(19) Deutsches Patent- und Markenamt

(10) **DE 11 2021 007 337 B4** 2025.04.24

(12) # Patentschrift

(21) Deutsches Aktenzeichen: **11 2021 007 337.0**
(86) PCT-Aktenzeichen: **PCT/JP2021/018664**
(87) PCT-Veröffentlichungs-Nr.: **WO 2022/244079**
(86) PCT-Anmeldetag: **17.05.2021**
(87) PCT-Veröffentlichungstag: **24.11.2022**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **11.01.2024**
(45) Veröffentlichungstag der Patenterteilung: **24.04.2025**

(51) Int Cl.: ***H04L 9/08*** (2006.01)
H04L 9/06 (2006.01)
H04L 9/14 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)
G06F 21/62 (2013.01)
G09C 1/00 (2006.01)

Innerhalb von neun 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).

(73) Patentinhaber:
MITSUBISHI ELECTRIC CORPORATION, Tokyo, JP

(74) Vertreter:
Pfenning, Meinig & Partner mbB Patentanwälte, 10719 Berlin, DE

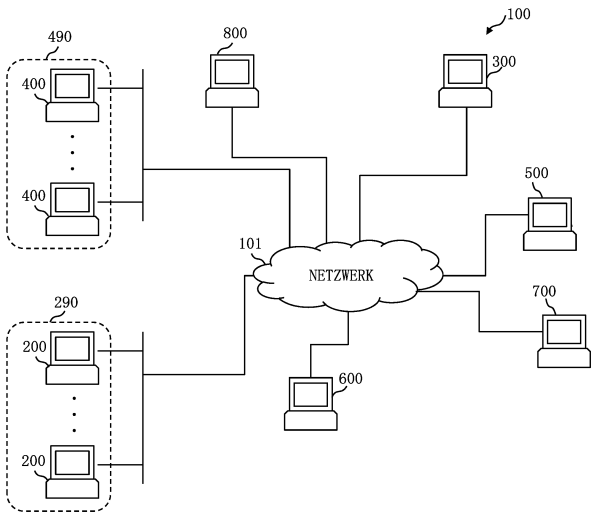
(72) Erfinder:
Kawai, Yutaka, Tokyo, JP

(56) Ermittelter Stand der Technik:

US	**2018 / 0 254 901**	**A1**
WO	**2018/ 225 248**	**A1**
JP	**6 867 718**	**B1**

(54) Bezeichnung: **CHIFFRETEXT-UMWANDLUNGSSYSTEM, UMWANDLUNGSSCHLÜSSEL-ERZEUGUNGSVERFAHREN UND UMWANDLUNGSSCHLÜSSEL-ERZEUGUNGSPROGRAMM**

(57) Hauptanspruch: Chiffretext-Umwandlungssystem (100), umfassend:
eine Umwandlungsschlüssel-Erzeugungsvorrichtung (600), umfassend
eine Umwandlungsziel-Einstelleinheit (603) zum Erzeugen eines attributbasierten Verschlüsselungsschlüssels und eines attributbasierten Chiffretextes, der mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird, gemäß einem attributbasierten Verschlüsselungsschema; und
eine Umwandlungsschlüssel-Erzeugungseinheit (604)
zum Erzeugen eines Umwandlungsschlüssels, der einen ersten Common-Key-Chiffretext in einen zweiten Common-Key-Chiffretext umwandelt, der ein Chiffretext ist, der mit einem ersten Common-Key-Kryptographieschema übereinstimmt und der sich von dem ersten Common-Key-Chiffretext unterscheidet, auf der Grundlage einer ersten kryptographischen Common-Key-Information, die beim Erzeugen des ersten Common-Key-Chiffretextes verwendet wird, durch Verschlüsseln eines Klartextes mit einem ersten geheimen Schlüssel gemäß dem ersten Common-Key-Kryptographieschema, und
zum Erzeugen eines dritten Common-Key-Chiffretextes gemäß einem zweiten Common-Key-Kryptographieschema zu erzeugen, indem ein zweiter geheimer Schlüssel, der zum Entschlüsseln des zweiten Common-Key-Chiffretextes verwendet wird, mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Offenbarung bezieht sich auf ein Chiffretext-Umwandlungssystem, ein Umwandlungsschlüssel-Erzeugungsverfahren und ein Umwandlungsschlüssel-Erzeugungsprogramm.

STAND DER TECHNIK

[0002] Ein Proxy Re-Encryption (PRE)-Schema ist ein System, in dem die Entschlüsselungsbefugnis eines Chiffretextes an eine andere Person delegiert wird, anstatt den Chiffretext zu entschlüsseln. Die Nicht-Patentliteratur 1 offenbart ein PRE-Schema (Attribute-Based PRE, ABPRE) zur attributbasierten Verschlüsselung eines beliebigen Schemas. Mit dem in der Nicht-Patent-Literatur 1 offenbarte Schema wird die Proxy-Wiederverschlüsselung zwischen verschiedenen attributbasierten Verschlüsselungen realisiert. Die Nichtpatentliteratur 2 offenbart ein Verfahren zum Ändern eines Schlüssels einer Common-Key-Kryptographie, ohne einen Chiffretext der Common-Key-Kryptographie zu entschlüsseln.
Weitere Verschlüsselungsverfahren sind in der Patentliteratur 1, der Patentliteratur 2 und der Patentliteratur 3 offenbart.

REFERENZLISTE

NICHT-PATENTLITERATUR

Nicht-Patentliteratur 1: Zuoxia Yu et al., „Achieving Flexibility for ABE with Outsourcing via Proxy Re-Encryption“, ASIACCS' 18, June 4-8, 2018, Session 16: Applied Crypto 2, S. 659-672

Nicht-Patentliteratur 2: Amril Syalim et. al, „Realizing Proxy Re-encryption in the Symmetric World“, ICIEIS (International Conference on Informatics Engineering and Information Science) 2011, Informatics Engineering and Information Science, S. 259-274.

