1復号鍵情報の第1記憶領域への記憶は、A u Cベンダ30によってキャリア20に提供された、データをA u C装置100に書き込み可能な仕組みを利用することによって、キャリア20によって行われてもよい。第2記憶領域は、第2復号鍵情報を記憶する領域として予め定められた領域であってよい。

[0041] 復号鍵情報受信部110は、第2復号鍵情報を受信する。復号鍵情報受信部110は、外部から第2復号鍵情報を受信してよい。復号鍵情報受信部110は、例えば、P B Xベンダ装置400からネットワーク80を介して第2復号鍵情報を受信する。復号鍵情報受信部110は、受信した第2復号鍵情報を、鍵情報記憶部102の第2記憶領域に記憶する。

[0042] 復号鍵生成部112は、鍵情報記憶部102に記憶されている第1復号鍵情報と第2復号鍵情報とに基づいて復号鍵を生成する。復号鍵を第1復号鍵情報及び第2復号鍵情報に分割する方法及び第1復号鍵情報及び第2復号鍵情報に基づいて復号鍵を生成する方法としては、任意の方法を採用し得る。例えば、復号鍵を前半と後半とに分割し、当該前半と当該後半とを結合することによって復号鍵が生成される。また、例えば、予め定められた規則に基づいて復号鍵を分割し、復号鍵生成部112は、当該規則を参照して、第1復号鍵情報及び第2復号鍵情報から復号鍵を生成する。

[0043] 第1復号鍵情報と第2復号鍵情報とは、データ量が異なってもよい。例えば、第1復号鍵情報は第2復号鍵情報よりもデータ量が多く、第2復号鍵情報は第1復号鍵情報よりもデータ量が少なくてもよい。これにより、第1復号鍵情報のデータ量と第2復号鍵情報のデータ量とを同じにする場合と比較して、キャリア装置200からP B Xベンダ装置400、及びP B Xベンダ装置400からA u C装置100に対して送信される鍵情報のデータ量を低減

することができる。

[0044] また、例えば、第1復号鍵情報は第2復号鍵情報よりもデータ量が少なく、第2復号鍵情報は第1復号鍵情報よりもデータ量が多くてよい。これにより、第1復号鍵情報のデータ量と第2復号鍵情報のデータ量とを同じにする場合と比較して、例えば、A u Cベンダ30内において、複数のA u C装置100に書き込まれる第1復号鍵情報のデータ量を低減することができ、A u Cベンダ30内における通信負荷、処理負荷を低減することができる。

[0045] 暗号化情報受信部114は、暗号化情報を受信する。暗号化情報受信部114は、例えば、P B Xベンダ装置400から暗号化情報を受信する。

[0046] 復号部116は、暗号化情報受信部114が受信した暗号化情報を、復号鍵生成部112によって生成された復号鍵を用いて復号化する。復号化された情報は、認証用情報である。当該認証用情報は、上述の第1の認証用情報であってよい。

[0047] 加入者情報取得部118は、複数の加入者情報を取得する。加入者情報取得部118は、例えば、P B Xベンダ装置400から受信したS I M情報に含まれるI M S Iと、S I M情報に含まれるe K Iを復号部116によって復号化された認証用情報に含まれる第2の認証用情報用の鍵を用いて復号化したK値とを取得する。

[0048] 加入者情報記憶部120は、加入者情報取得部118が取得した加入者情報を記憶する。加入者情報記憶部120は、K値とI M S Iとを対応付けて記憶する。

[0049] 認証要求受信部122は、携帯端末52の認証要求を受信する。認証要求には、携帯端末52のS I MのS I M情報が含まれる。携帯端末52のS I M情報には、携帯端末52のI M S Iが含まれてよい。

[0050] 認証部124は、認証要求受信部122が受信した認証要求を受け付ける。認証部124は、認証要求に含まれるI M S Iと、加入者情報記憶部120に当該I M S Iと対応付けて記憶されているK値と、復号部116によって復号化された認証用情報とに基づいて、携帯端末52のS I Mを認証する。

。

[0051] 図4は、鍵情報記憶部102の構成の一例を概略的に示す。鍵情報記憶部102は、第1復号鍵情報を外部から参照不可能な形式で記憶している記憶領域104と、外部から入力された第2復号鍵情報を記憶するための記憶領域106とを有する。記憶領域104は、第1記憶領域の一例である。記憶領域106は第2記憶領域の一例である。

[0052] 図5は、A u C装置100による処理の流れの一例を概略的に示す。ここでは、ある企業50内に配置されたA u C装置100による、携帯端末52のS I Mの認証処理の流れを概略的に説明する。

[0053] S 2 0 2では、A u C装置100が配置された企業50に対して割り当てられた加入者情報を加入者情報取得部118が取得して、加入者情報記憶部120に記憶する。S 2 0 4では、認証要求受信部122が、企業50内の携帯端末52の認証要求を受信する。認証部124は、認証要求受信部122が受信した認証要求を受け付ける。

[0054] S 2 0 6では、認証部124が、認証要求に含まれるI M S Iに対応するK値を加入者情報記憶部120から読み出す。S 2 0 8では、認証部124が、乱数であるR A N Dを発生し、R A N D及びK値と、復号部116によって復号化された認証用情報とを用いて、想定応答を生成する。

[0055] S 2 1 0では、認証部124が、携帯端末52にR A N Dを送信する。携帯端末52のS I Mは、当該R A N Dを受信する。S I Mは、受信したR A N Dと、記憶しているK値及び認証用情報とを用いて、応答情報を生成し、A u C装置100に送信する。

