(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 103 03 074 B4** 2008.10.30

(12) **Patentschrift**

(21) Aktenzeichen: **103 03 074.3**
(22) Anmeldetag: **27.01.2003**
(43) Offenlegungstag: **28.08.2003**
(45) Veröffentlichungstag der Patenterteilung: **30.10.2008**

(51) Int Cl.[8]: ***H04L 9/28*** (2006.01)

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten(§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:
2002-18810 (P) 28.01.2002 JP

(73) Patentinhaber:
National Institute of Information and Communications Technology,Incorporated Administrative Agency, Tokio/Tokyo, JP

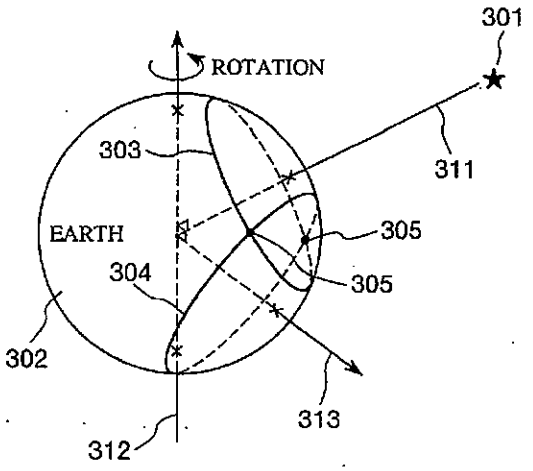
(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, 80802 München

(72) Erfinder:
Takahashi, Fujinobu, Koganei, Tokio/Tokyo, JP; Umeno, Ken, Koganei, Tokio/Tokyo, JP; Kondo, Tetsuro, Koganei, Tokio/Tokyo, JP

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US 57 57 916 A
US 41 70 776 A

(54) Bezeichnung: **Authentisierungssystem, Authentisierungsvorrichtung, Authentisierungszielvorrichtung, Authentisierungsverfahren, Verfahren zum Authentisiert-Werden, Programm und Informationsaufzeichnungsmedium**

(57) Hauptanspruch: Authentisierungssystem (101), das eine Authentisierungsvorrichtung (131) und eine Authentisierungszielvorrichtung (151) umfasst, wobei beide eine Radiowelle von einem gemeinsamen Radiostern zu einer gemeinsamen Beobachtungszeit beobachten, wobei
(a) die Authentisierungsvorrichtung (131) eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet;
(b) die Authentisierungszielvorrichtung (151) eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet und eine Informationsnachricht, die eine Information über die beobachtete Radiowelle enthält, an die Authentisierungsvorrichtung sendet; und
(c) die Authentisierungsvorrichtung (131) die Informationsnachricht, die von der Authentisierungszielvorrichtung (151) gesendet wird, empfängt,
eine Position der Authentisierungszielvorrichtung (151) in Bezug auf die Authentisierungsvorrichtung auf der Basis der "Information der Radiowelle, die durch die Authentisierungsvorrichtung (151) beobachtet wurde, die in der empfangenen Informationsnachricht enthalten ist" und "einer Information der Radiowelle, die von der Authentisierungsvorrichtung (131) beobachtet wurde", schätzt, und
die Authentisierung für die Informationsnachricht in einem Fall, bei dem eine Position der Authentisierungszielvorrichtung (151), die in der...



Beschreibung

HINTERGRUND DER ERFINDUNG

GEBIET DER ERFINDUNG

[0001] Die vorliegende Erfindung bezieht sich auf ein Authentisierungssystem, eine Authentisierungsvorrichtung, eine Authentisierungszielvorrichtung, ein Authentisierungsverfahren, ein Verfahren zum Authentisiert-Werden, ein Programm um dies auf einem Computer zu verwirklichen, und ein von einem Computer lesbares Informationsaufzeichnungsmedium für das Aufzeichnen des Programms.

[0002] Insbesondere bezieht sich die vorliegende Erfindung auf ein Authentisierungssystem, eine Authentisierungsvorrichtung, eine Authentisierungszielvorrichtung, ein Authentisierungsverfahren und ein Verfahren zum Authentisiert-Werden, die für die Authentisierung einer Authentisierungszielvorrichtung durch das Vergleichen einer Position der Authentisierungszielvorrichtung, die durch das Beobachten einer Radiowelle von einem gemeinsamen Radiostern zu einer gemeinsamen Beobachtungszeit geschätzt wird, mit der wirklichen Position der Authentisierungszielvorrichtung geeignet ist, und auf ein Programm, um dies zu verwirklichen, und auf ein vom Computer lesbares Informationsaufzeichnungsmedium für das Speichern dieses Programms.

BESCHREIBUNG DES STANDES DER TECHNIK

[0003] Konventionellerweise wurden auf dem Gebiet der Informationskommunikationstechnologien Authentisierungstechniken für die Bestätigung, wer der Erzeuger der Nachricht oder der Sender der Nachricht ist, untersucht. Heutzutage haben Unterschriftauthentisierungssysteme und Verschlüsselungskommunikationssysteme, die eine Verschlüsselung mit einem öffentlichen Schlüssel verwenden, eine weite Verbreitung gefunden.

[0004] Mittlerweile sind Versuche unternommen worden, Radiowellen, die von Radiosternen, wie Quasaren und Maser-Radioquellen (die Wasser-Maser-Radioquellen, Ammoniak-Maser-Radioquellen und Methanol-Maser-Radioquellen einschließen), ausgestrahlt werden, unter Verwendung einer VLBI (Very Long Baseline Interferometry = Interferometrie mit sehr langer Basislinie = VLB-Interferometrie) zu empfangen und die empfangenen Radiowellen in verschiedenen technischen Gebieten zu verwenden. Man erhält Vorteile, dadurch dass Signale, die durch eine VLBI empfangen werden, eine ideale vollständige Zufälligkeit aufweisen, und dass Radiowellen von Radiosternen an jedem Punkt auf der Erde empfangen werden können (man beachte, dass Radiowellen von einigen Arten von Radiosternen an jedem Punkt empfangen werden können, so lange der Punkt auf einer Oberfläche existiert, die zu den Radiosternen zeigt).

[0005] Somit haben Techniken, die eine VLBI für das Messen einer relativen Positionsbeziehung zwischen einem Punkt und einem anderen Punkt auf der Erde verwendet werden, allmählich praktische Verwendung gefunden.

[0006] Im Gebiet der Informationstechnologien ist jedoch eine sicherere Authentisierungstechnik, die ein "Vorspiegeln" verhindert, erforderlich. Insbesondere heutzutage, wo Information über die Grenzen hinweg so oft ausgetauscht wird, ist mehr Sicherheit für geheime Informationen, die zur japanischen Regierung und zu japanischen Firmen aus Übersee gesandt wird, notwendig.

[0007] US 5,757,916 beschreibt ein Authentisierungssystem, bei dem sich ein Benutzer bei einem Host-System authentifiziert, wobei der Host die geographische Position der des Benutzers als Kriterium der erfolgreichen Authentifizierung verwendet. Mehrere Signale von Satelliten werden zu einem Zeitpunkt von einer Empfangsvorrichtung, die die Signale weiter bearbeitet um die Position des Benutzers zu bestimmen, empfangen. Die ermittelte Position wird zusammen mit einer Meldung für die Authentifikation an das Host-System gesendet und mit einer dort registrierten Position des Benutzers verglichen.

[0008] In der Druckschrift US 4,170,776 wird ein Beobachtungssystem zur Verstellung der Verformung der Erdoberfläche beschrieben, bei dem eine Radioquelle auf dem Mond empfangen wird. Das Signal wird an zwei unterschiedlichen Orten auf der Erde zeitgleich von einer Strahlungsquelle empfangen und korreliert, um entsprechende Laufzeitunterschiede festzustellen und daraus auf die Positionen der Stationen zueinander zurückschließen.

ZUSAMMENFASSUNG DER ERFINDUNG

[0009] Die vorliegende Erfindung wurde vorgenommen, um das obige Problem zu lösen. Eine Aufgabe der vorliegenden Erfindung besteht somit darin, ein Authentisierungssystem, eine Authentisierungsvorrichtung, eine Authentisierungszielvorrichtung, ein Authentisierungsverfahren und ein Verfahren zum Authentisiert-Werden, die für das Authentisieren einer Authentisierungszielvorrichtung durch das Vergleichen einer Position der Authentisierungszielvorrichtung, die durch das Beobachten einer Radiowelle von einem gemeinsamen Radiostern zu einer gemeinsamen Beobachtungszeit geschätzt wird, mit der wirklichen Position der Authentisierungszielvorrichtung geeignet ist, ein Programm für das Realisieren dieses auf einem Computer und ein von einem Computer lesbares Informationsaufzeichnungsmedium für das Speichern dieses Programms bereit zu

stellen.

[0010] Um die obige Aufgabe zu lösen, wird die folgende Erfindung gemäß dem Prinzip der vorliegenden Erfindung beschrieben.

[0011] Ein Authentisierungssystem gemäß einer ersten Ausführungsform der vorliegenden Erfindung ist ein Authentisierungssystem, das eine Authentisierungsvorrichtung und eine Authentisierungszielvorrichtung umfasst, wobei beide eine Radiowelle von einem gemeinsamen Radiostern zu einer gemeinsamen Beobachtungszeit beobachten. Das Authentisierungssystem arbeitet folgendermaßen.

[0012] Die Authentisierungsvorrichtung beobachtet eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit.

[0013] Andererseits beobachtet die Authentisierungszielvorrichtung eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit und sendet eine Informationsnachricht, die Information über die beobachtete Radiowelle einschließt, an die Authentisierungsvorrichtung.

[0014] Weiter empfängt die Authentisierungsvorrichtung die Informationsnachricht, die von der Authentisierungszielvorrichtung gesendet wird, schätzt eine Position der Authentisierungszielvorrichtung in Bezug auf die Authentisierungsvorrichtung auf der Basis "der Information der Radiowelle, die durch die Authentisierungszielvorrichtung beobachtet wurde, die in der empfangenen Informationsnachricht enthalten ist", und "der Information der Radiowelle, die durch die Authentisierungsvorrichtung beobachtet wurde" und legt die Authentisierung für die Information in einem Fall, bei dem eine Position der Authentisierungszielvorrichtung, die in der Authentisierungsvorrichtung im Vorhinein gespeichert wurde, und die geschätzte Position der Authentisierungszielvorrichtung innerhalb einem vorbestimmten Fehlerbereich einander entsprechen, als Erfolg fest.

[0015] Im Authentisierungssystem gemäß der vorliegenden Erfindung können "die gemeinsame Beobachtungszeit und/oder der gemeinsame Radiostern" durch eine Vorbereitungsnachricht, die von der Authentisierungsvorrichtung an die Authentisierungszielvorrichtung im Vorhinein zu senden ist, bezeichnet werden.

[0016] Im Authentisierungssystem gemäß der vorliegenden Erfindung können "die gemeinsame Beobachtungszeit und/oder der gemeinsame Radiostern" durch eine Vorbereitungsnachricht, die von der Authentisierungszielvorrichtung an die Authentisierungsvorrichtung im Vorhinein zu senden ist, bezeichnet werden.

[0017] Im Authentisierungssystem gemäß der vorliegenden Erfindung kann die Anzahl der Radiosterne gleich oder größer als 2 sein.

[0018] Im Authentisierungssystem gemäß der vorliegenden Erfindung, kann der gemeinsame Radiostern eine Maserradioquelle (die eine Wassermaserradioquelle, eine Ammoniakmaserradioquelle und eine Methanolmaserradioquelle einschließt) oder ein Quasar sein.

[0019] Im Authentisierungssystem gemäß der vorliegenden Erfindung können in einem Fall, bei dem die Authentisierung für die Informationsnachricht als ein Erfolg festgelegt wird, die Authentisierungsvorrichtung und die Authentisierungszielvorrichtung eine Verschlüsselungskommunikation unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet wird, durchführen.