PATENTLITERATUR

Patentliteratur 1: JP 6867718 B1

Patentliteratur 2: WO 2018/225248 A1

Patentliteratur 3: US 2018/0254901 A1

ABRISS

TECHNISCHES PROBLEM

[0003] Ein typisches Proxy-Wiederverschlüsselungsverfahren wie das in der Nichtpatentliteratur 1 offenbarte Verfahren ist eine Technik zur Umwandlung eines Chiffretextes eines bestimmten Public-Key-Kryptographieschemas in einen Chiffretext eines anderen Public-Key-Kryptographieschemas. Die in der Nichtpatentliteratur 2 offengelegte Technik ist eine Technik zur Umwandlung eines Chiffretextes der Common-Key-Kryptographie in einen Chiffretext der Common-Key-Kryptographie.

[0004] Bei der Umwandlung eines Chiffretextes eines Common-Key-Kryptographieschemas in einen Chiffretext auf der Grundlage eines Public-Key-Kryptographieschemas nach dem Stand der Technik bleibt nichts anderes übrig, als den Chiffretext des Common-Key-Kryptographieschemas einmal zu entschlüsseln, um einen Klartext zu erhalten, und danach den durch das Public-Key-Kryptographieschema erhaltenen Klartext zu verschlüsseln. Da der Klartext offengelegt wird, ist die Sicherheit gering.

[0005] Ziel der vorliegenden Offenbarung ist es, einen mit einem Common-Key-Kryptographieschema verschlüsselten Chiffretext in einen Chiffretext umzuwandeln, der auf einem Public-Key-Kryptographieschema basiert, anstatt den mit dem Common-Key-Kryptographieschema verschlüsselten Chiffretext zu entschlüsseln.

LÖSUNG DES PROBLEMS

[0006] Ein Chiffretext-Umwandlungssystem gemäß der vorliegenden Offenbarung umfasst:

eine Umwandlungsschlüssel-Erzeugungsvorrichtung, enthaltend

eine Umwandlungsziel-Einstelleinheit zum Erzeugen eines attributbasierten Verschlüsselungsschlüssels und eines attributbasierten Chiffretextes, der mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird, gemäß einem attributbasierten Verschlüsselungsschema; und

eine Umwandlungsschlüssel-Erzeugungseinheit

zum Erzeugen eines Umwandlungsschlüssels, der einen ersten Common-Key-Chiffretext in einen zweiten Common-Key-Chiffretext umwandelt, der ein Chiffretext ist, der mit einem ersten Common-Key-Kryptographieschema übereinstimmt und der sich von dem ersten Common-Key-Chiffretext unterscheidet, auf der Grundlage einer ersten kryptographischen Common-Key-Information, die beim Erzeugen des ersten Common-Key-Chiffretextes verwendet wird, durch Verschlüsseln eines Klartextes mit einem ersten geheimen Schlüssel gemäß dem ersten Common-Key-Kryptographieschema, und

zum Erzeugen eines dritten Common-Key-Chiffretextes gemäß einem zweiten Common-Key-Kryptographieschema zu erzeugen, indem ein zweiter geheimer Schlüssel, der zum Entschlüsseln des zweiten Common-Key-Chiffretextes verwendet wird, mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird.

VORTEILHAFTE WIRKUNGEN DER ERFINDUNG

[0007] Bei der vorliegenden Offenlegung ist ein attributbasierter Chiffretext ein Chiffretext eines Public-Key-Kryptographieschemas . Ein dritter Common-Key-Chiffretext ist ein Chiffretext, der durch Verschlüsseln eines zweiten geheimen Schlüssels mit einem attributbasierten Verschlüsselungsschlüssel erhalten wird, der zur Erzeugung des attributbasierten Chiffretextes verwendet wird. Hier wird der zweite geheime Schlüssel verwendet, um einen zweiten Common-Key-Chiffretext zu entschlüsseln. Der zweite Common-Key-Chiffretext ist also ein Chiffretext, der auf dem Public-Key-Kryptographieschema basiert. Ferner ist ein erster Common-Key-Chiffretext ein Chiffretext, der durch ein erstes Common-Key-Kryptographieschema verschlüsselt wird, das ein Common-Key-Kryptographieschema ist. Der zweite Common-Key-Chiffretext ist ein Chiffretext, der durch Umwandlung des ersten Common-Key-Chiffretextes mit Hilfe eines Umwandlungsschlüssels gewonnen wird. Bei der Umwandlung des ersten Common-Key-Chiffretextes in den zweiten Common-Key-Chiffretext ist es nicht erforderlich, den ersten Common-Key-Chiffretext zu entschlüsseln.

[0008] Daher ist es gemäß der vorliegenden Offenlegung möglich, einen mit einem Common-Key-Kryptographieschema verschlüsselten Chiffretext in einen Chiffretext umzuwandeln, der auf einem Public-Key-Kryptographieschema basiert, ohne den mit dem Common-Key-Kryptographieschema verschlüsselten Chiffretext zu entschlüsseln.

KURZBESCHREIBUNG DER ZEICHNUNGEN

Fig. 1 ist eine Darstellung, die ein Konfigurationsbeispiel für ein Chiffretext-Umwandlungssystem 100 gemäß Ausführungsform 1 zeigt.

Fig. 2 ist eine Darstellung, die ein Konfigurationsbeispiels einer Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung 200 gemäß Ausführungsform 1 zeigt.

Fig. 3 ist eine Darstellung, die ein Konfigurationsbeispiel einer Parametererzeugungsvorrichtung 300 zeigt.

Fig. 4 ist eine Darstellung, die ein Konfigurationsbeispiel einer Vorrichtung zur Erzeugung geheimer Benutzerschlüssel 400 gemäß Ausführungsform 1 zeigt.

Fig. 5 ist eine Darstellung, die ein Konfigurationsbeispiel für eine Common-Key-Chiffretext-Erzeugungsvorrichtung 500 gemäß Ausführungsform 1 zeigt.

Fig. 6 ist eine Darstellung, die ein Konfigurationsbeispiel für eine Umwandlungsschlüssel-Erzeugungsvorrichtung 600 gemäß Ausführungsform 1 zeigt.

Fig. 7 ist eine Darstellung, die ein Konfigurationsbeispiel einer Umwandlungsvorrichtung 700 gemäß Ausführungsform 1 zeigt.

Fig. 8 ist eine Darstellung, die ein Konfigurationsbeispiel für eine Entschlüsselungsvorrichtung 800 gemäß Ausführungsform 1 zeigt.

Fig. 9 ist eine Darstellung, die ein Beispiel für die Hardwarekonfiguration jeder Vorrichtung zeigt, mit der das Chiffretext-Umwandlungssystem 100 gemäß Ausführungsform 1 ausgestattet ist.