[0056] S 2 1 2では、認証部124が、携帯端末52によって送信された応答情報を受信する。S 2 1 4では、S 2 0 8において生成した想定応答と、S 2 1 2において受信した応答情報とを比較することにより、S I Mの認証を行う。

[0057] なお、ここでは、A u C装置100がコアネットワーク全体の役割を果たす場合を例に挙げて説明したが、コアネットワークが複数の装置によって構

成され、A u C装置100がH S Sの装置である場合、認証部124は、S208において生成した想定応答と、R A N Dとを、MMEに送信してよい。そして、MMEが、携帯端末52にR A N Dを送信し、携帯端末52によって送信された応答情報と、想定応答とを比較することによって、S I Mの認証を行ってよい。

[0058] 図6は、キャリア20において準備される復号鍵の一例を概略的に示す。キャリア20は、複数のP B Xベンダ40毎に異なる復号鍵を準備してよい。図6では、P B Xベンダであるa社41用の復号鍵610、P B Xベンダであるb社42用の復号鍵620、P B Xベンダであるc社43用の復号鍵630を例示している。

[0059] 復号鍵610、復号鍵620、及び復号鍵630は、第1復号鍵情報がK e y A 650で共通であり、第2復号鍵情報が互いに異なる。復号鍵610における第2復号鍵情報はK e y B a 612であり、復号鍵620における第2復号鍵情報はK e y B b 622であり、復号鍵630における第2復号鍵情報はK e y B c 632である。

[0060] このように、複数のP B Xベンダ40毎に異なる復号鍵を準備することによって、複数のP B Xベンダ40で共通の復号鍵を用いる場合と比較して、いずれかの復号鍵が漏えいしてしまった場合に影響の及ぶ範囲を狭くすることができる。

[0061] 図7は、キャリア20において準備される復号鍵の他の一例を概略的に示す。ここでは、図6とは異なる点を主に説明する。

[0062] 図7に示す例において、復号鍵610、復号鍵620、及び復号鍵630は、第1復号鍵情報も、第2復号鍵情報も互いに異なる。復号鍵610における第1復号鍵情報はK e y A a 651であり、第2復号鍵情報はK e y B a 612である。復号鍵620における第1復号鍵情報はK e y A b 652であり、第2復号鍵情報はK e y B b 622である。復号鍵630における第1復号鍵情報はK e y A c 653であり、第2復号鍵情報はK e y B c 632である。

- [0063] このように、第1復号鍵情報についても、複数のPBXベンダ40毎に異ならせることによって、複数のPBXベンダ40で共通の第1復号鍵情報を用いる場合と比較して、第1復号鍵情報が漏えいしてしまった場合に影響が及ぶ範囲を狭くすることができる。
- [0064] 図8は、AuCベンダ装置300の機能構成の一例を概略的に示す。AuCベンダ装置300は、復号鍵情報取得部302、復号鍵情報記憶部304、及び記憶制御部306を備える。
- [0065] 復号鍵情報取得部302は、第1復号鍵情報を取得する。復号鍵情報取得部302は、例えば、キャリア装置200から第1復号鍵情報を受信する。また、復号鍵情報取得部302は、例えば、AuCベンダ30のオペレータによって入力された第1復号鍵情報を取得する。また、復号鍵情報取得部302は、例えば、外部からデータをAuC装置100に書き込み可能な仕組を提供し、当該仕組を介して入力された第1復号鍵情報を取得する。復号鍵情報記憶部304は、復号鍵情報取得部302が取得した第1復号鍵情報を記憶する。
- [0066] 記憶制御部306は、復号鍵情報記憶部304に記憶されている第1復号鍵情報を外部から参照不可能な形式でAuC装置100に記憶させる。記憶制御部306は、例えば、製造中のAuC装置100に第1復号鍵情報を記憶させる。また、記憶制御部306は、例えば、製造完了後、出荷前のAuC装置100に第1復号鍵情報を記憶させる。
- [0067] 図9は、AuC装置100として機能するコンピュータ1200のハードウェア構成の一例を概略的に示す。コンピュータ1200にインストールされたプログラムは、コンピュータ1200を、本実施形態に係る装置の1又は複数の「部」として機能させ、又はコンピュータ1200に、本実施形態に係る装置に関連付けられるオペレーション又は当該1又は複数の「部」を実行させることができ、及び／又はコンピュータ1200に、本発明の実施形態に係るプロセス又は当該プロセスの段階を実行させることができる。そのようなプログラムは、コンピュータ1200に、本明細書に記載のフロー

チャート及びブロック図のブロックのうちのいくつか又はすべてに関連付けられた特定のオペレーションを実行させるべく、CPU 1212によって実行されてよい。

[0068] 本実施形態によるコンピュータ1200は、CPU 1212、RAM 1214、及びグラフィックコントローラ1216を含み、それらはホストコントローラ1210によって相互に接続されている。コンピュータ1200はまた、通信インタフェース1222、記憶装置1224、DVDドライブ1226、及びICカードドライブのような入出力ユニットを含み、それらは入出力コントローラ1220を介してホストコントローラ1210に接続されている。DVDドライブ1226は、DVD-ROMドライブ及びDVD-RAMドライブ等であってよい。記憶装置1224は、ハードディスクドライブ及びソリッドステートドライブ等であってよい。コンピュータ1200はまた、ROM 1230及びキーボードのようなレガシの入出力ユニットを含み、それらは入出力チップ1240を介して入出力コントローラ1220に接続されている。

[0069] CPU 1212は、ROM 1230及びRAM 1214内に記憶されたプログラムに従い動作し、それにより各ユニットを制御する。グラフィックコントローラ1216は、RAM 1214内に提供されるフレームバッファ等又はそれ自体の中に、CPU 1212によって生成されるイメージデータを取得し、イメージデータがディスプレイデバイス1218上に表示されるようにする。