[0020] Im Authentisierungssystem gemäß der vorliegenden Erfindung können in einem Fall, bei dem die Authentisierung für die Informationsnachricht als ein Erfolg festgelegt wird, die Authentisierungsvorrichtung und die Authentisierungszielvorrichtung eine Verschlüsselungskommunikation unter Verwendung eines gemeinsamen Schlüssels, der im Vorhinein in Verbindung mit der Authentisierungsvorrichtung und der Authentisierungszielvorrichtung ausgewählt wird, durchführen.

[0021] Im Authentisierungssystem gemäß der vorliegenden Erfindung können in einem Fall, bei dem die Authentisierung für die Informationsnachricht als ein Erfolg festgelegt wird, die Authentisierungsvorrichtung und die Authentisierungszielvorrichtung eine Verschlüsselungskommunikation unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der zwischen ihnen geteilt wird, einem geheimen Schlüssel, der der Authentisierungsvorrichtung zugehört, und einem geheimen Schlüssel, der der Authentisierungszielvorrichtung zugehört, erzeugt wird, durchführen.

[0022] Im Authentisierungssystem gemäß der vorliegenden Erfindung kann der öffentliche Schlüssel, der von der Authentisierungsvorrichtung und der Authentisierungszielvorrichtung geteilt wird, aus "Information der Radiowelle, die durch die Authentisierungszielvorrichtung beobachtet wurde" erzeugt werden.

[0023] Eine Authentisierungsvorrichtung gemäß einem anderen Aspekt der vorliegenden Erfindung ist die Authentisierungsvorrichtung, die im oben beschriebenen Authentisierungssystem enthalten ist.

[0024] Eine Authentisierungszielvorrichtung gemäß einem anderen Aspekt der vorliegenden Erfindung ist die Authentisierungszielvorrichtung, die im oben be-

schriebenen Authentisierungssystem enthalten ist.

[0025] Ein Authentisierungsverfahren gemäß einem anderen Aspekt der vorliegenden Erfindung ist ein Authentisierungsverfahren der Beobachtung einer Radiowelle von einem Radiostern, der einer Authentisierungszielvorrichtung gemeinsam ist, zu einer Beobachtungszeit, die der Authentisierungszielvorrichtung gemeinsam ist, und umfasst einen Beobachtungsschritt, einen Informationsempfangsschritt, einen Schätzschritt und einen Bestimmungsschritt.

[0026] Im Beobachtungsschritt wird eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet.

[0027] Im Informationsempfangsschritt wird eine Informationsnachricht, die von der Authentisierungszielvorrichtung gesendet wird, empfangen.

[0028] Im Schätzschritt wird eine Position der Authentisierungszielvorrichtung auf der Basis "einer Information der Radiowelle, die durch die Authentisierungszielvorrichtung beobachtet wurde, die in der empfangenen Informationsnachricht enthalten ist" und "einer Information der Radiowelle, die im Beobachtungsschritt beobachtet wurde", geschätzt.

[0029] Im Bestimmungsschritt wird eine Authentisierung für die Informationsnachricht in einem Fall, bei dem eine Position der Authentisierungszielvorrichtung, die im Vorhinein gespeichert wurde, und die geschätzte Position der Authentisierungszielvorrichtung innerhalb eines vorbestimmten Fehlerbereichs einander entsprechen, als ein Erfolg festgelegt.

[0030] Das Authentisierungsverfahren gemäß der vorliegenden Erfindung kann weiter einen Vorbereitungssendeschritt umfassen. Im Vorbereitungssendeschritt kann eine Vorbereitungsnachricht für das Bezeichnen "der gemeinsamen Beobachtungszeit und/oder des gemeinsamen Radiosterns" an die Authentisierungszielvorrichtung im Vorhinein gesandt werden.

[0031] Das Authentisierungsverfahren gemäß der vorliegenden Erfindung kann weiter einen Vorbereitungsempfangsschritt umfassen. Im Vorbereitungsempfangsschritt kann eine Vorbereitungsnachricht für das Bezeichnen "einer Beobachtungszeit und/oder eines Radiosterns" empfangen werden.

[0032] Andererseits kann im Beobachtungsschritt eine Radiowelle in einem Fall beobachtet werden, bei dem die empfangene Vorbereitungsnachricht eine Beobachtungszeit bezeichnet, durch das Betrachten der bezeichneten Beobachtungszeit als die gemeinsame Beobachtungszeit, und in einem Fall, bei dem die empfangene Vorbereitungsnachricht einen Radiostern bezeichnet, durch das Betrachten des bezeichneten Radiosterns als gemeinsamen Radiostern.

[0033] Das Authentisierungsverfahren gemäß der vorliegenden Erfindung kann weiter einen Verschlüsselungskommunikationsdurchführungsschritt umfassen. Im Verschlüsselungskommunikationsdurchführungsschritt kann eine Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet wird, in einem Fall, bei der die Authentisierung für die Informationsnachricht als Erfolg festgelegt wird, durchgeführt werden.

[0034] Das Authentisierungsverfahren gemäß der vorliegenden Erfindung kann weiter einen Verschlüsselungskommunikationsdurchführungsschritt umfassen. Im Verschlüsselungskommunikationsdurchführungsschritt kann eine Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der im Vorhinein in Verbindung mit der Authentisierungszielvorrichtung ausgewählt wird, in einem Fall, bei der die Authentisierung für die Informationsnachricht als Erfolg festgelegt wird, durchgeführt werden.

[0035] Das Authentisierungsverfahren gemäß der vorliegenden Erfindung kann weiter einen Verschlüsselungskommunikationsdurchführungsschritt umfassen. Im Verschlüsselungskommunikationsdurchführungsschritt kann eine Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der mit der Authentisierungszielvorrichtung geteilt wird, einem vorbestimmten geheimen Schlüssel und einem geheimen Schlüssel, der der Authentisierungszielvorrichtung zugehört, erzeugt wird, in einem Fall, bei der die Authentisierung für die Informationsnachricht als Erfolg festgelegt wird, durchgeführt werden.

[0036] Das Authentisierungsverfahren gemäß der vorliegenden Erfindung kann weiter einen Erzeugungsschritt des öffentlichen Schlüssels umfassen. Im Erzeugungsschritt des öffentlichen Schlüssels kann der öffentliche Schlüssel, der mit der Authentisierungszielvorrichtung geteilt wird, aus "Information einer Radiowelle, die durch die Authentisierungszielvorrichtung beobachtet wird" erzeugt werden.

[0037] Ein Verfahren zum Authentisiert-Werden gemäß einem anderen Aspekt der vorliegenden Erfindung ist ein Verfahren zum Authentisiert-Werden, in dem eine Radiowelle von einem Radiostern, der einer Authentisierungsvorrichtung gemeinsam ist, zu einer Beobachtungszeit, die der Authentisierungsvorrichtung gemeinsam ist, beobachtet wird, wobei es einen Beobachtungsschritt und einen Sendeschritt

umfasst.

[0038] Im Beobachtungsschritt wird eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet.

[0039] Im Sendeschritt wird eine Informationsnachricht, die Information der beobachteten Radiowelle enthält, an die Authentisierungsvorrichtung gesandt.

[0040] Das Verfahren zum Authentisiert-Werden gemäß der vorliegenden Erfindung kann weiter einen Vorbereitungssendeschritt umfassen. Im Vorbereitungssendeschritt kann eine Vorbereitungsnachricht für das Bezeichnen "der gemeinsamen Beobachtungszeit und/oder des gemeinsamen Radiosterns" zur Authentisierungsvorrichtung im Vorhinein gesandt werden.

[0041] Das Verfahren zum Authentisiert-Werden gemäß der vorliegenden Erfindung kann weiter einen Vorbereitungsempfangsschritt umfassen. Im Vorbereitungsempfangsschritt kann eine Vorbereitungsnachricht für das Bezeichnen "einer Beobachtungszeit und/oder eines Radiosterns" empfangen werden.

[0042] Andererseits kann im Beobachtungsschritt eine Radiowelle in einem Fall beobachtet werden, bei dem die empfangene Vorbereitungsnachricht eine Beobachtungszeit bezeichnet, durch das Betrachten der bezeichneten Beobachtungszeit als gemeinsame Beobachtungszeit, und in einem Fall, bei der die empfangene Vorbereitungsnachricht einen Radiostern bezeichnet, durch das Betrachten des bezeichneten Radiosterns als gemeinsamen Radiostern.

[0043] Das Verfahren zum Authentisiert-Werden gemäß der vorliegenden Erfindung kann weiter einen Verschlüsselungskommunikationsdurchführungsschritt umfassen. Im Verschlüsselungskommunikationsdurchführungsschritt kann eine Verschlüsselungskommunikation mit der Authentisierungsvorrichtung unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet ist, in einem Fall, bei dem die Authentisierungsvorrichtung die Authentisierung für die Information als Erfolg festsetzt, durchgeführt werden.

[0044] Das Verfahren zum Authentisiert-Werden gemäß der vorliegenden Erfindung kann weiter einen Verschlüsselungskommunikationsdurchführungsschritt umfassen. Im Verschlüsselungskommunikationsdurchführungsschritt kann eine Verschlüsselungskommunikation mit der Authentisierungsvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der im Vorhinein in Verbindung mit der Authentisierungsvorrichtung ausgewählt wird, in einem Fall, bei dem die Authentisierungsvorrichtung die Authentisierung für die Information als Erfolg festsetzt, durchgeführt werden.

[0045] Das Verfahren zum Authentisiert-Werden gemäß der vorliegenden Erfindung kann weiter einen Verschlüsselungskommunikationsdurchführungsschritt umfassen. Im Verschlüsselungskommunikationsdurchführungsschritt kann eine Verschlüsselungskommunikation mit der Authentisierungsvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der mit der Authentisierungsvorrichtung geteilt wird, einem geheimen Schlüssel, der der Authentisierungsvorrichtung zugehört, und einem vorbestimmten geheimen Schlüssel erzeugt wird, in einem Fall, bei dem die Authentisierung für die Information als Erfolg festgesetzt wurde, durchgeführt werden.

[0046] Das Verfahren zum Authentisiert-Werden gemäß der vorliegenden Erfindung kann weiter einen Erzeugungsschritt eines öffentlichen Schlüssels umfassen. Im Erzeugungsschritt des öffentlichen Schlüssels kann der öffentliche Schlüssel, der mit der Authentisierungsvorrichtung geteilt wird, aus "Information der Radiowelle, die im Beobachtungsschritt beobachtet wurde" erzeugt werden.

[0047] Ein Programm gemäß einem anderen Aspekt der vorliegenden Erfindung dient zur Steuerung eines Computers, damit dieser als die Authentisierungsvorrichtung, die oben beschrieben wurde, dient, und für das Steuern eines Computers, um das oben beschriebene Authentisierungsverfahren durchzuführen.

[0048] Ein Programm gemäß einem anderen Aspekt der vorliegenden Erfindung dient zur Steuerung eines Computers, damit dieser als Authentisierungszielvorrichtung, die oben beschrieben wurde, dient, und für das Steuern eines Computers, um das oben beschriebene Verfahren zum Authentisiert-Werden durchzuführen.

[0049] Ein vom Computer lesbares Informationsaufzeichnungsmedium (das eine Compact-Disk, eine flexible Platte, eine Festplatte, eine magnetisch-optische Platte, eine digitale Bildplatte, ein Magnetband oder einen Halbleiterspeicher einschließt) speichert gemäß einem anderen Aspekt der vorliegenden Erfindung jedes der oben beschriebenen Programme.

[0050] Dieses Informationsaufzeichnungsmedium kann unabhängig von einem Computer verteilt oder verkauft werden. Jedes der oben beschriebenen Programme kann selbst über ein Computerkommunikationsnetzwerk, wie das Internet, verteilt oder verkauft werden.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0051] Diese Aufgabe und andere Aufgaben und Vorteile der vorliegenden Erfindung werden beim Lesen der folgenden detaillierten Beschreibung und der

begleitenden Zeichnungen deutlicher.