Fig. 10 ist ein Flussdiagramm, das den Betrieb der Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung 200 gemäß Ausführungsform 1 veranschaulicht.

Fig. 11 ist ein Flussdiagramm, das den Betrieb der Parametererzeugungsvorrichtung 300 gemäß Ausführungsform 1 veranschaulicht.

Fig. 12 ist ein Flussdiagramm, das den Betrieb der Benutzergeheimschlüssel-Erzeugungsvorrichtung 400 gemäß Ausführungsform 1 veranschaulicht.

Fig. 13 ist ein Flussdiagramm, das den Betrieb der Common-Key-Chiffretext-Erzeugungsvorrichtung 500 gemäß Ausführungsform 1 veranschaulicht.

Fig. 14 ist ein Flussdiagramm, das den Betrieb der Umwandlungsschlüssel-Erzeugungsvorrichtung 600 gemäß Ausführungsform 1 veranschaulicht.

Fig. 15 ist ein Flussdiagramm, das den Betrieb der Umwandlungsvorrichtung 700 gemäß Ausführungsform 1 veranschaulicht.

Fig. 16 ist ein Flussdiagramm, das den Betrieb der Entschlüsselungsvorrichtung 800 gemäß Ausführungsform 1 veranschaulicht.

Fig. 17 ist eine Darstellung, die ein Hardware-Konfigurationsdiagramm jeder Vorrichtung zeigt, mit der ein Chiffretext-Umwandlungssystem 100 gemäß einer Modifikation von Ausführungsform 1 ausgestattet ist.

BESCHREIBUNG DER AUSFÜHRUNGSFORMEN

[0009] In der Beschreibung und den Zeichnungen der Ausführungsform sind gleiche und gleichwertige Elemente mit dem gleichen Bezugszeichen versehen. Die Beschreibung von Elementen, die mit demselben Bezugszeichen versehen sind, wird in geeigneter Weise weggelassen oder vereinfacht. Pfeile in den Zeichnungen zeigen hauptsächlich Datenflüsse oder Prozessabläufe an. Beachten Sie, dass der Begriff „Einheit“ oder „Vorrichtung“ durch „Schaltkreis“, „Methode“, „Stufe“, „Verfahren“, „Prozess“ oder „Schaltung“ angemessen ersetzt werden kann.

Ausführungsform 1.

[0010] Die vorliegende Ausführungsform wird nachstehend unter Bezugnahme auf Zeichnungen detailliert beschrieben.

*** Beschreibung von Konfigurationen ***

[0011] **Fig.** 1 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für ein Chiffretext-Umwandlungssystem 100 gemäß der vorliegenden Ausführungsform zeigt.

[0012] Wie in **Fig.** 1 dargestellt, ist ein Chiffretext-Umwandlungssystem 100 mit einer Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtungsgruppe 290 versehen, die aus einer Mehrzahl von Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtungen 200, einer Parametererzeugungsvorrichtung 300, einer Benutzer-Geheimschlüssel-Erzeugungsvorrichtungsgruppe 490, die aus einer Mehrzahl von Benutzer-Geheimschlüssel-Erzeugungsvorrichtungen 400 besteht, einer Common-Key-Chiffretext-Erzeugungsvorrichtung 500, einer Umwandlungsschlüssel-Erzeugungsvorrichtung 600, einer Umwandlungsvorrichtung 700 und einer Entschlüsselungsvorrichtung 800 besteht. Bei den Vorrichtungen, mit denen das Chiffretext-Umwandlungssystem 100 ausgestattet ist, handelt es sich jeweils um einen Computer, und ein spezielles Beispiel für einen Computer ist ein Personal Computer (PC). Mindestens zwei der Vorrichtungen, mit denen das Chiffretext-Umwandlungssystem 100 ausgestattet ist, können jeweils aus einem Computer bestehen.

[0013] Ein Netzwerk 101 ist ein Kommunikationsweg zur Verbindung der Vorrichtungen, mit denen das Chiffretext-Umwandlungssystem 100 ausgestattet ist. Ein konkretes Beispiel für ein Netzwerk 101 ist das Internet, es kann aber auch ein anderes Netzwerk sein.

[0014] Die Vorrichtungen, mit denen das Chiffretext-Umwandlungssystem 100 ausgestattet ist, müssen nicht über das Netzwerk 101 verbunden sein, sondern können in einem lokalen Netzwerk (LAN) platziert werden, das in einer bestimmten Einrichtung liegt.

[0015] Die Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung 200 erzeugt einen Common-Key-Chiffretext-Geheimschlüssel und überträgt den erzeugten Common-Key-Chiffretext-Geheimschlüssel an die Common-Key-Chiffretext-Erzeugungsvorrichtung 500 und die Umwandlungsschlüssel-Erzeugungsvorrichtung 600.

[0016] Bei der Parametererzeugungsvorrichtung 300 handelt es sich um einen Computer, der einen gemeinsamen Parameter für das Chiffretext-Umwandlungssystem 100 erzeugt und den erzeugten gemeinsamen Parameter über das Netzwerk 101 an Mehrzahl von Benutzergeheimschlüssel-Erzeugungsvorrichtungen 400, die Umwandlungsschlüssel-Erzeugungsvorrichtung 600, die Umwandlungsvorrichtung 700 und die Entschlüsselungsvorrichtung 800 überträgt. Es ist zu beachten, dass der gemeinsame Parameter direkt per Post oder ähnlichem übermittelt werden kann, statt über das Netzwerk 101.

[0017] Die Benutzergeheimschlüssel-Erzeugungsvorrichtung 400 erzeugt einen geheimen Benutzerschlüssel und überträgt den erzeugten geheimen Benutzerschlüssel an die Entschlüsselungsvorrichtung 800.

[0018] Die Common-Key-Chiffretext-Erzeugungsvorrichtung 500 fungiert als Datenverschlüsselungsvorrichtung. Die Common-Key-Chiffretext-Erzeugungsvorrichtung 500 empfängt den geheimen Common-Key-Kryptographie-Schlüssel von der Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung 200 und nimmt einen Klartext M als Eingabe. Unter Verwendung des geheimen Common-Key-Chiffretext-Schlüssels und des Klartextes M erzeugt die Common-Key-Chiffretext-Erzeugungsvorrichtung 500 einen Common-Key-Chiffretext skC und eine Hilfsinformation für den Chiffretext auxC, und gibt den erzeugten Common-Key-Chiffretext skC und die Hilfsinformation für den Chiffretext auxC aus.