[0070] 通信インタフェース1222は、ネットワークを介して他の電子デバイスと通信する。記憶装置1224は、コンピュータ1200内のCPU 1212によって使用されるプログラム及びデータを記憶する。DVDドライブ1226は、プログラム又はデータをDVD-ROM 1227等から読み取り、記憶装置1224に提供する。ICカードドライブは、プログラム及びデータをICカードから読み取り、及び／又はプログラム及びデータをICカードに書き込む。

- [0071] ROM 1230はその中に、アクティブ化時にコンピュータ1200によって実行されるブートプログラム等、及び／又はコンピュータ1200のハードウェアに依存するプログラムを記憶する。入出力チップ1240はまた、様々な入出力ユニットをUSBポート、パラレルポート、シリアルポート、キーボードポート、マウスポート等を介して、入出力コントローラ1220に接続してよい。
- [0072] プログラムは、DVD-ROM1227又はICカードのようなコンピュータ可読記憶媒体によって提供される。プログラムは、コンピュータ可読記憶媒体から読み取られ、コンピュータ可読記憶媒体の例でもある記憶装置1224、RAM1214、又はROM1230にインストールされ、CPU1212によって実行される。これらのプログラム内に記述される情報処理は、コンピュータ1200に読み取られ、プログラムと、上記様々なタイプのハードウェアリソースとの間の連携をもたらす。装置又は方法が、コンピュータ1200の使用に従い情報のオペレーション又は処理を実現することによって構成されてよい。
- [0073] 例えば、通信がコンピュータ1200及び外部デバイス間で実行される場合、CPU1212は、RAM1214にロードされた通信プログラムを実行し、通信プログラムに記述された処理に基づいて、通信インタフェース1222に対し、通信処理を命令してよい。通信インタフェース1222は、CPU1212の制御の下、RAM1214、記憶装置1224、DVD-ROM1227、又はICカードのような記録媒体内に提供される送信バッファ領域に記憶された送信データを読み取り、読み取られた送信データをネットワークに送信し、又はネットワークから受信した受信データを記録媒体上に提供される受信バッファ領域等へ書き込む。
- [0074] また、CPU1212は、記憶装置1224、DVDドライブ1226（DVD-ROM1227）、ICカード等のような外部記録媒体に記憶されたファイル又はデータベースの全部又は必要な部分がRAM1214に読み取られるようにし、RAM1214上のデータに対し様々なタイプの処理を

実行してよい。CPU 1212は次に、処理されたデータを外部記録媒体にライトバックしてよい。

[0075] 様々なタイプのプログラム、データ、テーブル、及びデータベースのような様々なタイプの情報が記録媒体に記憶され、情報処理を受けてよい。CPU 1212は、RAM 1214から読み取られたデータに対し、本開示の随所に記載され、プログラムの命令シーケンスによって指定される様々なタイプのオペレーション、情報処理、条件判断、条件分岐、無条件分岐、情報の検索／置換等を含む、様々なタイプの処理を実行してよく、結果をRAM 1214に対しライトバックする。また、CPU 1212は、記録媒体内のファイル、データベース等における情報を検索してよい。例えば、各々が第2の属性の属性値に関連付けられた第1の属性の属性値を有する複数のエントリが記録媒体内に記憶される場合、CPU 1212は、当該複数のエントリの中から、第1の属性の属性値が指定されている条件に一致するエントリを検索し、当該エントリ内に記憶された第2の属性の属性値を読み取り、それにより予め定められた条件を満たす第1の属性に関連付けられた第2の属性の属性値を取得してよい。

[0076] 上で説明したプログラム又はソフトウェアモジュールは、コンピュータ 1200上又はコンピュータ 1200近傍のコンピュータ可読記憶媒体に記憶されてよい。また、専用通信ネットワーク又はインターネットに接続されたサーバシステム内に提供されるハードディスク又はRAMのような記録媒体が、コンピュータ可読記憶媒体として使用可能であり、それによりプログラムを、ネットワークを介してコンピュータ 1200に提供する。

[0077] 本実施形態におけるフローチャート及びブロック図におけるブロックは、オペレーションが実行されるプロセスの段階又はオペレーションを実行する役割を持つ装置の「部」を表わしてよい。特定の段階及び「部」が、専用回路、コンピュータ可読記憶媒体上に記憶されるコンピュータ可読命令と共に供給されるプログラマブル回路、及び／又はコンピュータ可読記憶媒体上に記憶されるコンピュータ可読命令と共に供給されるプロセッサによって実装

されてよい。専用回路は、デジタル及び／又はアナログハードウェア回路を含んでよく、集積回路（ＩＣ）及び／又はディスクリート回路を含んでよい。プログラマブル回路は、例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、及びプログラマブルロジックアレイ（ＰＬＡ）等のような、論理積、論理和、排他的論理和、否定論理積、否定論理和、及び他の論理演算、フリップフロップ、レジスタ、並びにメモリエlementを含む、再構成可能なハードウェア回路を含んでよい。

[0078] コンピュータ可読記憶媒体は、適切なデバイスによって実行される命令を記憶可能な任意の有形なデバイスを含んでよく、その結果、そこに記憶される命令を有するコンピュータ可読記憶媒体は、フローチャート又はブロック図で指定されたオペレーションを実行するための手段を作成すべく実行され得る命令を含む、製品を備えることになる。コンピュータ可読記憶媒体の例としては、電子記憶媒体、磁気記憶媒体、光記憶媒体、電磁記憶媒体、半導体記憶媒体等が含まれてよい。コンピュータ可読記憶媒体のより具体的な例としては、フロッピー（登録商標）ディスク、ディスケット、ハードディスク、ランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、消去可能プログラマブルリードオンリメモリ（ＥＰＲＯＭ又はフラッシュメモリ）、電氣的消去可能プログラマブルリードオンリメモリ（ＥＥＰＲＯＭ）、静的ランダムアクセスメモリ（ＳＲＡＭ）、コンパクトディスクリードオンリメモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）、ブルーレイ（登録商標）ディスク、メモリスティック、集積回路カード等が含まれてよい。