[0052] Fig. 1 ist ein beispielhaftes Diagramm, das eine schematische Struktur eines Authentisierungssystem gemäß einer Ausführungsform der vorliegenden Erfindung zeigt;

[0053] Fig. 2 ist ein Flussdiagramm, das den Ablauf eines Verfahrens für die Authentisierung und ein Verfahren für das Authentisiert-werden gemäß einer Ausführungsform der vorliegenden Erfindung zeigt;

[0054] Fig. 3 ist ein beispielhaftes Diagramm, das schematisch gemeinsame Wellenfrontverzögerungslinien einer Radiowelle von einem Radiostern zeigt;

[0055] Fig. 4 ist ein beispielhaftes Diagramm, das gemeinsame Verzögerungszeitverhältnislinien einer Radiowelle von einem Radiostern zeigt;

[0056] Fig. 5 ist ein Diagramm, das Ergebnisse der Berechnung einer zweidimensionalen schnellen Fourier-Transformation zeigt, wobei die Verzögerung und das Verzögerungszeitverhältnis erhalten werden können;

[0057] Fig. 6 ist ein erläuterndes Diagramm, das die Beziehung zwischen einer gemeinsamen Wellenfrontverzögerungslinie, einer gemeinsamen Verzögerungszeitverhältnislinie und einer geschätzten Position zeigt; und

[0058] Fig. 7 ist ein beispielhaftes Diagramm, das eine schematische Struktur eines Authentisierungssystems gemäß einer anderen Ausführungsform der vorliegenden Erfindung zeigt.

DETAILLIERTE BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

Ausführungsform der Erfindung

[0059] Nachfolgend wird nun eine Ausführungsform der vorliegenden Erfindung erläutert. Die nachfolgend beschriebene Ausführungsform soll nur erläuternden Zwecken dienen und den Umfang der vorliegenden Erfindung nicht einschränken. Somit wird, sogar dann wenn Fachleute eine Ausführungsform verwenden können, bei der einzelne Elemente oder alle Elemente, die in der nachfolgend beschriebenen Ausführungsform eingeschlossen sind, durch äquivalente Elemente ersetzt werden, eine solche Ausführungsform auch als eingeschlossen im Umfang der vorliegenden Erfindung betrachtet.

[0060] Fig. 1 ist ein beispielhaftes Diagramm, das eine schematische Struktur eines Authentisierungssystems gemäß einer Ausführungsform der vorliegenden Erfindung zeigt. Fig. 2 ist ein Flussdiagramm, das ein Verfahren für die Authentisierung und ein Verfahren für das Authentisiert-Werden, die im Authentisierungssystem, das in Fig. 1 gezeigt ist, durchgeführt werden sollen, zeigt. Die folgende Erläuterung erfolgt unter Bezug auf solche Diagramme.

[0061] Ein Authentisierungssystem **101** umfasst eine Authentisierungsvorrichtung **131** und eine Authentisierungszielvorrichtung **151**. Die Authentisierungsvorrichtung **131** beobachtet eine Radiowelle von einem Radiostern, bei dem es sich um denselben Radiostern handelt, dessen Radiowelle die Authentisierungszielvorrichtung **151** beobachtet, zur selben Zeit, wie die Authentisierungszielvorrichtung **151** diese beobachtet.

[0062] Die Authentisierungsvorrichtung **131** umfasst eine Beobachtungseinheit **132**, eine Informationsempfangseinheit **133**, eine Schätzeinheit **134**, eine Speichereinheit **135**, eine Bestimmungseinheit **136** und eine Vorbereitungssendeeinheit **137**.

[0063] Die Authentisierungszielvorrichtung **151** umfasst eine Beobachtungseinheit **152**, eine Informationssendeeinheit **153** und eine Vorbereitungsempfangseinheit **154**.

[0064] Zuerst sendet die Vorbereitungssendeeinheit **137** der Authentisierungsvorrichtung **131** eine Vorbereitungsnachricht für das Bezeichnen einer Beobachtungszeit und eines Radiostern an die Authentisierungszielvorrichtung **151** (Schritt **201**).

[0065] Die Beobachtungszeit muss eine Zeit nach der Zeit des Sendens der Vorbereitungsnachricht sein, die um eine Zeitdauer versetzt ist, die für das Fertigmachen der Authentisierungsvorrichtung **131** und der Authentisierungszielvorrichtung **151** für die Beobachtung benötigt wird. Es ist jedoch vorteilhaft, wenn die Zeitdauer, die von der Sendezeit der Nachricht an vergeht, so kurz wie möglich ist.

[0066] Wie oben beschrieben wurde, so kann eine Maserradioquelle (die eine Wassermaserradioquelle, eine Ammoniakmaserradioquelle und eine Methanolmaserradioquelle einschließt) oder ein Quasar als Radiostern bezeichnet werden. Die Anzahl der bezeichneten Radiosterne ist nicht auf einen begrenzt, sondern sie kann mehrere umfassen.

[0067] Andererseits empfängt die Vorbereitungsempfangseinheit **154** der Authentisierungszielvorrichtung **151** die Vorbereitungsnachricht für das Bezeichnen einer Beobachtungszeit und eines Radiostern, die in Schritt S201 gesendet wird, von der Authentisierungsvorrichtung **131** (Schritt **202**).

[0068] Die Beobachtungseinheit **132** der Authentisierungsvorrichtung **131** beobachtet eine Radiowelle vom Radiostern, der in der Vorbereitungsnachricht bezeichnet wurde, zur Beobachtungszeit, die in der

Vorbereitungsnachricht bezeichnet wurde (Schritt **203**).

[0069] Und die Beobachtungseinheit **152** der Authentisierungszielvorrichtung **151** beobachtet eine Radiowelle vom Radiostern, der in der Vorbereitungsnachricht bezeichnet wurde, zur Beobachtungszeit, die in der Vorbereitungsnachricht bezeichnet wurde (Schritt S204).

[0070] Die Beobachtungseinheit **132** der Authentisierungsvorrichtung **131** und die Beobachtungseinheit **152** der Authentisierungszielvorrichtung **151** beziehen sich auf ihre (nicht dargestellten) jeweiligen Referenzuhren. Somit können beiden den Radiostern zur korrekten Zeit beobachten.

[0071] Somit beobachten die Authentisierungsvorrichtung **131** und die Authentisierungszielvorrichtung **151** eine Radiowelle vom selben Radiostern zur selben Beobachtungszeit.

[0072] Dann sendet die Informationssendeeinheit **153** der Authentisierungszielvorrichtung **151** eine Informationsnachricht, die Information über die beobachtete Radiowelle enthält, an die Authentisierungsvorrichtung **131** (Schritt S205).

[0073] Die Informationsempfangseinheit **133** der Authentisierungsvorrichtung **131** empfängt die Informationsnachricht, die von der Authentisierungszielvorrichtung **151** gesendet wird (Schritt S206).

[0074] Dann schätzt die Schätzeinheit **134** der Authentisierungsvorrichtung **131** die Position der Authentisierungszielvorrichtung **151** in Bezug auf die Authentisierungsvorrichtung **131** auf der Basis der "Information über die Radiowelle, die durch die Authentisierungszielvorrichtung **151** beobachtet wird", die in der im Schritt S206 empfangenen Informationsnachricht enthalten ist, und basierend auf der Information über die Radiowelle, die durch die Beobachtungseinheit **132** der Authentisierungsvorrichtung **131** selbst beobachtet wurde (Schritt S207).

[0075] Dadurch kann die Authentisierungsvorrichtung **131** authentisieren, ob die Informationsnachricht von einer spezifischen Koordinatenposition auf der Erde (der Position der Authentisierungszielvorrichtung **151**) zu einer spezifischen Zeit (der gemeinsamen Beobachtungszeit) gesendet wurde.

[0076] Die Speichereinheit **135** speichert im Voraus Positionen einer oder mehrerer Authentisierungszielvorrichtungen, die die Authentisierungszielvorrichtung **151**, die die Authentisierungsvorrichtung **131** nun authentisiert, einschließt.

[0077] Die Bestimmungseinheit **136** bestimmt, ob die Position der Authentisierungszielvorrichtung **151**, die im Voraus in der Speichereinheit **135** gespeichert wurde, und die Position der Authentisierungszielvorrichtung **151**, die im Schritt S207 geschätzt wurde, innerhalb eines vorbestimmten Fehlerbereichs einander entsprechen (Schritt S208).

[0078] In einem Fall, bei dem die Positionen einander entsprechen (Schritt S208, Ja), wird die Authentisierung für die Informationsnachricht als Erfolg festgelegt (Schritt S209). Dann benachrichtigt die Authentisierungsvorrichtung **131** die Authentisierungszielvorrichtung **151**, dass die Authentisierung zu einem Erfolg geführt hat (Schritt S210), und die Authentisierungszielvorrichtung **151** empfängt die Benachrichtigung, dass die Authentisierung zu einem Erfolg geführt hat (Schritt S211).

[0079] Somit sind das Verfahren für die Authentisierung und das Verfahren für das Authentisiert-Werden beendet. Danach können die Authentisierungsvorrichtung **131** und die Authentisierungszielvorrichtung **151** ein Nach-Authentisierungsverfahren (beispielsweise eine Kommunikation zwischen sich unter Verwendung einer Verschlüsselung, wie das später beschrieben wird) beginnen.

[0080] Andererseits wird in einem Fall, bei dem die beiden Positionen einander nicht entsprechen (Schritt S208, Nein) die Authentisierung für die Informationsnachricht als misslungen festgelegt (Schritt S212). Die Authentisierungsvorrichtung **131** benachrichtigt die Authentisierungszielvorrichtung, dass die Authentisierung nicht zu einem Erfolg geführt hat (nicht gezeigt), und die Authentisierungszielvorrichtung **151** empfängt die Benachrichtigung, dass die Authentisierung misslungen ist (nicht gezeigt). Somit sind das Verfahren für die Authentisierung und das Verfahren für das Authentisiert-Werden beendet.

[0081] Gemäß der vorliegenden Ausführungsform wird die Authentisierung durch das Schätzen der Position der Authentisierungszielvorrichtung **151** zu einer spezifischen Zeit und das Vergleichen der geschätzten Position mit der schon bekannten Position der Authentisierungszielvorrichtung **151** durchgeführt.

[0082] Es ist möglich, eine ähnliche Positionsschätzung unter Verwendung einer Radiowelle von einem künstlichen Satelliten für das GPS (globales Positioniersystem) durchzuführen. Wenn der Administrator des künstlichen Satelliten einige Freiheit besitzt, so kann er oder sie die Information über die Beobachtung einer Radiowelle fälschen oder sich an dieser zu schaffen machen. Andererseits besteht gemäß der vorliegenden Ausführungsform, da ein Radiostern verwendet wird, bei dem es sich um einen natürlichen Himmelskörper handelt, keine Möglichkeit zur Fälschung oder zum unerlaubten Eingriff. Ein anderer Unterschied zum GPS besteht darin, dass der Emp-

fang der Signale vollständig offen ist, und somit jedermann die Signale frei empfangen kann.

[0083] Wenn weiterhin in der vorliegenden Ausführungsform jemand ein "Vortäuschen" versucht, so muss er oder sie eine Radiowelle von einem Radiostern zur bezeichneten Beobachtungszeit am Ort, an dem die Authentisierungszielvorrichtung **151** tatsächlich existiert, empfangen. Gemäß den Prinzipien der Relativitätstheorie ist jedoch eine Bewegung mit einer Geschwindigkeit höher als der Lichtgeschwindigkeit unmöglich. Somit ist es praktisch unmöglich, dass die täuschende Person eine Radiowelle von einem Radiostern zur Beobachtungszeit am Ort, an dem die Authentisierungszielvorrichtung **151** existiert, empfängt.