[0019] Die Umwandlungsschlüssel-Erzeugungsvorrichtung 600 empfängt einen öffentlichen Schlüssel von der Parametererzeugungsvorrichtung 300, den Common-Key-Kryptographie-Geheimschlüssel von der Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung 200 und Hilfsinformationen über den Chiffretext von der Common-Key-Chiffretext-Erzeugungsvorrichtung 500 und nimmt eine Entschlüsselungsbedingung L als Eingabe. Unter Verwendung des öffentlichen Schlüssels, des Common-Key-Chiffretext-Geheimschlüssels und der Chiffretext-Hilfsinformationen erzeugt die Umwandlungsschlüssel-Erzeugungsvorrichtung 600 einen Umwandlungsschlüssel ck und gibt den erzeugten Umwandlungsschlüssel ck aus. Die Entschlüsselungsbedingung L ist eine Bedingung, die mit einer logischen Formel ausdrückt, dass ein Benutzer in der Lage ist, einen Chiffretext nach der Konvertierung zu entschlüsseln.

[0020] Die Umwandlungsvorrichtung 700 erhält den Umwandlungsschlüssel von der Umwandlungsschlüssel-Erzeugungsvorrichtung 600 und den Common-Key-Chiffretext von der Common-Key-Chiffretext-Erzeugungsvorrichtung 500. Unter Verwendung des Umwandlungsschlüssels und des Common-Key-Chiffretextes erzeugt die Umwandlungsvorrichtung 700 einen Common-Key-Chiffretext nach Umwandlung skC' und einen Public-Key-Chiffretext nach Umwandlung pkC, und gibt den erzeugten Public-Key-Chiffretext nach Umwandlung skC' und den Public-Key-Chiffretext nach Umwandlung pkC an die Entschlüsselungsvorrichtung 800 aus.

[0021] Die Entschlüsselungsvorrichtung 800 empfängt den Common-Key-Chiffretext (skC', auxC') nach Umwandlung und den Public-Key-Chiffretext pkC nach Umwandlung von der Umwandlungsvorrichtung 700 und den geheimen Benutzerschlüssel von der Benutzergeheimschlüssel-Erzeugungsvorrichtung 400. Die Entschlüsselungsvorrichtung 800 entschlüsselt den Chiffretext unter Verwendung des empfangenen geheimen Benutzerschlüssels und gibt ein Entschlüsselungsergebnis aus.

[0022] Eine Konfiguration der vorliegenden Ausführungsform wird im Folgenden beschrieben.

[0023] Fig. 2 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für die Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung 200 zeigt.

[0024] Wie in **Fig.** 2 dargestellt, ist die Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung 200 mit einer Eingabeeinheit 201, einer Common-Key-Kryptographie-Schlüsselerzeugungseinheit 202 und einer Übertragungseinheit 203 versehen.

[0025] Obwohl nicht dargestellt, ist die Common-Key-Kryptographie-Schlüsselerzeugungsvorrichtung 200 mit einem Aufzeichnungsmedium versehen, das Daten speichert, die in den einzelnen Einheiten der Common-Key-Kryptographie-Schlüssel-Erzeugungsvorrichtung 200 zu verwenden sind.

[0026] Die Eingabeeinheit 201 akzeptiert die Eingabe einer Bitlänge eines im vorliegenden System verwendeten Schlüssels.

[0027] Die Common-Key-Kryptographie-Schlüsselerzeugungseinheit 202 erzeugt einen geheimen Common-Key-Kryptographie-Schlüssel, der eine Berechnungsgrundlage für das Chiffretext-Umwandlungssystem 100 darstellt. Obwohl nicht dargestellt, kann die Common-Key-Kryptographie-Schlüsselerzeugungseinheit 202 mit einer Zufallszahlengenerierungsfunktion oder ähnlichem ausgestattet sein, um den geheimen Schlüssel der Common-Key-Kryptographie zu erzeugen.

[0028] Die Übertragungseinheit 203 überträgt den von der Common-Key-Kryptographie-Schlüsselerzeugungseinheit 202 erzeugten Common-Key-Chiffretext-Geheimschlüssel an jede der Common-Key-Chiffretext-Erzeugungseinheit 500 und der Umwandlungsschlüssel-Erzeugungsvorrichtung 600.

[0029] **Fig.** 3 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für die gemeinsame Parametererzeugungsvorrichtung 300 zeigt.

[0030] Wie in **Fig.** 3 dargestellt, ist die Gemeinsame-Parameter-Erzeugungsvorrichtung 300 mit einer Eingabeeinheit 301, einer Gemeinsamen-Parameter-Erzeugungsvorrichtung 302 und einer Übertragungseinheit 303 versehen.

[0031] Obwohl nicht dargestellt, ist die Gemeinsame-Parameter-Erzeugungsvorrichtung 300 mit einem Aufzeichnungsmedium versehen, das Daten speichert, die in den einzelnen Einheiten der Gemeinsamen-Parameter-Erzeugungsvorrichtung 300 zu verwenden sind.

[0032] Die Eingabeeinheit 301 akzeptiert die Eingabe einer Bitlänge des Schlüssels, der im Chiffretext-Umwandlungssystem 100 verwendet wird.

[0033] Die Gemeinsame-Parameter-Erzeugungsvorrichtung 302 erzeugt jeweils einen öffentlichen Schlüssel pk und einen geheimen Hauptschlüssel msk, die bei der vom Chiffretext-Umwandlungssystem 100 durchgeführten Berechnung verwendet werden. Obwohl nicht dargestellt, kann die Gemeinsame-Parameter-Erzeugungsvorrichtung 302 mit einer Funktion zur Erzeugung von Zufallszahlen oder ähnlichem ausgestattet sein, um sowohl den öffentlichen Schlüssel pk als auch den geheimen Hauptschlüssel msk zu erzeugen.