[0079] コンピュータ可読命令は、アセンブラ命令、命令セットアーキテクチャ（ＩＳＡ）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、又はＳｍａｌｌｔａｌｋ、ＪＡＶＡ（登録商標）、Ｃ＋＋等のようなオブジェクト指向プログラミング言語、及び「Ｃ」プログラミング言語又は同様のプログラミング言語のような従来の手続型プログラミング言語を含む、１又は複数のプログラミング言語の任意の組み合わせ

せで記述されたソースコード又はオブジェクトコードのいずれかを含んでよい。

[0080] コンピュータ可読命令は、汎用コンピュータ、特殊目的のコンピュータ、若しくは他のプログラム可能なデータ処理装置のプロセッサ、又はプログラマブル回路が、フローチャート又はブロック図で指定されたオペレーションを実行するための手段を生成するために当該コンピュータ可読命令を実行すべく、ローカルに又はローカルエリアネットワーク（LAN）、インターネット等のようなワイドエリアネットワーク（WAN）を介して、汎用コンピュータ、特殊目的のコンピュータ、若しくは他のプログラム可能なデータ処理装置のプロセッサ、又はプログラマブル回路に提供されてよい。プロセッサの例としては、コンピュータプロセッサ、処理ユニット、マイクロプロセッサ、デジタル信号プロセッサ、コントローラ、マイクロコントローラ等を含む。

[0081] 上記実施形態では、移動体通信ネットワークがLTEネットワークである場合を主に例に挙げて説明したが、これに限らない。コアネットワークが対応する移動体通信ネットワークは、例えば、3G（3rd Generation）ネットワーク、5G（5th Generation）ネットワーク、及び5Gより後の移動体通信ネットワークであってもよい。コアネットワークが3Gネットワークに対応する場合であって、コアネットワークが複数の装置によって構成される場合、AuC装置100は、HLR（Home Location Register）の装置であってよい。コアネットワークが5Gネットワークに対応する場合であって、コアネットワークが複数の装置によって構成される場合、AuC装置100は、UDM（Unified Data Management）の装置であってよい。また、本実施形態に係るAuC装置100は、LTE over Wi-Fi（登録商標）に適用されてもよい。

[0082] 以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変

更又は改良を加えることが可能であることが当業者に明らかである。そのような変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、請求の範囲の記載から明らかである。

[0083] 請求の範囲、明細書、及び図面中において示した装置、システム、プログラム、及び方法における動作、手順、ステップ、及び段階などの各処理の実行順序は、特段「より前に」、「先立って」などと明示しておらず、また、前の処理の出力を後の処理で用いるのでない限り、任意の順序で実現しうることに留意すべきである。請求の範囲、明細書、及び図面中の動作フローに関して、便宜上「まず、」、「次に、」などを用いて説明したとしても、この順で実施することが必須であることを意味するものではない。

符号の説明

- [0084] 20 キャリア
- 30 AuCペンダ
- 32 ネットワーク
- 40 PBXペンダ
- 41 a社
- 42 b社
- 43 c社
- 50 企業
- 52 携帯端末
- 80 ネットワーク
- 100 AuC装置
- 102 鍵情報記憶部
- 104 記憶領域
- 106 記憶領域
- 110 復号鍵情報受信部
- 112 復号鍵生成部
- 114 暗号化情報受信部

- 1 1 6 復号部
- 1 1 8 加入者情報取得部
- 1 2 0 加入者情報記憶部
- 1 2 2 認証要求受信部
- 1 2 4 認証部
- 2 0 0 キャリア装置
- 3 0 0 A u C ベンダ装置
- 3 0 2 復号鍵情報取得部
- 3 0 4 復号鍵情報記憶部
- 3 0 6 記憶制御部
- 4 0 0 P B X ベンダ装置
- 6 1 0 復号鍵
- 6 1 2 K e y B a
- 6 2 0 復号鍵
- 6 2 2 K e y B b
- 6 3 0 復号鍵
- 6 3 2 K e y B c
- 6 5 0 K e y A
- 6 5 1 K e y A a
- 6 5 2 K e y A b
- 6 5 3 K e y A c
- 1 2 0 0 コンピュータ
- 1 2 1 0 ホストコントローラ
- 1 2 1 2 C P U
- 1 2 1 4 R A M
- 1 2 1 6 グラフィックコントローラ
- 1 2 1 8 ディスプレイデバイス
- 1 2 2 0 入出力コントローラ