[0084] Das Prinzip der Positionsschätzungstechnik unter Verwendung einer VLBI wird nachfolgend detaillierter erläutert.

Verfahren der Positionsschätzung

[0085] Fig. 3 ist ein erläuterndes Diagramm, das schematisch gemeinsame Wellenfrontverzögerungslinien einer Radiowelle von einem Radiostern zeigt. Die folgende Erläuterung erfolgt unter Bezug auf dieses Diagramm unter der Annahme, dass die Erde eine Kugel ist.

[0086] Eine Radiowelle, die vom einem Radiostern **301** abgestrahlt wird, breitet ihr Wellenfronten kugelförmig vom Radiostern **301** aus. Somit kommt eine gemeinsame Wellenfront zur selben Zeit an Punkten an, die auf einer Schnittlinie **303** einer "Ebene rechtwinklig zur einer Linie **311**, die den Radiostern **301** mit dem Zentrum der Erde **302** verbindet", und "der Oberfläche **302** der Erde" existieren, an. Somit wird diese Schnittlinie **303** die gemeinsame Wellenfrontverzögerungslinie genannt. Die gemeinsamen Wellenfrontverzögerungslinien sind als konzentrische Kreise angeordnet, wobei ihre Zentren auf der Linie **311** liegen.

[0087] Fig. 4 ist ein erläuterndes Diagramm, das schematisch gemeinsame Verzögerungszeitverhältnislinien einer Radiowelle von einem Radiostern zeigt. Die folgende Erläuterung erfolgt in Bezug auf dieses Diagramm.

[0088] Die Erde **302** rotiert um ihre Achse. Somit sind konzentrische Kreise, von denen jeder aus Punkten besteht, die ein gemeinsames Verzögerungszeitverhältnis aufweisen, auf einer Achse **313** rechtwinklig zu einer Ebene angeordnet ist, die durch "eine Linie **311**, die den Radiostern **301** mit dem Zentrum der Erde **302** verbindet" und "einer Polachse **312** der Erde **302** (einer Linie, die den Nordpol und den Südpol verbindet)" gezogen wird. Jede Linie **304**, die sich mit diesen Punkten, die ein gemeinsames Verzögerungszeitverhältnis aufweisen, verbindet, wird eine gemeinsame Verzögerungszeitverhältnislinie genannt.

[0089] Es ist möglich, die Verzögerung der Authentisierungszielvorrichtung **151** in Bezug auf die Authentisierungsvorrichtung **131** und das Verzögerungszeitverhältnis zu erhalten, indem Information, die jeweils durch die Authentisierungsvorrichtung **131** und durch die Authentisierungszielvorrichtung **151** aus der gleichzeitigen Beobachtung einer Radiowelle, die sich miteinander überlagern, erhalten wird, und das Anwenden einer schnellen Fouriertransformation auf das Ergebnis der Überlagerung, um deren Gipfel herauszufinden, zu erhalten.

[0090] Insbesondere werden das Beobachtungsergebnis, das durch die Authentisierungsvorrichtung **131** erhalten wurde, und das Beobachtungsergebnis, das durch die Authentisierungszielvorrichtung **151** erhalten wurde, mit einer Zeitdifferenz zwischen ihnen verschoben, und man erhält die Korrelation zwischen ihnen. Dann wird eine zweidimensionale schnelle Fouriertransformation in Richtung der Verzögerungszeitachse und in Richtung der Verzögerungszeitverhältnisachse auf die Korrelation zwischen diesen, die bei jeder Zeitdifferenz erhalten wird, angewandt.

[0091] Fig. 5 zeigt Ergebnisse der Berechnung der zweidimensionalen schnellen Fouriertransformation in der Richtung der Verzögerungszeit und der Richtung des Verzögerungszeitverhältnisses. In Fig. 5 stellt die Achse der "Δ Verzögerungszeit" die Verzögerungszeitachse dar, und die Achse der "Δ Interferenzfrequenz (fringe frequency)" stellt die Verzögerungszeitverhältnisachse dar.

[0092] Wie in Fig. 6 gezeigt ist, schneiden sich eine gemeinsame Wellenfrontverzögerungslinie **303**, die die Schnittlinie einer Wellenfront und der Oberfläche der Erde, die der erhaltenden Verzögerung entspricht, darstellt, und eine gemeinsame Verzögerungszeitverhältnislinie **304**, die die Schnittlinie einer Wellenfront und der Oberfläche der Erde, die dem erhaltenen Verzögerungszeitverhältnis entspricht, darstellt, einander an den Punkten **305**. Solche Schnittpunkte **305** können als die Positionen der Authentisierungszielvorrichtung **151** auf der Oberfläche der Erde bestimmt werden. Ein solches Verfahren der Schätzung der Position der Authentisierungszielvorrichtung **151** wird als "Wellenfrontsynchronisationsverfahren" bezeichnet.

[0093] Im allgemeinen weisen die Linien zwei Schnittpunkte **305** auf. Somit sollte unter Bezug auf die Position der Authentisierungszielvorrichtung **151**, die in der Speichereinheit **135** der Authentisierungsvorrichtung **131** gespeichert ist, die Position, die durch einen Schnittpunkt **305** angezeigt wird, der sich

entfernter von der gespeicherten Position befindet, ignoriert werden, und die Position, die durch den anderen Schnittpunkt **305** angezeigt wird, der sich näher an der gespeicherten Position befindet, sollte als das Schätzergebnis verwendet werden.

[0094] Wenn die Position des Schnittpunkts **305**, die in obiger Weise erhalten wird, der Position der Authentisierungsvorrichtung **151**, die in der Speichereinheit **135** gespeichert ist, innerhalb eines vorbestimmten Fehlerbereichs entspricht, so kann die Radiowelleninformation, die von der Authentisierungszielvorrichtung **151** gesendet wird, authentisiert werden, als erhalten von einer Beobachtung, die zur bezeichneten Beobachtungszeit an der Position, an der die Authentisierungszielvorrichtung **151** existiert, gemacht wurde.

[0095] In der obigen Erläuterung wurde angenommen, dass es nur einen Radiostern gibt. Wenn jedoch eine Vielzahl von Radiosternen verwendet werden, kann die Position der Authentisierungszielvorrichtung **151** genauer und präziser geschätzt werden.

[0096] In einem Fall, bei dem nur eine diskrete Radioquelle, wie ein Quasar verwendet wird, ist es möglich, eine Radiowellenbeobachtungsinformation, die so scheint, als wäre sie an der richtigen Position der Authentisierungszielvorrichtung **151** erhalten worden, unter Verwendung der Radiowellenbeobachtungsinformation, die an einer andere Position erhalten wurde, zu fälschen, indem Information über einen Radiostern und eine Beobachtungszeit im vorhinein erhalten wird, und die Referenzuhr mit großen Geschick manipuliert wird. Somit kann ein "Vortäuschen" nicht vollständig verhindert werden.

[0097] Durch die Verwendung einer Maserradioquelle, die eine komplizierte Struktur aufweist (wie eine Doppelaugenstruktur) oder durch die Verwendung einer Vielzahl von Radiosternen, die dicht beieinander in der Himmelsphäre existieren, kann einer solchen "Vortäuschung" entgegengewirkt werden. In einem Fall, bei dem es eine Vielzahl von Radioquellen in derselben Richtung gibt, wenn man vom Zentrum der Erde **302** aus schaut, ist es im Gegensatz zum Fall einer diskreten Radioquelle, wenn nur eine Radioquelle vorhanden ist, sogar durch das Manipulieren der Referenzuhr unmöglich, die Phasenverschiebung zu fälschen. Somit ist es unter Verwendung einer Radiowellenbeobachtungsposition, die an einer anderen Position erhalten wurde, unmöglich, eine Radiowellenbeobachtungsinformation zu fälschen, so dass sie scheinbar an der Position der Authentisierungszielvorrichtung **151** erhalten wurde.

[0098] Gemäß der vorliegenden Ausführungsform kann eine im Vergleich zur konventionellen Technik sichere Raum-Zeit-Koordinatenauthorisierungstechnik verwirklicht werden.

Andere Ausführungsform

[0099] In der oben beschriebenen Ausführungsform gibt die Authentisierungsvorrichtung **131** eine Bezeichnung einer Beobachtungszeit und eines Radiosterns an die Authentisierungszielvorrichtung **151**. Im Gegensatz dazu kann die Authentisierungszielvorrichtung **151** eine Bezeichnung einer Beobachtungszeit und eines Radiosterns an die Authentisierungsvorrichtung **131** geben. In diesem Fall sollte die Vorbereitungssendeeinheit **137** in der Authentisierungszielvorrichtung **151** installiert werden, und die Vorbereitungsempfangseinheit **154** sollte in der Authentisierungsvorrichtung **131** installiert werden.

[0100] Im Gegensatz zu obigem kann eine Ausführungsform, bei der die Authentisierungsvorrichtung **131** einen Radiostern bezeichnet, und bei der die Authentisierungszielvorrichtung **151** eine Beobachtungszeit bezeichnet, und eine dazu umgekehrte Ausführungsform verwendbar sein.

Andere Ausführungsform

[0101] Fig. 7 ist ein beispielhaftes Diagramm, das eine schematische Struktur eines Authentisierungssystems gemäß einer anderen Ausführungsform der vorliegenden Erfindung zeigt. Die folgende Erläuterung erfolgt unter Bezug auf dieses Diagramm. Die vorliegenden Ausführungsform wird erläutern, wie die Datenkommunikation unter Verwendung einer Verschlüsselungstechnik durchzuführen ist, nachdem die Authentisierung erfolgreich im Authentisierungssystem der oben beschriebenen Ausführungsformen beendet wurde.

[0102] Die Authentisierungsvorrichtung **131** und die Authentisierungszielvorrichtung **151** des Authentisierungssystems **101** gemäß der vorliegenden Ausführungsform umfasst eine Verschlüsselungskommunikationseinheit **631** beziehungsweise eine Verschlüsselungskommunikationseinheit **651** zusätzlich zu den Elementen in den obigen Ausführungsformen.

[0103] Nachdem die Authentisierung zu einem Erfolg geführt hat, können die Verschlüsselungskommunikationseinheit **631** der Authentisierungsvorrichtung **131** und die Verschlüsselungskommunikationseinheit **651** der Authentisierungszielvorrichtung **151** eine Verschlüsselungskommunikation gemäß den nachfolgenden Verfahren durchführen.

(1) Erstes Verfahren

[0104] Die Authentisierungszielvorrichtung **151** umfasst Verschlüsselungsschlüsselinformation, die für die Verschlüsselungskommunikation zu verwenden ist, in der Informationsnachricht zusätzlich zur Information auf der beobachteten Radiowelle. Die Authentisierungsvorrichtung **131** und die Authentisie-

rungszielvorrichtung **151** führen eine Verschlüsselungskommunikation unter Verwendung dieses Verschlüsselungsschlüssels durch.

(2) Zweites Verfahren

[0105] Die Authentisierungsvorrichtung **131** und die Authentisierungszielvorrichtung **151** wählen zusammen im voraus einen gemeinsamen Schlüssel in geheimer Weise. Die Authentisierungsvorrichtung **131** und die Authentisierungszielvorrichtung **151** führen eine Verschlüsselungskommunikation unter Verwendung dieses gemeinsamen Verschlüsselungsschlüssels durch.

(3) Drittes Verfahren

[0106] In diesem Verfahren werden ein geheimer Schlüssel A, der der Authentisierungsvorrichtung **131** gehört, ein geheimer Schlüssel B, der der Authentisierungszielvorrichtung **151** gehört, und ein öffentlicher Schlüssel C, der gemäß einem bestimmten Verfahren erhalten wird, verwendet. Da beispielsweise die Radiowelleninformation, die man als Ergebnis der Beobachtung eines Radiosterns erhält, eine ausgezeichnete Eigenschaft als Zufallszahl aufweist, kann die Radiowelleninformation, die durch die Authentisierungsvorrichtung **151** aus der Beobachtung eines Radiosterns erhalten wird, als öffentlicher Schlüssel C verwendet werden.