[0034] Die Übertragungseinheit 303 überträgt den von der Gemeinsame-Parameter-Erzeugungsvorrichtung 302 erzeugten öffentlichen Schlüssel pk an jede der Umwandlungsschlüssel-Erzeugungsvorrichtung 600 und der Umwandlungsvorrichtung 700. Die Übertragungseinheit 303 überträgt auch den geheimen Hauptschlüssel msk an jede der mehreren Benutzergeheimschlüssel-Erzeugungsvorrichtungen 400.

[0035] **Fig.** 4 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für die Benutzergeheimschlüssel-Erzeugungsvorrichtung 400 zeigt. Wie in **Fig.** 4 dargestellt, ist die Benutzergeheimschlüssel-Erzeugungsvorrichtung 400 mit einer Eingabeeinheit 401, einer Schlüsselempfangseinheit 402, einer Schlüsselerzeugungseinheit 403 und einer Schlüsselübertragungseinheit 404 ausgestattet.

[0036] Obwohl nicht dargestellt, ist die Benutzergeheimschlüssel-Erzeugungsvorrichtung 400 mit einem Aufzeichnungsmedium versehen, das Daten speichert, die in den einzelnen Einheiten der Benutzergeheimschlüssel-Erzeugungsvorrichtung 400 verwendet werden sollen.

[0037] Die Eingabeeinheit 401 nimmt einen Attributparameter Γ als Eingabe entgegen.

[0038] Die Schlüsselempfangseinheit 402 empfängt den geheimen Hauptschlüssel msk.

[0039] Die Schlüsselerzeugungseinheit 403 erzeugt einen geheimen Benutzerschlüssel sk_{Γ}. Obwohl nicht dargestellt, kann die Schlüsselerzeugungseinheit 403 mit einer Zufallszahlengenerierungsfunktion oder ähnlichem ausgestattet sein, um den geheimen Benutzerschlüssel sk_{Γ} zu erzeugen.

[0040] Die Schlüsselübertragungseinheit 404 überträgt den von der Schlüsselerzeugungseinheit 403 erzeugten geheimen Benutzerschlüssel sk_Γ an die Entschlüsselungsvorrichtung 800.

[0041] **Fig.** 5 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für die Common-Key-Chiffretext-Erzeugungsvorrichtung 500 zeigt. Wie in **Fig.** 5 dargestellt, ist die Common-Key-Chiffretext-Erzeugungsvorrichtung 500 mit einer Eingabeeinheit 501, einer Schlüsselempfangseinheit 502, einer Verschlüsselungseinheit 503 und einer Übertragungseinheit 504 ausgestattet.

[0042] Obwohl nicht dargestellt, ist die Common-Key-Chiffretext-Erzeugungsvorrichtung 500 mit einem Aufzeichnungsmedium versehen, das Daten speichert, die in den einzelnen Einheiten der Common-Key-Chiffretext-Erzeugungsvorrichtung 500 verwendet werden sollen.

[0043] Die Eingabeeinheit nimmt den Klartest M als Eingabe an.

[0044] Die Schlüsselempfangseinheit 502 empfängt den geheimen Schlüssel sk der Common-Key-Kryptografie.

[0045] Die Verschlüsselungsvorrichtung 503 erzeugt den Common-Key-Chiffretext skC und die Hilfsinformationen auxC. Obwohl nicht dargestellt, kann die Verschlüsselungsvorrichtung 503 mit einer Zufallszahlengenerierungsfunktion oder ähnlichem ausgestattet sein, um den Common-Key-Chiffretext skC zu erzeugen. Die Verschlüsselungsvorrichtung 503 erzeugt einen ersten Common-Key-Chiffretext.

[0046] Die Übertragungseinheit 504 leitet den Common-Key-Chiffretext skC an die Umwandlungsvorrichtung 700 und die Hilfsinformationen auxC an die Umwandlungsschlüssel-Erzeugungsvorrichtung 600 weiter.

[0047] **Fig.** 6 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für die Umwandlungsschlüssel-Erzeugungsvorrichtung 600 zeigt.

[0048] Wie in **Fig.** 6 dargestellt, ist die Umwandlungsschlüssel-Erzeugungsvorrichtung 600 mit einer Schlüsselempfangseinheit 601, einer Eingabeeinheit 602, einer Umwandlungsziel-Einstelleinheit 603, einer Umwandlungsschlüssel-Erzeugungseinheit 604 und einer Übertragungseinheit 605 versehen.

[0049] Obwohl nicht dargestellt, ist die Umwandlungsschlüssel-Erzeugungsvorrichtung 600 mit einem Aufzeichnungsmedium versehen, das Daten speichert, die in den einzelnen Einheiten der Umwandlungsschlüssel-Erzeugungsvorrichtung 600 verwendet werden sollen.

[0050] Die Schlüsselempfangseinheit 601 empfängt jeweils den öffentlichen Schlüssel pk, den geheimen Schlüssel sk und die Hilfsinformationen auxC.

[0051] Die Eingabeeinheit 602 nimmt die Entschlüsselungsbedingung L von außen als Eingabe entgegen.

[0052] Die Umwandlungsziel-Einstelleinheit 603 erzeugt einen Public-Key-Chiffretext P, der Teil des Umwandlungsschlüssels ist, aus dem von der Schlüsselempfangseinheit 601 empfangenen öffentlichen Schlüssel pk und der von der Eingabeeinheit 602 eingegebenen Entschlüsselungsbedingung L. Die Umwandlungsziel-Einstelleinheit 603 erzeugt einen attributbasierten Verschlüsselungsschlüssel und einen attributbasierten Chiffretext, der mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird, gemäß einem attributbasierten Verschlüsselungsschema.