1 2 2 2 通信インタフェース

1 2 2 4 記憶装置

1 2 2 6 DVDドライブ

1 2 2 7 DVD-ROM

1 2 3 0 ROM

1 2 4 0 入出力チップ

請求の範囲

- [請求項1] 第1復号鍵情報を外部から参照不可能な形式で記憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する鍵情報記憶部と、
- 前記第1記憶領域に記憶されている前記第1復号鍵情報と、前記第2記憶領域に記憶された前記第2復号鍵情報とに基づいて復号鍵を生成する復号鍵生成部と、
- 前記復号鍵を用いて、暗号化された情報を復号化する復号部と、
- 携帯端末の認証要求を受け付け、前記認証要求に含まれる前記携帯端末のSIM (Subscriber Identity Module) のSIM情報と、前記復号部によって復号化された情報とに基づいて、前記SIMの認証を行う認証部と
- を備える認証装置。
- [請求項2] 前記第2復号鍵情報を外部から受信して前記第2記憶領域に記憶する第2復号鍵情報受信部
- を備える、請求項1に記載の認証装置。
- [請求項3] 前記第2復号鍵情報受信部は、インターネットを介して送信された前記第2復号鍵情報を受信する、請求項2に記載の認証装置。
- [請求項4] 前記第1復号鍵情報は、前記第2復号鍵情報よりもデータ量が多い、請求項1から3のいずれか一項に記載の認証装置。
- [請求項5] 前記第1復号鍵情報は、前記第2復号鍵情報よりもデータ量が少ない、請求項1から3のいずれか一項に記載の認証装置。
- [請求項6] 複数の加入者情報を記憶する加入者情報記憶部であって、前記複数の加入者情報のそれぞれは、加入者識別番号と、SIM毎に固有の鍵情報とを含む加入者情報記憶部
- を備え、
- 前記SIM情報は前記加入者識別番号を含み、
- 前記認証部は、前記SIM情報に含まれる加入者識別番号と、前記

加入者情報記憶部に当該加入者識別番号と対応付けて記憶されている鍵情報と、前記復号部によって復号化された情報とに基づいて、前記SIMの認証を行う、請求項1から5のいずれか一項に記載の認証装置。

[請求項7] 前記加入者識別番号は、IMSI (International Mobile Subscriber Identity) であり、
前記鍵情報は、K値である、
請求項6に記載の認証装置。

[請求項8] 請求項1から7のいずれか一項に記載の認証装置と、
前記認証装置を管理する管理装置であって、前記認証装置の前記第1記憶領域に前記第1復号鍵情報を記憶させる記憶制御部を有する管理装置と
を備えるシステム。

[請求項9] 前記管理装置は、
前記第1復号鍵情報を外部から受信する第1復号鍵情報受信部
を備え、
前記記憶制御部は、前記第1復号鍵情報受信部が受信した前記第1復号鍵情報を前記第1記憶領域に記憶させる、請求項8に記載のシステム。

[請求項10] 第1復号鍵情報を外部から参照不可能な形式で記憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する鍵情報記憶部を有する認証装置により実行される、
前記第1記憶領域に記憶されている前記第1復号鍵情報と、前記第2記憶領域に記憶された前記第2復号鍵情報とに基づいて復号鍵を生成する復号鍵生成段階と、
前記復号鍵を用いて、暗号化された情報を復号化する復号段階と、
携帯端末の認証要求を受け付け、前記認証要求に含まれる前記携帯

端末のSIMのSIM情報と、前記復号段階において復号化された情報とに基づいて、前記SIMの認証を行う認証段階とを備える認証方法。

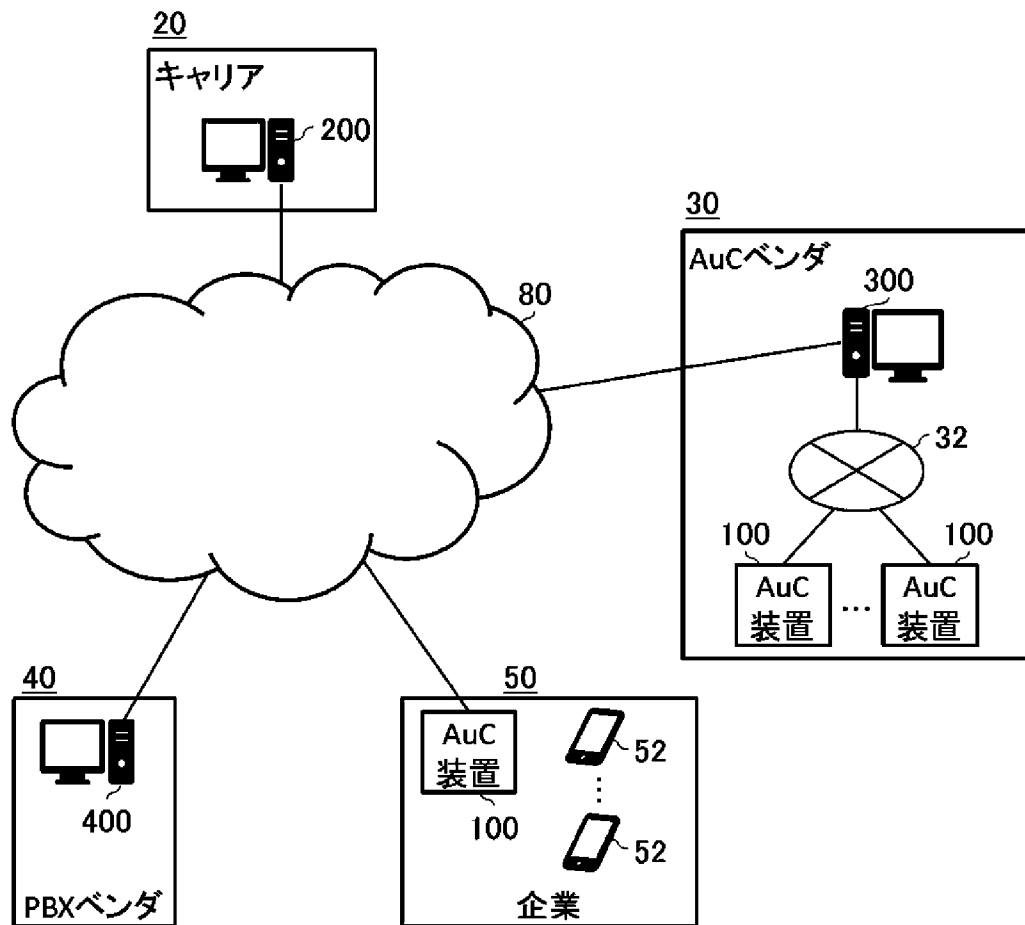
[請求項11] 第1復号鍵情報を外部から参照不可能な形式で記憶している第1記憶領域と、外部から入力された第2復号鍵情報を記憶するための第2記憶領域とを有する鍵情報記憶部を有するコンピュータに、