[0107] Es wird nun eine Operation f, die die folgende Eigenschaft erfüllt, betrachtet.

$$f(B, f(A, C)) = f(A, f(B, C)) = Z$$

[0108] Eine solche Operation, die eine Kommutativität aufweist, ist auf dem Feld der Verteilungstechniken für einen öffentlichen Schlüssel weithin bekannt.

[0109] Die Authentisierungsvorrichtung **131** berechnet f(A, C) und sendet das an die Authentisierungszielvorrichtung **151**. Die Authentisierungszielvorrichtung **151** berechnet f(B, f(A, C)) = Z unter Verwendung der empfangenen f(A, C) und B, um somit einem gemeinsamen Schlüssel Z zu erhalten.

[0110] Andererseits berechnet die Authentisierungszielvorrichtung **151** f(B, C) und sendet das an die Authentisierungsvorrichtung **131**. Die Authentisierungsvorrichtung **131** berechnet f(A, f(B, C)) = Z unter Verwendung des empfangenen f(B, C) und A, um somit dem gemeinsamen Schlüssel Z zu erhalten.

[0111] Auf diese Weise können die Authentisierungsvorrichtung **131** und die Authentisierungszielvorrichtung **151** den gemeinsamen Schlüssel Z teilen. Somit kann bei der Verschlüsselungskommunikation, wenn eine zu übertragende Nachricht unter Verwendung des gemeinsamen Schlüssels Z verschlüsselt wird, sowohl die Authentisierungsvorrichtung **131** als auch die Authentisierungszielvorrichtung **151** die Nachricht entschlüsseln.

[0112] Als eine Operation f, die eine solche Eigenschaft aufweist, kann $f(x, y) = y^x \bmod p$(x, y und p sind positive ganze Zahlen) betrachtet werden.

[0113] Wie oben erläutert wurde, so ist es gemäß der vorliegenden Erfindung möglich, ein Authentisierungssystem, eine Authentisierungsvorrichtung, eine Authentisierungszielvorrichtung, ein Authentisierungsverfahren und ein Verfahren des Authentisiert-Werdens, die für das Authentisieren einer Authentisierungszielvorrichtung durch das Vergleichen einer Position der Authentisierungszielvorrichtung, die durch das Beobachten einer Radiowelle von einem gemeinsamen Radiostern zu einer gemeinsamen Beobachtungszeit geschätzt wird, mit der realen Position der Authentisierungszielvorrichtung geeignet ist, ein Programm um dies zu verwirklichen, und ein von einem Computer lesbares Informationsaufzeichnungsmedium für das Speichern dieses Programms bereit zu stellen.

[0114] Verschiedene Ausführungsformen und Änderungen können dabei vorgenommen werden, ohne vom breiten Wesen und dem Umfang der Erfindung abzuweichen. Die oben beschriebenen Ausführungsformen sollen die vorliegende Erfindung darstellen aber den Umfang der vorliegenden Erfindung nicht begrenzen. Der Umfang der vorliegenden Erfindung wird durch die angefügten Ansprüche statt durch die Ausführungsformen gezeigt. Verschiedene Modifikationen, die innerhalb der Bedeutung eines Äquivalents der Ansprüche der Erfindung und innerhalb der Ansprüche vorgenommen werden, sollen als im Umfang der vorliegenden Erfindung betrachtet werden.

Bezugszeichenliste

Fig. 1

132	Beobachtungseinheit
133	Informationsempfangseinheit
134	Schätzeinheit
135	Speichereinheit
136	Bestimmungseinheit

137	Vorbereitungssendeeinheit
152	Beobachtungseinheit
153	Informationssendeeinheit
154	Vorbereitungsempfangseinheit
AUTHENTICATION APPARATUS	Authentisierungsvorrichtung
AUTHENTICATION TARGET APPARATUS	Authentisierungszielvorrichtung
AUTHENTICATION RESULT	Authentisierungsergebnis

Fig. 2

PROCESS FOR AUTHENTICATION	Verfahren für die Authentisierung
PROCESS FOR BEING AUTHENTICATION	Verfahren zum Authentisiert-Werden
S201	Sende Vorbereitungsnachricht
S202	Empfange Vorbereitungsnachricht
S203	Beobachte Radiostern
S204	Beobachte Radiostern
S205	Sende Informationsnachricht
S206	Empfange Informationsnachricht
S207	Schätze Position der Authentisierungszielvorrichtung
S208	Positionen entsprechen einander ?
S209	Lege Authentisierung als Erfolg fest
S210	Benachrichtige über Erfolg
S211	Empfange Benachrichtigung
S212	Lege Authentisierung als misslungen fest

Fig. 3

ROTATION	Rotation
RADIO STAR	Radiostern
EARTH	Erde

Fig. 4

ROTATION	Rotation
RADIO STAR	Radiostern
EARTH	Erde

Fig. 5

CORRELATION STRENGTH	Korrelationsstärke
FRINGE FREQUENCY	Interferenzfrequenz
DELAY TIME	Verzögerungszeit

Fig. 6

ROTATION	Rotation
EARTH	Erde

Fig. 7

132	Beobachtungseinheit
133	Informationsempfangseinheit
134	Schätzeinheit
135	Speichereinheit
136	Bestimmungseinheit
137	Vorbereitungssendeeinheit
152	Beobachtungseinheit
153	Informationssendeeinheit
154	Vorbereitungsempfangseinheit
AUTHENTICATION APPARATUS	Authentisierungsvorrichtung
AUTHENTICATION TARGET APPARATUS	Authentisierungszielvorrichtung
AUTHENTICATION RESULT	Authentisierungsergebnis
631	Verschlüsselungskommunikationseinheit
651	Verschlüsselungskommunikationseinheit

Patentansprüche

1. Authentisierungssystem (**101**), das eine Authentisierungsvorrichtung (**131**) und eine Authentisierungszielvorrichtung (**151**) umfasst, wobei beide eine Radiowelle von einem gemeinsamen Radiostern zu einer gemeinsamen Beobachtungszeit beobachten, wobei

(a) die Authentisierungsvorrichtung (**131**) eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet;

(b) die Authentisierungszielvorrichtung (**151**) eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet und eine Informationsnachricht, die eine Information über die beobachtete Radiowelle enthält, an die Authentisierungsvorrichtung sendet; und

(c) die Authentisierungsvorrichtung (**131**) die Informationsnachricht, die von der Authentisierungszielvorrichtung (**151**) gesendet wird, empfängt,

eine Position der Authentisierungszielvorrichtung (**151**) in Bezug auf die Authentisierungsvorrichtung auf der Basis der "Information der Radiowelle, die

durch die Authentisierungsvorrichtung (**151**) beobachtet wurde, die in der empfangenen Informationsnachricht enthalten ist" und "einer Information der Radiowelle, die von der Authentisierungsvorrichtung (**131**) beobachtet wurde", schätzt, und
die Authentisierung für die Informationsnachricht in einem Fall, bei dem eine Position der Authentisierungszielvorrichtung (**151**), die in der Authentisierungsvorrichtung (**131**) im Vorhinein gespeichert wurde, und die geschätzte Position der Authentisierungszielvorrichtung (**151**) einander innerhalb eines vorbestimmten Fehlerbereichs entsprechen, als Erfolg festlegt.

2. Authentisierungssystem (**101**) nach Anspruch 1, wobei "die gemeinsame Beobachtungszeit und/oder der gemeinsamen Radiostern" durch eine Vorbereitungsnachricht, die von der Authentisierungsvorrichtung (**131**) an die Authentisierungszielvorrichtung (**151**) im Vorhinein zu senden ist, bezeichnet werden.

3. Authentisierungssystem (**101**) nach Anspruch 1, wobei "die gemeinsame Beobachtungszeit und/oder der gemeinsame Radiostern" durch eine Vorbereitungsnachricht, die von der Authentisierungszielvorrichtung (**151**) an die Authentisierungsvorrichtung (**131**) im Vorhinein zu senden ist, bezeichnet werden.

4. Authentisierungssystem (**101**) nach Anspruch 1, wobei die Anzahl der gemeinsamen Radiosterne gleich oder größer als 2 ist.

5. Authentisierungssystem (**101**) nach Anspruch 1, wobei der gemeinsame Radiostern eine Maserradioquelle (die eine Wassermaserradioquelle, eine Ammoniakmaserradioquelle und eine Methanolmaserradioquelle einschließt) oder ein Quasar ist.

6. Authentisierungssystem (**101**) nach Anspruch 1, wobei in einem Fall, bei dem die Authentisierung für die Informationsnachricht als ein Erfolg festgelegt wird, die Authentisierungsvorrichtung (**131**) und die Authentisierungszielvorrichtung (**151**) eine Verschlüsselungskommunikation unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet ist, durchführen.

7. Authentisierungssystem (**101**) nach Anspruch 1, wobei in einem Fall, bei dem die Authentisierung für die Informationsnachricht als ein Erfolg festgelegt wird, die Authentisierungsvorrichtung (**131**) und die Authentisierungszielvorrichtung (**151**) eine Verschlüsselungskommunikation unter Verwendung eines gemeinsamen Schlüssels, der im Vorhinein in Verbindung mit der Authentisierungsvorrichtung (**131**) und der Authentisierungszielvorrichtung (**151**) ausgewählt wird, durchführen.

8. Authentisierungssystem (**101**) nach Anspruch 1, wobei in einem Fall, bei dem die Authentisierung für die Informationsnachricht als ein Erfolg festgelegt wird, die Authentisierungsvorrichtung (**131**) und die Authentisierungszielvorrichtung (**151**) eine Verschlüsselungskommunikation unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der zwischen ihnen geteilt wird, einem geheimen Schlüssel, der der Authentisierungsvorrichtung (**131**) zugehört, und einem geheimem Schlüssel, der der Authentisierungszielvorrichtung (**151**) zugehört, erzeugt wird, durchführen.

9. Authentisierungssystem (**101**) nach Anspruch 8, wobei der öffentliche Schlüssel, der zwischen der Authentisierungsvorrichtung (**131**) und der Authentisierungszielvorrichtung (**151**) geteilt wird, aus "Information einer Radiowelle, die durch die Authentisierungszielvorrichtung (**151**) beobachtet wird", erzeugt wird.

10. Authentisierungsvorrichtung (**131**), die eine Radiowelle von einem Radiostern, den sie mit einer Authentisierungszielvorrichtung (**151**) gemeinsam hat, zu einer Beobachtungszeit, die sie mit der Authentisierungszielvorrichtung (**151**) gemeinsam hat, beobachtet, umfassend:
eine Beobachtungseinheit (**132**), die eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet;
eine Informationsempfangseinheit (**133**), die eine Informationsnachricht, die von der Authentisierungszielvorrichtung (**151**) gesendet wird, empfängt;
eine Schätzeinheit (**134**), die eine Position der Authentisierungszielvorrichtung (**151**) in Bezug auf die Authentisierungsvorrichtung (**131**) auf der Basis einer "Information einer Radiowelle, die durch die Authentisierungszielvorrichtung (**151**) beobachtet wird, die in der empfangenen Informationsnachricht eingeschlossen ist" und "einer Information der Radiowelle, die durch die Beobachtungseinheit (**132**) beobachtet wird" schätzt;
eine Speichereinheit (**135**), die die Position(en) einer oder mehrerer Authentisierungszielvorrichtung(en) (**151**) im Voraus speichert; und
eine Bestimmungseinheit (**136**), die die Authentisierung für die Informationsnachricht als einen Erfolg festlegt, wenn eine Position der Authentisierungszielvorrichtung (**151**), die in der Speichereinheit (**135**) im Vorhinein gespeichert wurde, und die geschätzte Position der Authentisierungszieleinheit (**151**) einander innerhalb eines vorbestimmten Fehlerbereichs entsprechen.