[0053] Die Umwandlungsschlüssel-Erzeugungseinheit 604 erzeugt aus dem geheimen Common-Key-Kryptographie-Schlüssel sk und den Hilfsinformationen auxC, die von der Schlüsselempfangseinheit 601 empfangen werden, den Teil S des Umwandlungsschlüssels. Die Umwandlungsschlüssel-Erzeugungseinheit 604 erzeugt einen Umwandlungsschlüssel, der den ersten Common-Key-Chiffretext in einen zweiten Common-Key-Chiffretext umwandelt, der ein Chiffretext ist, der mit einem ersten Common-Key-Kryptographieschema übereinstimmt und sich von dem ersten Common-Key-Chiffretext unterscheidet, und zwar auf der Grundlage erster kryptographischer Common-Key-Informationen, die beim Erzeugen des ersten Common-Key-Chiffretextes verwendet wurden, indem ein Klartext gemäß dem ersten Common-Key-Kryptographieschema mit einem ersten geheimen Schlüssel verschlüsselt wird. Die Umwandlungsschlüssel-Erzeugungseinheit 604 erzeugt einen dritten Common-Key-Chiffretext nach einem zweiten Common-Key-Kryptographieschema durch Verschlüsseln eines zweiten geheimen Schlüssels, der zum Entschlüsseln des zweiten Common-Key-Chiffretextes verwendet wird, mit dem attributbasierten Verschlüsselungsschlüssel. Ein spezielles Beispiel für

das erste Common-Key-Kryptographieschema ist ein Blockchiffrier-Counter-Mode-Schema. Die erste kryptographische Common-Key-Information kann aus dem ersten geheimen Schlüssel und einer ersten Hilfsinformation bestehen, die bei der Verschlüsselung nach dem Blockchiffrier-Counter-Mode-Schema verwendet wird. Die Umwandlungsschlüssel-Erzeugungseinheit 604 kann den Umwandlungsschlüssel unter Verwendung der ersten kryptographischen Common-Key-Information und der zweiten kryptographischen Common-Key-Information erzeugen, die aus dem zweiten geheimen Schlüssel und der zweiten Hilfsinformation besteht, die bei der Verschlüsselung nach dem Blockchiffrier-Counter-Mode-Schema verwendet werden. Die Umwandlungsschlüssel-Erzeugungseinheit 604 kann als Umwandlungsschlüssel ein exklusives ODER eines Ergebnisses der Ausführung des ersten Common-Key-Kryptographie-Schemas unter Verwendung der ersten kryptographischen Common-Key-Information und eines Ergebnisses der Ausführung des ersten Common-Key-Kryptographie-Schemas unter Verwendung der zweiten kryptographischen Common-Key-Information berechnen.

[0054] Obwohl nicht dargestellt, können die Umwandlungsziel-Einstelleinheit 603 und die Umwandlungsschlüssel-Erzeugungseinheit 604 jeweils mit einer Zufallszahlen-Erzeugungsfunktion oder ähnlichem ausgestattet sein, um den Umwandlungsschlüssel zu erzeugen.

[0055] Die Übertragungseinheit 605 integriert generierte Umwandlungsschlüssel und gibt einen integrierten Umwandlungsschlüssel an die Umwandlungsvorrichtung 700 als den Umwandlungsschlüssel ck (= (P, S)) aus.

[0056] **Fig.** 7 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für die Umwandlungsvorrichtung 700 zeigt. Wie in **Fig.** 7 dargestellt, ist die Umwandlungsvorrichtung 700 mit einer Schlüsselempfangseinheit 701, einer Chiffretext-Empfangseinheit 702, einer Umwandlungseinheit 703 und einer Übertragungseinheit 704 ausgestattet.

[0057] Obwohl nicht dargestellt, ist die Umwandlungsvorrichtung 700 mit einem Aufzeichnungsmedium versehen, das Daten speichert, die in den einzelnen Einheiten der Umwandlungsvorrichtung 700 verwendet werden sollen.

[0058] Die Schlüsselempfangseinheit 701 empfängt jeweils den öffentlichen Schlüssel pk und den Umwandlungsschlüssel ck.

[0059] Die Chiffretext-Empfangseinheit 702 empfängt den Common-Key-Chiffretext skC.

[0060] Die Umwandlungseinheit 703 wandelt den Common-Key-Chiffretext skC mit Hilfe eines Teils des Umwandlungsschlüssels ck um, wodurch der Common-Key-Chiffretext skC in den Common-Key-Chiffretext nach Umwandlung skC' umgewandelt wird. Der Common-Key-Chiffretext nach Umwandlung skC' ist ein Chiffretext, für den die Entschlüsselungsbedingung bezüglich des Public-Key-Chiffretextes P gilt. Die Umwandlungseinheit 703 erzeugt auch den Public-Key-Chiffretext nach Umwandlung pkC unter Verwendung eines Teils des Umwandlungsschlüssels ck. Die Umwandlungseinheit 703 berechnet als zweiten Common-Key-Chiffretext ein exklusives ODER des ersten Common-Key-Chiffretextes und des Umwandlungsschlüssels.

[0061] Die Übertragungseinheit 704 gibt den Public-Key-Chiffretext pkC und den Common-Key-Chiffretext (skC', auxC') nach Umwandlung an die Entschlüsselungsvorrichtung 800 aus.

[0062] **Fig.** 8 ist ein Blockdiagramm, das ein Konfigurationsbeispiel für die Entschlüsselungsvorrichtung 800 zeigt. Wie in **Fig.** 8 dargestellt, ist die Entschlüsselungsvorrichtung 800 mit einer Chiffretext-Empfangseinheit 801, einer Schlüsselempfangseinheit 802, einer Entschlüsselungseinheit 803 und einer Ergebnisausgabeeinheit 804 ausgestattet.

[0063] Die Chiffretext-Empfangseinheit 801 empfängt den Public-Key-Chiffretext nach Umwandlung pkC und den Common-Key-Chiffretext nach Umwandlung (skC', auxC').

[0064] Die Schlüsselempfangseinheit 802 empfängt den geheimen Benutzerschlüssel sk_Γ von der Benutzergeheimschlüssel-Erzeugungsvorrichtung 400.

[0065] Die Entschlüsselungseinheit 803 berechnet den Klartext M, indem sie einen Entschlüsselungsprozess durchführt. In einem speziellen Beispiel des Entschlüsselungsprozesses entschlüsselt die Entschlüss-

elungseinheit 803 zunächst den attributbasierten Chiffretext unter Verwendung des geheimen Benutzerschlüssels, der mit den Attributinformationen übereinstimmt, die dem attributbasierten Verschlüsselungsschlüssel entsprechen, und gewinnt so den attributbasierten Verschlüsselungsschlüssel. Anschließend entschlüsselt die Entschlüsselungseinheit 803 den dritten Common-Key-Chiffretext unter Verwendung des erworbenen attributbasierten Verschlüsselungsschlüssels, wodurch sie den zweiten geheimen Schlüssel erhält. Anschließend findet die Entschlüsselungseinheit 803 als Klartext, der dem erworbenen zweiten Common-Key-Chiffretext entspricht, ein exklusives ODER eines Ergebnisses des Verschlüsselns der zweiten Hilfsinformation mit dem zweiten geheimen Schlüssel und des zweiten Common-Key-Chiffretextes.