前記第1記憶領域に記憶されている前記第1復号鍵情報と、前記第2記憶領域に記憶された前記第2復号鍵情報とに基づいて復号鍵を生成する復号鍵生成段階、

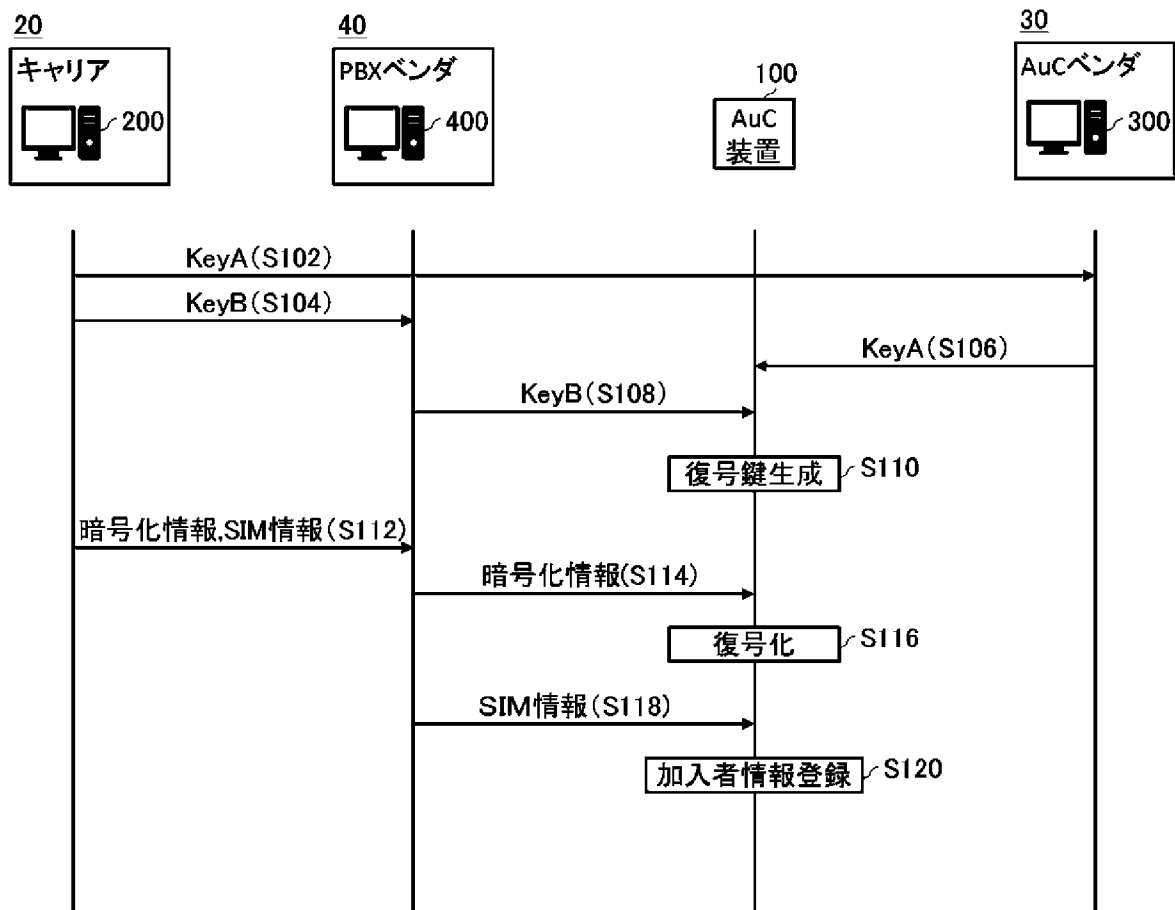
前記復号鍵を用いて、暗号化された情報を復号化する復号段階、及び

携帯端末の認証要求を受け付け、前記認証要求に含まれる前記携帯端末のSIMのSIM情報と、前記復号段階において復号化された情報とに基づいて、前記SIMの認証を行う認証段階を実行させるためのプログラム。

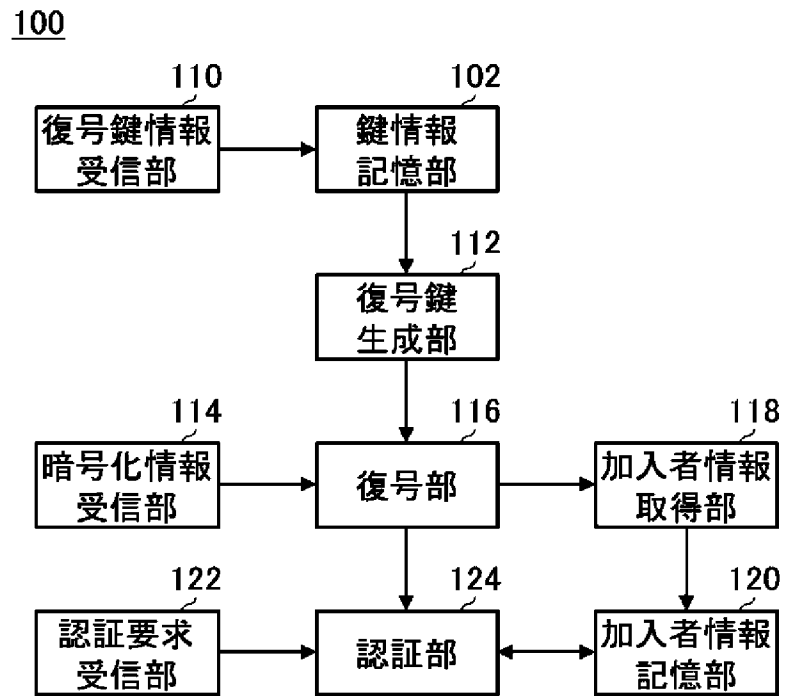
[図1]