11. Authentisierungsvorrichtung (**131**) nach Anspruch 10, wobei sie weiter eine Vorbereitungssendeeinheit (**137**), die eine Vorbereitungsnachricht für das Bezeichnen "der gemeinsamen Beobachtungszeit und/oder des gemeinsamen Radiosterns" an die Authentisierungszielvorrichtung (**151**) im Voraus sen-

det, umfasst.

12. Authentisierungsvorrichtung (**131**) nach Anspruch 10, wobei sie weiter eine Vorbereitungsempfangseinheit (**137**), die eine Vorbereitungsnachricht für das Bestimmen "einer Beobachtungszeit und/oder eines Radiosterns" umfasst,
wobei die Beobachtungseinheit (**132**) eine Radiowelle beobachtet in einem Fall, bei dem die empfangene Vorbereitungsnachricht eine Beobachtungszeit bezeichnet, durch das Betrachten der bezeichneten Beobachtungszeit als gemeinsame Beobachtungszeit, und in einem Fall, bei dem die empfangene Vorbereitungsnachricht einen Radiostern bezeichnet, durch das Betrachten des bezeichneten Radiosterns als gemeinsamen Radiostern.

13. Authentisierungsvorrichtung (**131**) gemäß Anspruch 10, wobei sie weiter eine Verschlüsselungskommunikationseinheit (**631**), die eine Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung (**151**) unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet ist, in einem Fall durchführt, bei dem die Bestimmungseinheit die Authentisierung der Informationsnachricht als Erfolg festlegt.

14. Authentisierungsvorrichtung (**131**) gemäß Anspruch 10, wobei sie weiter eine Verschlüsselungskommunikationseinheit (**631**), die eine Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung (**151**) unter Verwendung eines gemeinsamen Schlüssels, der im Voraus in Verbindung mit der Authentisierungszielvorrichtung (**151**) ausgewählt wird, in einem Fall durchführt, bei dem die Authentisierung der Informationsnachricht als Erfolg festlegt wird.

15. Authentisierungsvorrichtung (**131**) gemäß Anspruch 10, wobei sie weiter eine Verschlüsselungskommunikationseinheit (**631**), die eine Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung (**151**) unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der mit der Authentisierungszielvorrichtung (**151**) geteilt wird, einem geheimen Schlüssel, der der Authentisierungsvorrichtung (**131**) zugehört, und einem geheimen Schlüssel, der der Authentisierungszielvorrichtung (**151**) zugehört, erzeugt wird, durchführt.

16. Authentisierungsvorrichtung (**131**) nach Anspruch 15, wobei sie weiter eine Erzeugungseinheit für den öffentlichen Schlüssel umfasst, der den öffentlichen Schlüssel, der mit der Authentisierungszielvorrichtung geteilt wird, aus der "Information der Radiowelle, die durch die Authentisierungszielvorrichtung beobachtet wird" erzeugt.

17. Authentisierungszielvorrichtung (**151**), die eine Radiowelle von einem Radiostern, der einer Authentisierungsvorrichtung (**131**) gemeinsam ist, zu einer Beobachtungszeit, die der Authentisierungsvorrichtung (**131**) gemeinsam ist, beobachtet, umfassend:
eine Beobachtungseinheit (**152**), die eine Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit beobachtet; und
eine Sendeeinheit (**53**), die eine Informationsnachricht, die Information über die beobachtete Radiowelle enthält, an die Authentisierungsvorrichtung (**131**) sendet.

18. Authentisierungszielvorrichtung (**151**) gemäß Anspruch 17, wobei sie weiter eine Vorbereitungssendeeinheit (**154**), die eine Vorbereitungsnachricht für das Bezeichnen der "gemeinsamen Beobachtungszeit und/oder des gemeinsamen Radiosterns" an die Authentisierungsvorrichtung (**131**) im Voraus sendet.

19. Authentisierungszielvorrichtung (**151**) gemäß Anspruch 17, wobei sie weiter eine Vorbereitungsempfangseinheit (**154**), die eine Vorbereitungsnachricht für das Bezeichnen "einer Beobachtungszeit und/oder eines Radiosterns" empfängt, umfasst,
wobei die Beobachtungseinheit (**152**) eine Radiowelle in einem Fall betrachtet, bei dem die empfangene Vorbereitungsnachricht eine Beobachtungszeit bezeichnet, durch das Betrachten der bezeichneten Beobachtungszeit als gemeinsame Beobachtungszeit, und in einem Fall, bei dem die empfangene Vorbereitungsnachricht einen Radiostern bezeichnet, indem sie den bezeichneten Radiostern als den gemeinsamen Radiostern betrachtet.

20. Authentisierungszielvorrichtung (**151**) gemäß Anspruch 17, wobei sie weiter eine Verschlüsselungskommunikationseinheit (**651**), die eine Verschlüsselungskommunikation mit der Authentisierungsvorrichtung (**131**) unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet wird, in einem Fall durchführt, bei dem die Authentisierungsvorrichtung (**131**) eine Authentisierung für die Informationsnachricht als ein Erfolg festlegt.

21. Authentisierungszielvorrichtung (**151**) gemäß Anspruch 17, wobei sie weiter eine Verschlüsselungskommunikationseinheit (**651**), die eine Verschlüsselungskommunikation mit der Authentisierungsvorrichtung (**131**) unter Verwendung eines gemeinsamen Schlüssels, der im Voraus in Verbindung mit der Authentisierungsvorrichtung (**131**) ausgewählt wird, in einem Fall durchführt, bei dem die Authentisierungsvorrichtung (**131**) eine Authentisierung für die Informationsnachricht als Erfolg festlegt.

22. Authentisierungszielvorrichtung (**151**) gemäß Anspruch 17, wobei sie weiter eine Verschlüsse-

lungskommunikationseinheit (**651**), die eine Verschlüsselungskommunikation mit der Authentisierungsvorrichtung (**131**) unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der mit der Authentisierungsvorrichtung (**131**) geteilt wird, einem geheimen Schlüssel, der der Authentisierungsvorrichtung (**131**) zugehört und einem geheimen Schlüssel, der der Authentisierungszielvorrichtung (**151**) zugehört, erzeugt wird, in einem Fall durchführt, bei dem die Authentisierung für die Informationsnachricht als Erfolg festgelegt wird.

23. Authentisierungszielvorrichtung (**151**) gemäß Anspruch 22, wobei sie weiter einer Erzeugungseinheit für einen öffentlichen Schlüssel umfasst, die den öffentlichen Schlüssel, der mit der Authentisierungsvorrichtung (**131**) geteilt wird, aus "einer Information einer Radiowelle, die durch die Beobachtungseinheit (**152**) beobachtet wird", erzeugt.

24. Authentisierungsverfahren für das Beobachten einer Radiowelle von einem Radiostern, die einer Authentisierungsvorrichtung und einer Authentisierungszielvorrichtung gemeinsam ist, zu einer Beobachtungszeit, die der Authentisierungsvorrichtung und der Authentisierungszielvorrichtung gemeinsam ist, umfassend:
einen Beobachtungsschritt der Beobachtung einer Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit;
einen Informationsempfangsschritt des Empfangens einer Informationsnachricht, die von der Authentisierungszielvorrichtung gesendet wird;
einen Schätzschritt des Schätzens einer Position der Authentisierungszielvorrichtung auf der Basis einer "Information einer Radiowelle, die durch die Authentisierungszielvorrichtung beobachtet wird, die in der empfangenen Informationsnachricht enthalten ist" und "einer Information der Radiowelle, die im Beobachtungsschritt beobachtet wird"; und
einen Bestimmungsschritt für das Festlegen einer Authentisierung für die Informationsnachricht als ein Erfolg in einem Fall, bei dem eine Position der Authentisierungszielvorrichtung, die im Vorhinein gespeichert wurde, und die geschätzte Position der Authentisierungszielvorrichtung innerhalb eines vorbestimmten Fehlerbereichs einander entsprechen.

25. Authentisierungsverfahren nach Anspruch 24, wobei es weiter einen Vorbereitungssendeschritt des Sendens einer Vorbereitungsnachricht für das Bezeichnen der "gemeinsamen Beobachtungszeit und/oder des gemeinsamen Radiosterns" an die Authentisierungszielvorrichtung im Voraus umfasst.

26. Authentisierungsverfahren nach Anspruch 24, wobei es weiter einen Vorbereitungsempfangsschritt für das Empfangen einer Vorbereitungsnachricht für das Bezeichnen "einer Beobachtungszeit und/oder eines Radiosterns" umfasst,
wobei im Beobachtungsschritt eine Radiowelle in einem Fall beobachtet wird, bei dem die empfangene Vorbereitungsnachricht eine Beobachtungszeit bezeichnet, indem die bezeichnete Beobachtungszeit als gemeinsame Beobachtungszeit betrachtet wird, und einem Fall, bei dem die empfangene Vorbereitungsnachricht einen Radiostern bezeichnet, durch das Betrachten des bezeichneten Radiosterns als gemeinsamen Radiostern.

27. Authentisierungsverfahren nach Anspruch 24, wobei es weiter einen Verschlüsselungskommunikationsdurchführungsschritt für das Durchführen einer Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet wird, in einem Fall, bei dem die Authentisierung für die Informationsnachricht als Erfolg festgesetzt wird, umfasst.

28. Authentisierungsverfahren nach Anspruch 24, wobei es weiter einen Verschlüsselungskommunikationsdurchführungsschritt für das Durchführen einer Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der im Vorhinein in Verbindung mit der Authentisierungszielvorrichtung ausgewählt wird, in einem Fall, bei dem die Authentisierung für die Informationsnachricht als Erfolg festgesetzt wird, umfasst.

29. Authentisierungsverfahren nach Anspruch 24, wobei es weiter einen Verschlüsselungskommunikationsdurchführungsschritt für das Durchführen einer Verschlüsselungskommunikation mit der Authentisierungszielvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der mit der Authentisierungszielvorrichtung geteilt wird, einem vorbestimmten geheimen Schlüssel, und einem geheimen Schlüssel, der der Authentisierungszielvorrichtung zugehört, erzeugt wird, in einem Fall, bei dem die Authentisierung für die Informationsnachricht als Erfolg festgesetzt wird, umfasst.

30. Authentisierungsverfahren nach Anspruch 29, wobei es weiter einen Erzeugungsschritt des öffentlichen Schlüssels für das Erzeugen des öffentlichen Schlüssels, der mit der Authentisierungszielvorrichtung geteilt wird, aus "der Information einer Radiowelle, die durch die Authentisierungszielvorrichtung beobachtet wird" umfasst.

31. Verfahren zum Authentisiert-Werden, bei dem eine Radiowelle von einem Radiostern beobachtet wird, die einer Authentisierungsvorrichtung und einer Authentisierungszielvorrichtung gemeinsam ist, zu einer Beobachtungszeit, die der Authentisierungsvorrichtung und der Authentisierungszielvorrichtung gemeinsam ist, umfassend:

einen Beobachtungsschritt der Beobachtung einer Radiowelle vom gemeinsamen Radiostern zur gemeinsamen Beobachtungszeit; und
einen Sendeschritt des Sendens einer Informationsnachricht, die Information über die beobachtete Welle einschließt, an die Authentisierungsvorrichtung.

32. Verfahren zum Authentisiert-Werden nach Anspruch 31, wobei es weiter einen Vorbereitungssendeschritt des Sendens einer Vorbereitungsnachricht für das Bezeichnen der "gemeinsamen Beobachtungszeit und/oder des gemeinsamen Radiosterns" an die Authentisierungsvorrichtung im Vorhinein umfasst.