[0066] Die Ergebnisausgabeeinheit 804 gibt den Klartext M aus.

[0067] **Fig.** 9 ist eine Darstellung, die ein Beispiel für die Hardware-Ressourcen der einzelnen Vorrichtungen zeigt, mit denen das Chiffretext-Umwandlungssystem 100 gemäß der vorliegenden Ausführungsform ausgestattet ist. Jedes Chiffretext-Umwandlungssystem 100 kann aus einer Vielzahl von Computern bestehen.

[0068] Jede Vorrichtung des Chiffretext-Umwandlungssystems 100 ist mit einem Prozessor 11 (Central Processing Unit) ausgestattet. Der Prozessor 11 ist über einen Bus 12 mit Hardwarevorrichtungen wie einem Nur-Lese-Speicher (ROM) 13, einem Direktzugriffsspeicher (RAM) 14, einer Kommunikationsplatine 15, einer Anzeige 51 (Anzeigevorrichtung), einer Tastatur 52, einer Maus 53, einem Laufwerk 54 und einer Magnetplattenvorrichtung 20 verbunden und steuert diese Hardwarevorrichtungen. Das Laufwerk 54 ist eine Vorrichtung, die von einem Speichermedium wie einem Flexible Disk Drive (FD), einer Compact Disc (CD) und einer Digital Versatile Disc (DVD) liest und darauf schreibt.

[0069] Der Prozessor 11 ist ein integrierter Schaltkreis (IC), der eine Rechenverarbeitung durchführt. Ein konkretes Beispiel für den Prozessor 11 ist eine Zentraleinheit (CPU), ein Digitalsignalprozessor (DSP) oder eine Grafikverarbeitungseinheit (GPU). Jede Vorrichtung des Chiffretext-Umwandlungssystems 100 kann mit einer Vielzahl von Prozessoren ausgestattet sein, die den Prozessor 11 ersetzen. Die Vielzahl von Prozessoren teilen sich die Rollen des Prozessors 11.

[0070] Der ROM 13, der RAM 14, die Magnetplattenvorrichtung 20 und das Laufwerk 54 sind jeweils ein Beispiel für eine Speichervorrichtung. Die Tastatur 52, die Maus 53 und die Kommunikationsplatine 15 sind jeweils ein Beispiel für eine Eingabevorrichtung. Die Anzeige 51 und die Kommunikationsplatine 15 sind jeweils ein Beispiel für eine Ausgabevorrichtung.

[0071] Die Kommunikationsplatine 15 ist über ein Kabel oder drahtlos mit einem Netzwerk wie einem Local Area Network (LAN), dem Internet oder einer Telefonleitung verbunden. In einem konkreten Beispiel besteht die Kommunikationsplatine 15 aus einem Kommunikationschip oder einer Netzwerkschnittstellenkarte (NIC).

[0072] Ein Betriebssystem (Betriebssystem) 21, Programme 22 und Dateien 23 sind in der Magnetplattenvorrichtung 20 gespeichert. Ein spezifisches Beispiel für eine Magnetplattenvorrichtung 20 ist ein Festplattenlaufwerk (HDD). Alternativ kann die Magnetplattenvorrichtung 20 auch ein Flash-Speicher oder ähnliches sein.

[0073] Die Programme 22 umfassen Programme, die Funktionen ausführen, die in der vorliegenden Ausführungsform als einzelne Einheiten beschrieben werden. Ein konkretes Beispiel für ein solches Programm ist ein Datensuchprogramm oder ein Datenregistrierungsprogramm. Das Programm wird von dem Prozessor 11 gelesen und ausgeführt. Das heißt, das Programm veranlasst den Computer, als Einheit zu funktionieren, und veranlasst den Computer, ein Verfahren oder eine Methode der Einheit auszuführen. Jedes in der vorliegenden Spezifikation beschriebene Programm kann auf einem computerlesbaren nichtflüchtigen Aufzeichnungsmedium aufgezeichnet werden. Ein spezifisches Beispiel für ein nichtflüchtiges Aufzeichnungsmedium ist eine optische Platte oder ein Flash-Speicher. Jedes in der vorliegenden Spezifikation beschriebene Programm kann als Programmprodukt bereitgestellt werden.

[0074] Die Dateien 23 enthalten Daten, die in den einzelnen, in der vorliegenden Ausführungsform beschriebenen Einheiten zu verwenden sind. In einem konkreten Beispiel bestehen die relevanten Daten aus Eingabedaten, Ausgabedaten, einem Ermittlungsergebnis, einem Berechnungsergebnis und einem Verarbeitungsergebnis.

*** Beschreibung von Funktionsweisen***

[0075] Ein Betriebsverfahren des Chiffretext-Umwandlungssystems 100 entspricht einer Chiffretext-Umwandlungsmethode. Ein Programm, das Operationen des Chiffretext-Umwandlungssystems 100 implementiert, entspricht einem Chiffretext-Umwandlungsprogramm. Ein Betriebsverfahren einer dem Chiffretext-Umwandlungssystem 100 zur Verfügung gestellten Vorrichtung entspricht einer Methode, die in ihrem Namen einen Namen dieser dem Chiffretext-Umwandlungssystem 100 zur Verfügung gestellten Vorrichtung enthält. In einem konkreten Beispiel entspricht ein Betriebsverfahren der Umwandlungsschlüssel-Erzeugungsvorrichtung 600 einem Verfahren zur Erzeugung von Umwandlungsschlüsseln. Ein Programm, das Operationen einer dem Chiffretext-Umwandlungssystem 100 zur Verfügung gestellten Vorrichtung implementiert, entspricht einem Programm, das in seinem Namen einen Namen dieser dem Chiffretext-Umwandlungssystem 100 zur Verfügung gestellten Vorrichtung enthält. In einem konkreten Beispiel entspricht ein Programm, das die Operationen der Umwandlungsschlüssel-Erzeugungsvorrichtung 600 implementiert, einem Programm zur Erzeugung von Umwandlungsschlüsseln.

[0076] Nachfolgend werden die Operationen des Chiffretext-Umwandlungssystems 100 beschrieben, die einer Berechnungsmethode jeder Vorrichtung gemäß der vorliegenden Ausführungsform entsprechen.