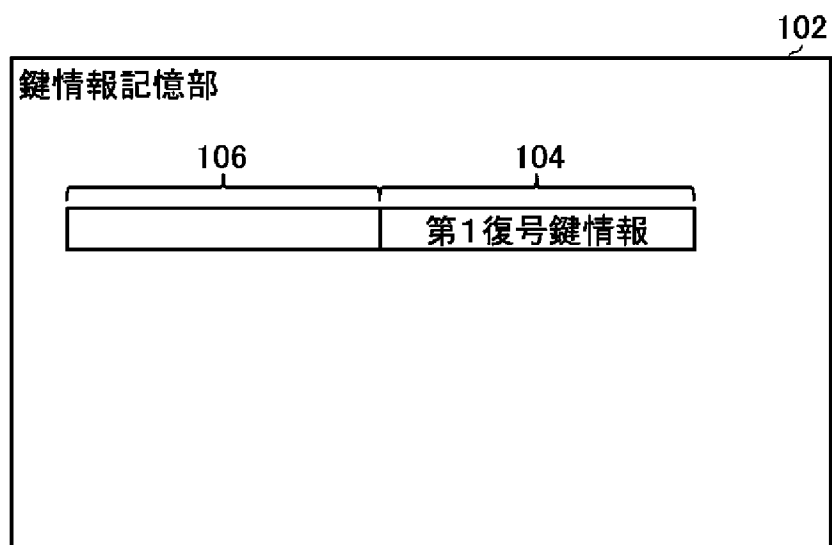
[図2]



[図3]



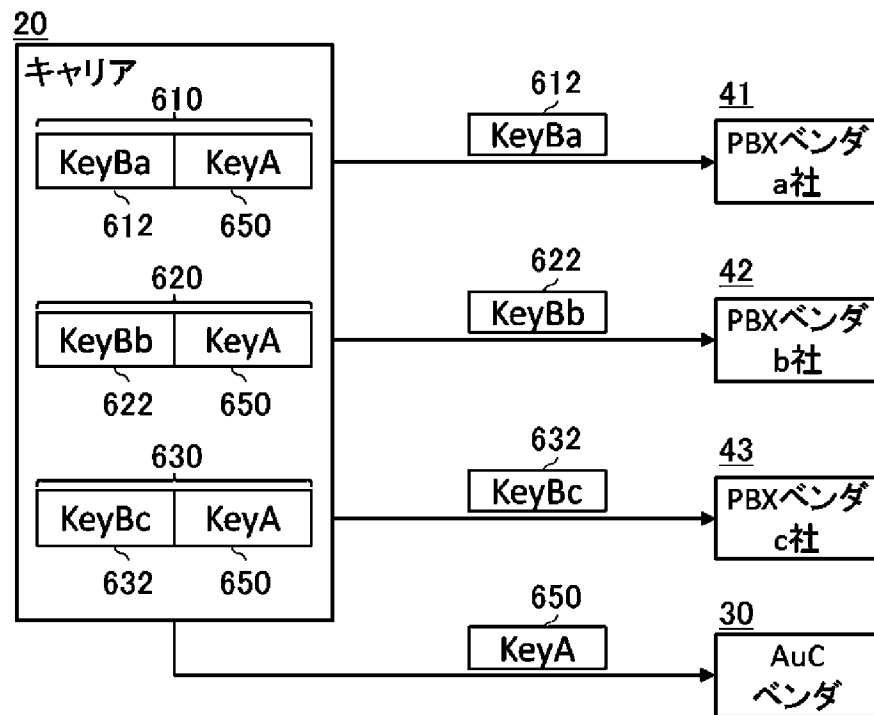
[図4]



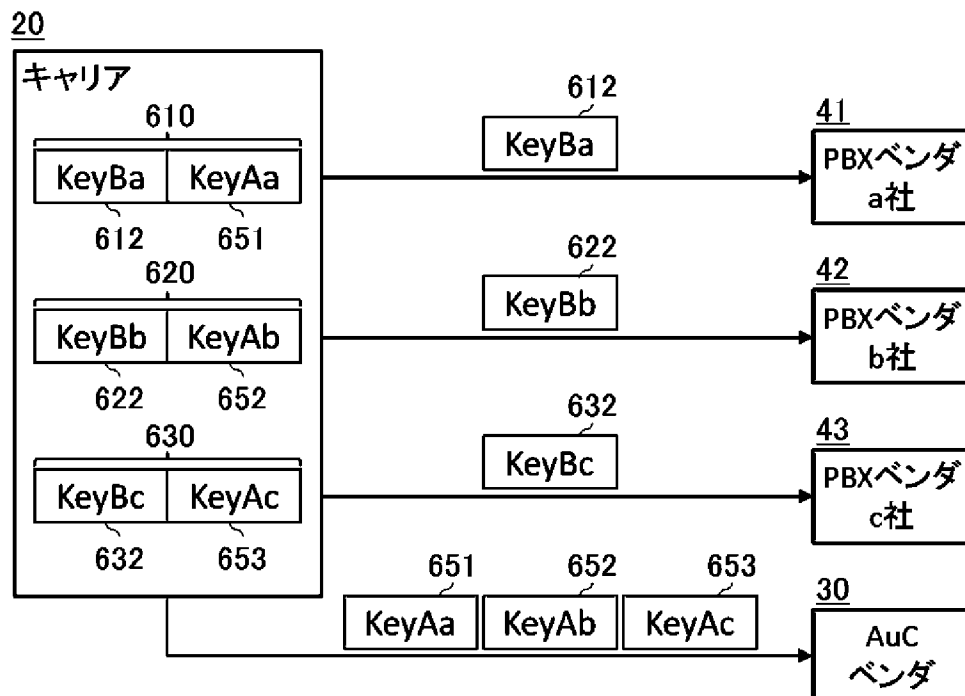
[図5]