33. Verfahren zum Authentisiert-Werden nach Anspruch 31, wobei es weiter einen Vorbereitungsempfangsschritt des Empfangens einer Vorbereitungsnachricht für das Bezeichnen "einer Beobachtungszeit und/oder eines Radiosterns" umfasst,
wobei im Beobachtungsschritt eine Radiowelle in einem Fall beobachtet wird, bei dem die empfangene Vorbereitungsnachricht eine Beobachtungszeit bezeichnet, durch das Betrachten der bezeichneten Beobachtungszeit als gemeinsame Beobachtungszeit, und in einem Fall, bei dem die empfangene Vorbereitungsnachricht einen Radiostern bezeichnet, durch das Betrachten des bezeichneten Radiosterns als gemeinsamen Radiostern.

34. Verfahren zum Authentisiert-Werden nach Anspruch 31, wobei es weiter einen Verschlüsselungskommunikationsdurchführungsschritt für das Durchführen der Verschlüsselungskommunikation mit der Authentisierungsvorrichtung unter Verwendung eines Verschlüsselungsschlüssels, der in der Informationsnachricht bezeichnet ist, in einem Fall, bei dem die Authentisierungsvorrichtung die Authentisierung für die Informationsnachricht als Erfolg festlegt, umfasst.

35. Verfahren zum Authentisiert-Werden nach Anspruch 31, wobei es weiter einen Verschlüsselungskommunikationsdurchführungsschritt für das Durchführen der Verschlüsselungskommunikation mit der Authentisierungsvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der im Vorhinein in Verbindung mit der Authentisierungsvorrichtung ausgewählt wurde, in einem Fall, bei dem die Authentisierungsvorrichtung die Authentisierung für die Informationsnachricht als Erfolg festlegt, umfasst.

36. Verfahren zum Authentisiert-Werden nach Anspruch 31, wobei es weiter einen Verschlüsselungskommunikationsdurchführungsschritt für das Durchführen der Verschlüsselungskommunikation mit der Authentisierungsvorrichtung unter Verwendung eines gemeinsamen Schlüssels, der aus einem öffentlichen Schlüssel, der mit der Authentisierungsvorrichtung geteilt wird, einem geheimen Schlüssel, der der Authentisierungsvorrichtung zugehört, und einem vorbestimmten geheimen Schlüssel erzeugt wird, in einem Fall, bei dem die Authentisierung für die Informationsnachricht als Erfolg festgelegt wird, umfasst.

37. Verfahren zum Authentisiert-Werden nach Anspruch 36, wobei es weiter einen Erzeugungsschritt für einen öffentlichen Schlüssel für das Erzeugen des öffentlichen Schlüssels, der mit der Authentisierungsvorrichtung geteilt wird, aus der "Information der Radiowelle, die im Beobachtungsschritt beobachtet wurde" umfasst.

38. Programmprodukt für das Steuern eines Computers, um als die Authentisierungsvorrichtung, die in Anspruch 10 angegeben wurde, zu dienen.

39. Programmprodukt für das Steuern eines Computers, um als die Authentisierungszielvorrichtung, die in Anspruch 17 angegeben wurde, zu dienen.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

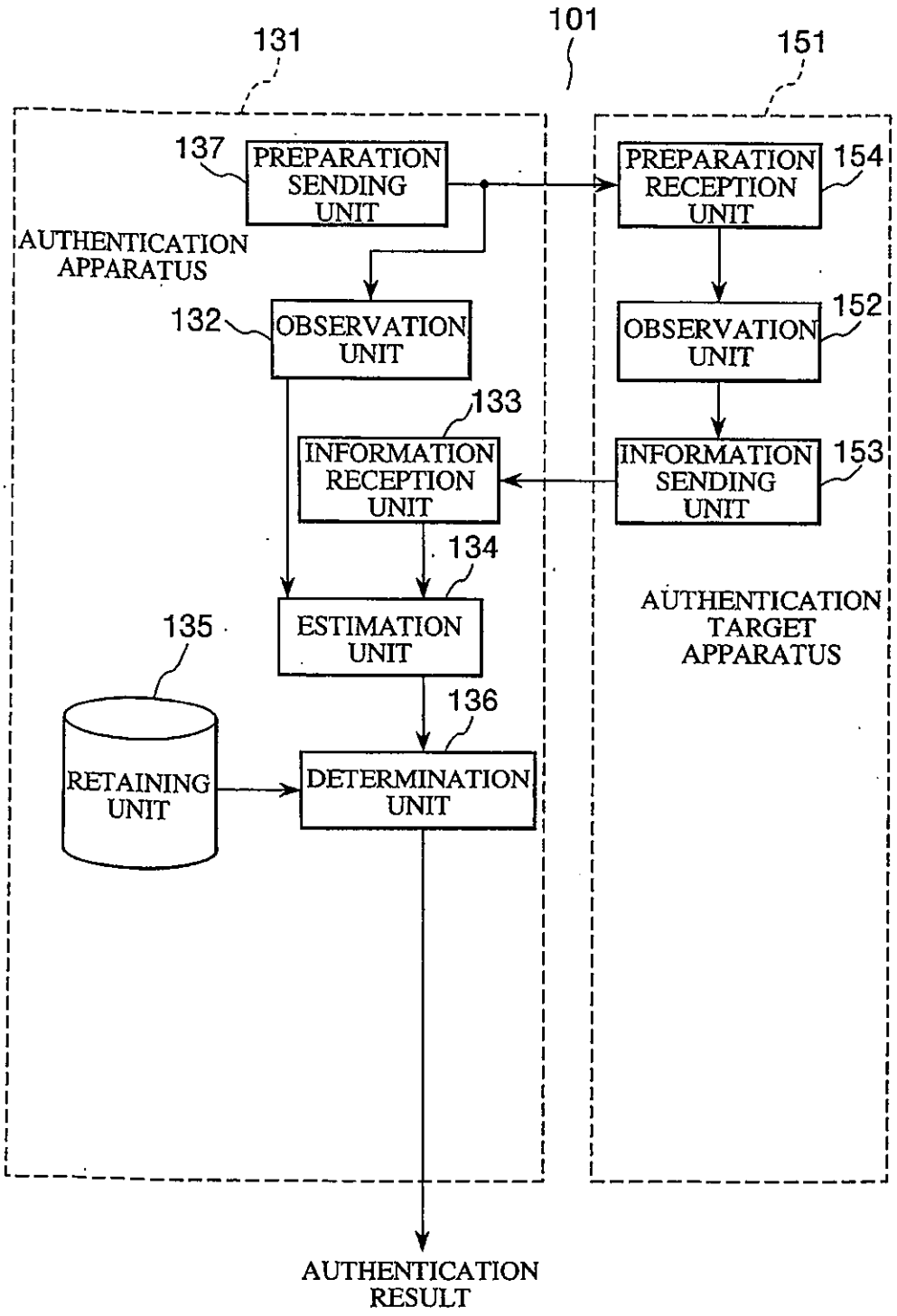


FIG.1

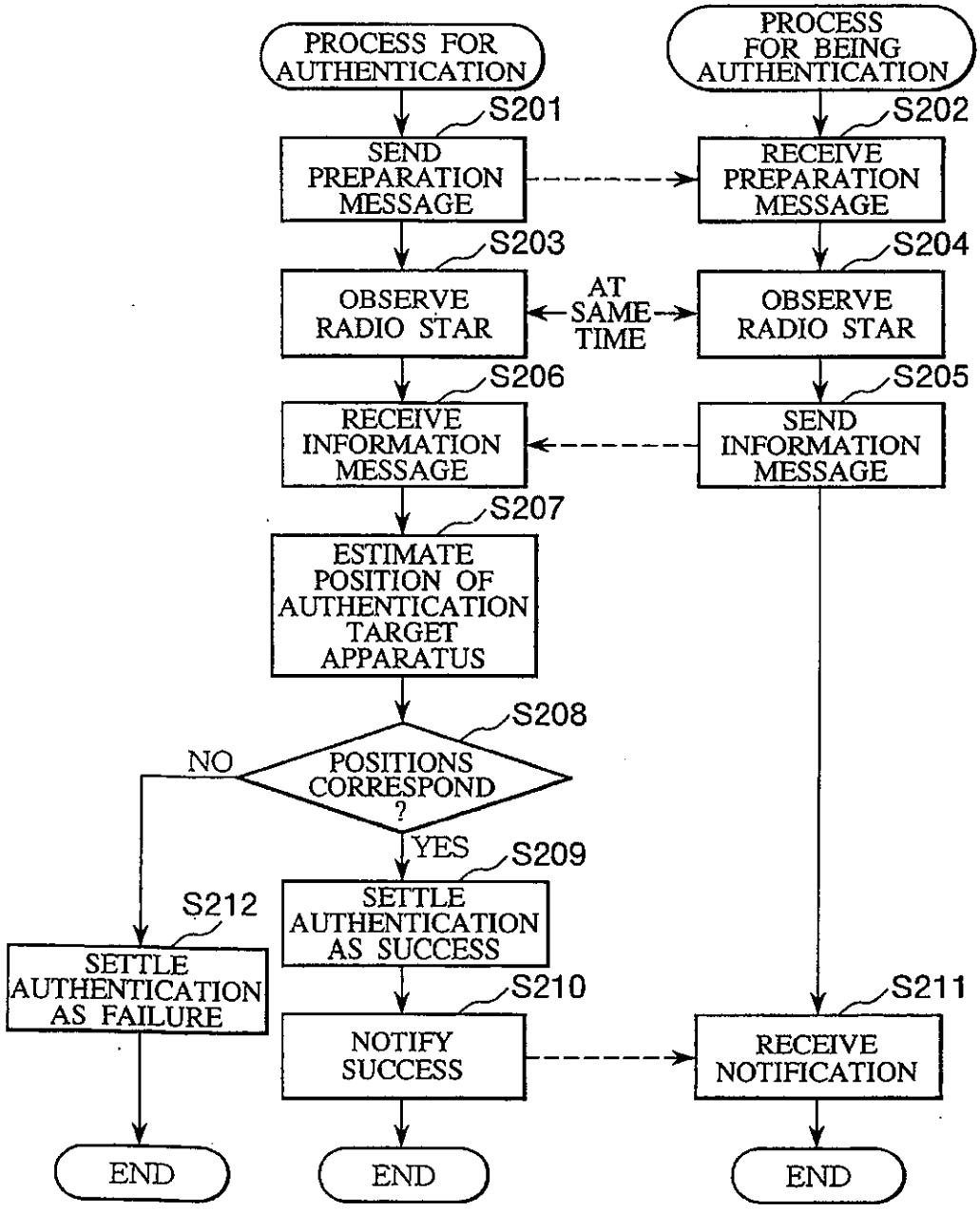

PROCESS FOR AUTHENTICATION
PROCESS FOR BEING AUTHENTICATION
S201
S202
SEND PREPARATION MESSAGE
RECEIVE PREPARATION MESSAGE
S203
S204
OBSERVE RADIO STAR
AT SAME TIME
OBSERVE RADIO STAR
S206
S205
RECEIVE INFORMATION MESSAGE
SEND INFORMATION MESSAGE
S207
ESTIMATE POSITION OF AUTHENTICATION TARGET APPARATUS
S208
NO
POSITIONS CORRESPOND ?
YES
S209
S212
SETTLE AUTHENTICATION AS SUCCESS
SETTLE AUTHENTICATION AS FAILURE
S210
S211
NOTIFY SUCCESS
RECEIVE NOTIFICATION
END
END
END