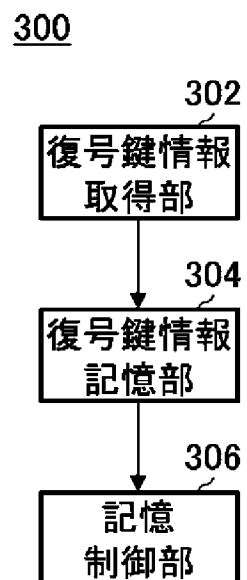
[図6]



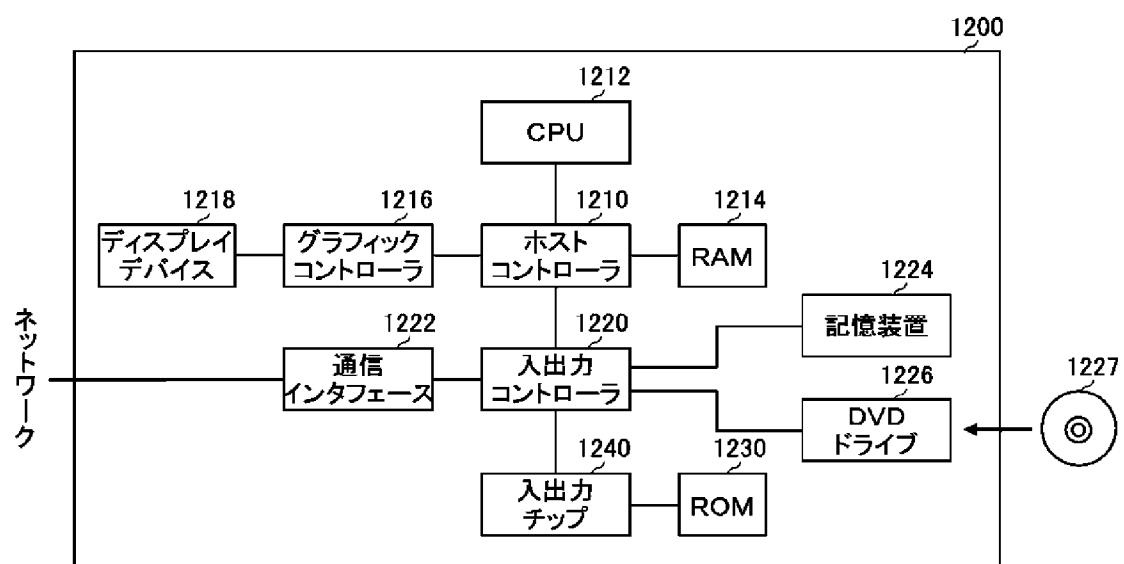
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/048402

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04W12/04 (2009.01) i, H04L9/08 (2006.01) i, H04L9/32 (2006.01) i,
H04W12/06 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. H04W12/04, H04L9/08, H04L9/32, H04W12/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-177642 A (NEC COMMUNICATION SYSTEM, LTD.) 29 June 2001, paragraphs [0002], [0025], fig. 1 (Family: none)	1-11
Y	JP 2005-20608 A (CANON INC.) 20 January 2005, paragraphs [0012]-[0026], fig. 2-4 (Family: none)	1-11
Y	JP 11-298470 A (HITACHI, LTD.) 29 October 1999, abstract, paragraphs [0022]-[0059], fig. 1 (Family: none)	1-11

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
07 March 2019 (07.03.2019)

Date of mailing of the international search report
19 March 2019 (19.03.2019)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/048402

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2015-530802 A (QUALCOMM INCORPORATED) 15 October 2015, paragraphs [0046]-[0047] & US 2014/0051422 A1 & WO 2014/028199 A1, paragraphs [0050]-[0051]	1-11

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04W12/04(2009.01)i, H04L9/08(2006.01)i, H04L9/32(2006.01)i, H04W12/06(2009.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. H04W12/04, H04L9/08, H04L9/32, H04W12/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2001-177642 A（日本電気通信システム株式会社）2001.06.29, [0002]、[0025]、[図1]（ファミリーなし）	1-11
Y	JP 2005-20608 A（キヤノン株式会社）2005.01.20, [0012] - [0026]、[図2] - [図4]（ファミリーなし）	1-11
Y	JP 11-298470 A（株式会社日立製作所）1999.10.29, [要約]、[0022] - [0059]、[図1]（ファミリーなし）	1-11

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

07.03.2019

国際調査報告の発送日

19.03.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

桑原 聡一

5 J

3984

電話番号 03-3581-1101 内線 3534

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2015-530802 A (クアルコム, インコーポレイテッド) 2015. 10. 15, [0 0 4 6] - [0 0 4 7] & US 2014/0051422 A1 & W0 2014/028199 A1, [0050]-[0051]	1-11