FIG.2

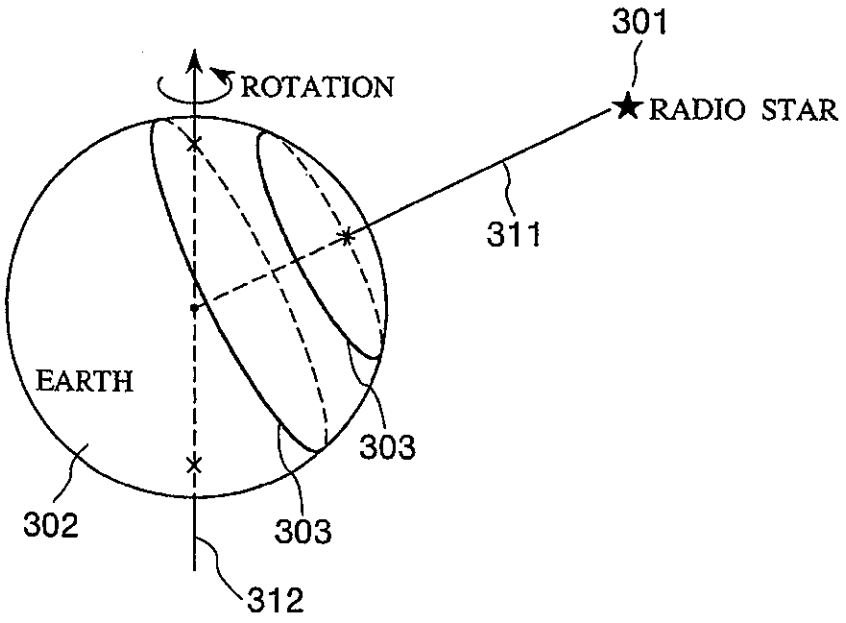

301
ROTATION
RADIO STAR
311
EARTH
303
302
303
312

FIG.3

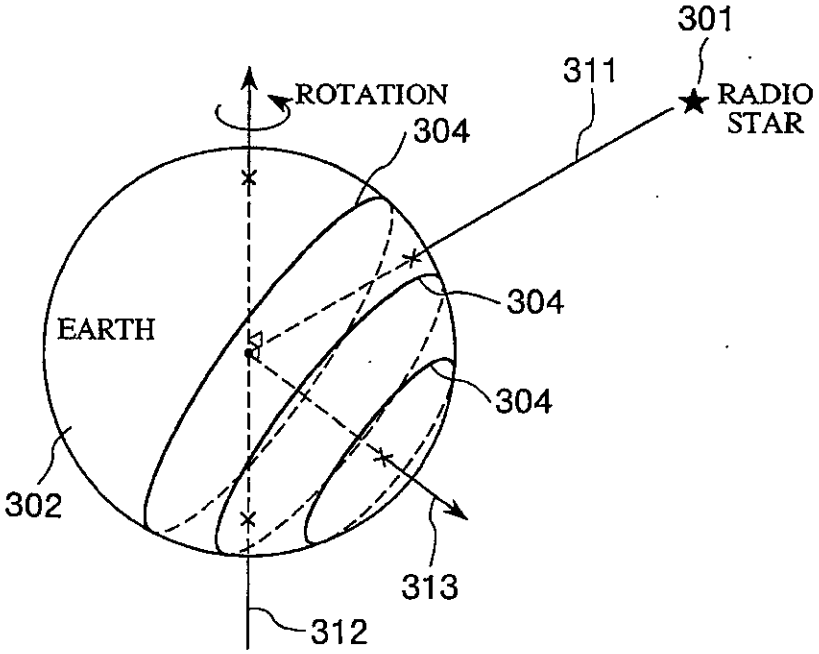

301
311
ROTATION
RADIO
STAR
304
304
EARTH
304
302
313
312

FIG.4

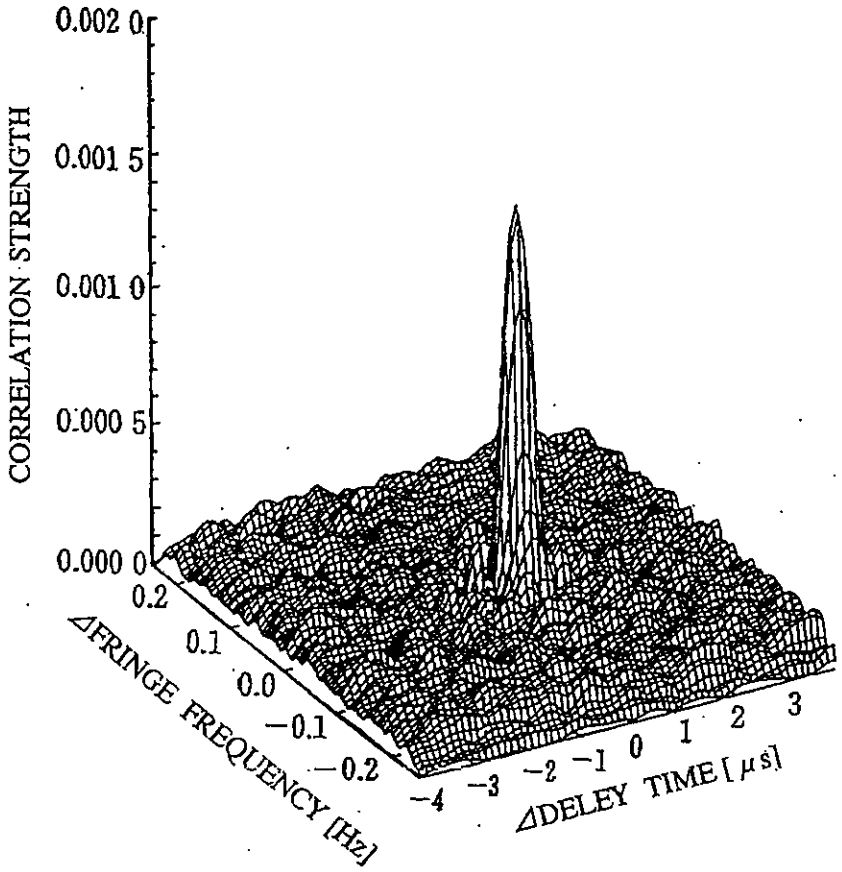

CORRELATION STRENGTH
0.002 0
0.001 5
0.001 0
0.000 5
0.000 0
0.2
0.1
0.0
−0.1
−0.2
ΔFRINGE FREQUENCY [Hz]
−4
−3
−2
−1
0
1
2
3
ΔDELEY TIME [μs]

FIG.5

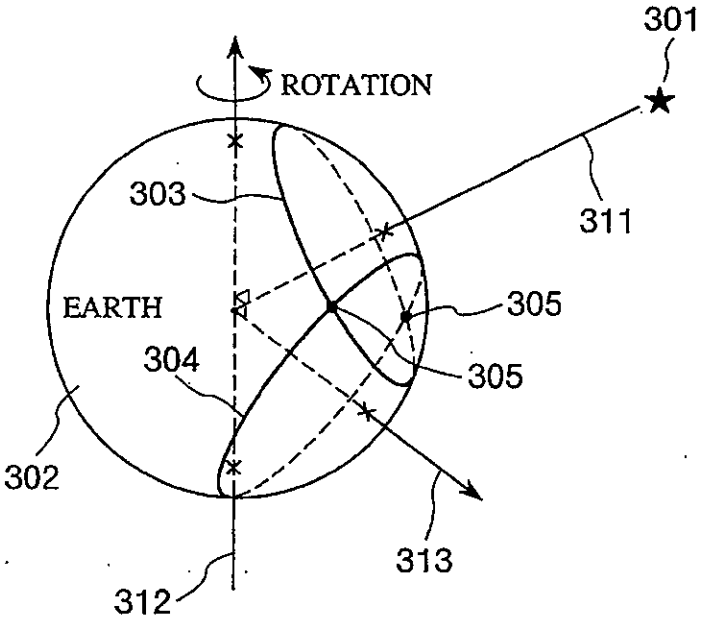

301
ROTATION
303
311
EARTH
305
304
305
302
313
312

FIG.6

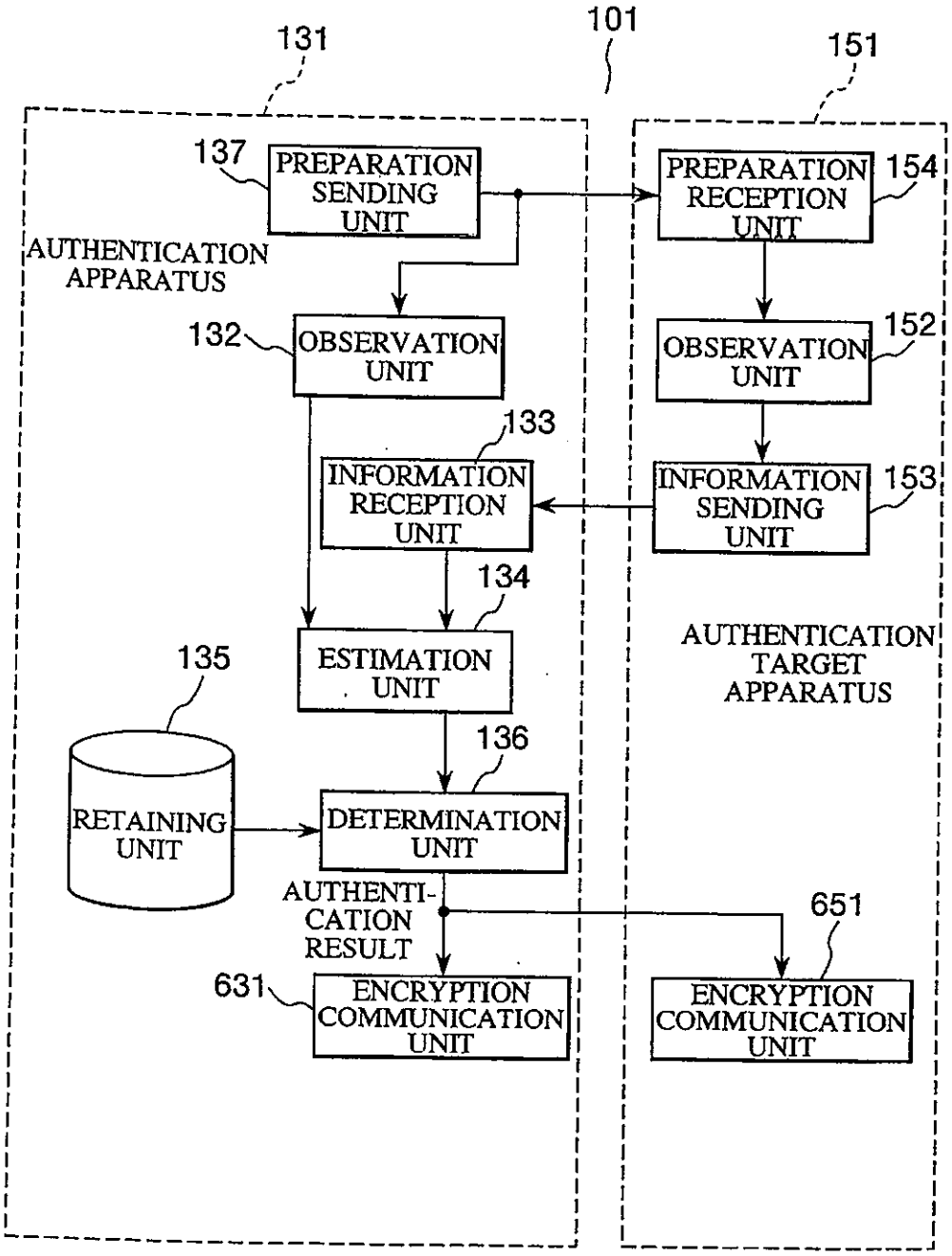

131
101
151
137
PREPARATION SENDING UNIT
AUTHENTICATION APPARATUS
PREPARATION RECEPTION UNIT
154
132
OBSERVATION UNIT
OBSERVATION UNIT
152
133
INFORMATION RECEPTION UNIT
INFORMATION SENDING UNIT
153
134
ESTIMATION UNIT
AUTHENTICATION TARGET APPARATUS
135
RETAINING UNIT
136
DETERMINATION UNIT
AUTHENTI-CATION RESULT
651
631
ENCRYPTION COMMUNICATION UNIT
ENCRYPTION COMMUNICATION UNIT

FIG.7