[0077] Vor der Beschreibung der Operationen des Chiffretext-Umwandlungssystems 100 werden eine grundlegende kryptographische Technik, die in der vorliegenden Ausführungsform verwendet wird, und die in der entsprechenden kryptographischen Technik verwendete Notation beschrieben.

[0078] Ein attributbasiertes Verschlüsselungsverfahren ist eine kryptografische Technik, bei der eine Entschlüsselung nur für einen Benutzer möglich ist, der einen geheimen Benutzerschlüssel besitzt, der aus einem Attributparameter Γ erzeugt wird, der eine Entschlüsselungsbedingung erfüllt, die mit der Entschlüsselungsbedingung L festgelegt wird. Der Attributparameter Γ ist ebenfalls ein Attributsatz. Das attributbasierte Verschlüsselungsverfahren besteht aus einem Algorithmus, der wie folgt aufgebaut ist.

[0079] Zunächst wird die Einrichtung ABESETUP, eine Schlüssellänge usw. eingegeben, und der geheime Hauptschlüssel msk und der öffentliche Schlüssel pk werden ausgegeben. Als Nächstes werden die Generierung des geheimen Benutzerschlüssels ABEKEYGEN, der geheime Hauptschlüssel msk und der Attributparameter Γ eingegeben, und der geheime Benutzerschlüssel sk_Γ, der dem Attributparameter Γ entspricht, wird generiert. Als Nächstes werden die Verschlüsselung ABEENC, der öffentliche Schlüssel pk und die Entschlüsselungsbedingung L eingegeben und ein Schlüssel K für die Common-Key-Kryptographie sowie der Public-Key-Chiffretext P, der mit dem Schlüssel K übereinstimmt, erzeugt. Als Nächstes werden die Entschlüsselung ABEDEC, der geheime Benutzerschlüssel sk_Γ und der Public-Key-Chiffretext als Eingabe genommen, und wenn der dem geheimen Benutzerschlüssel sk_Γ entsprechende Attributparameter Γ und die Entschlüsselungsbedingung L zur Erzeugung des Public-Key-Chiffretextes P übereinstimmen, wird der Schüssel K, mit dem der Public-Key-Chiffretext P verschlüsselt wird, ausgegeben.

[0080] Die Common-Key-Kryptographie ist ein kryptographisches Verfahren zur Verschlüsselung des Klartextes M unter Verwendung des geheimen Schlüssels sk der Common-Key-Kryptographie und zum Entschlüsseln einer Chiffre unter Verwendung des geheimen Schlüssels sk der Common-Key-Kryptographie. Wenn der geheime Schlüssel sk für die Common-Key-Kryptographie ein Zufallswert ist, nimmt die Verschlüsselung SKEENC den geheimen Schlüssel sk für die Common-Key-Kryptographie und den Klartext M als Eingabe und gibt einen Chiffretext C aus, der der entsprechenden Eingabe entspricht. Entschlüsselungs-SKEDEC nimmt den geheimen Common-Key-Chiffretext sk und den Chiffretext C als Eingabe und gibt den Klartext M aus, der der jeweiligen Eingabe entspricht.

[0081] In der vorliegenden Ausführungsform wird bei der Common-Key-Kryptografie eine Counter-Mode-Verschlüsselung und einer Counter-Mode-Entschlüsslung, die eine Blockchiffre verwenden, eingesetzt. Das entsprechende Verschlüsseln wird als SCTRENC, das entsprechende Entschlüsseln als SCTRDEC bezeichnet. Im Counter-Modus liegt ein Zählerwert als Hilfsinformation vor, und das Ver- und Entschlüsseln wird wie folgt durchgeführt. In der vorliegenden Spezifikation bedeutet + ein exklusives ODER, sofern nicht anders angegeben.

[Verschlüsseln]

$$C = \mathrm{SCTRENC}(sk, auxC) + M$$

[Entschlüsseln]

$$M = SCTRDEC(sk, auxC) + C$$

[0082] **Fig.** 10 ist ein Flussdiagramm, das ein Beispiel für die Erzeugung eines geheimen Schlüssels bei der Common-Key-Kryptografie zeigt. Der Schritt zur Erzeugung des geheimen Schlüssels bei der Common-Key-Kryptographie wird anhand von **Fig.** 10 beschrieben.

(Schritt S201: Informationseingabeschritt)

[0083] Die Eingabeeinheit 201 akzeptiert als Eingabe eine Schlüsselbitlänge k.

(Schritt S202: Schritt zur Erzeugung des geheimen Schlüssels)

[0084] Die Common-Key-Kryptographie-Schlüsselerzeugungseinheit 202 erzeugt eine k-Bit-Zufallszahl und behandelt die erzeugte Zufallszahl als den geheimen Common-Key-Kryptographie-Schlüssel sk.

(Schritt S203: Lieferschritt)

[0085] Die Übertragungseinheit 203 gibt den Common-Key-Kryptographie-SchlüsselErzeugungseinheit 600 den geheimen Common-Key-Chiffretext-Geheimschlüssel-Erzeugungsvorrichtung aus.

[0086] **Fig.** 11 ist ein Flussdiagramm, das ein Beispiel für einen Parametergenerierungsschritt zeigt. Der Schritt der Parametergenerierung wird anhand von **Fig.** 11 beschrieben.

(Schritt S301: Informationseingabeschritt)

[0087] Die Eingabeeinheit 301 akzeptiert als Eingabe die Bitlänge k des Schlüssels.

(Schritt S302: Schlüsselerzeugungsschritt)

[0088] Die Gemeinsame-Parameter-Erzeugungsvorrichtung 302 führt die Einrichtung der attributbasierten Verschlüsselung aus, um jeweils den geheimen Hauptschlüssel msk und den öffentlichen Schlüssel pk zu erzeugen.

(Schritt S303: Lieferschritt)

[0089] Die Übertragungseinheit 303 überträgt den geheimer Hauptschlüssel msk und den öffentlichen Schlüssel pk nach Bedarf an die Vorrichtungen.

[0090] **Fig.** 12 ist ein Flussdiagramm, das ein Beispiel für die Erzeugung eines geheimen Benutzerschlüssels darstellt. Der Schritt der Erzeugung des geheimen Benutzerschlüssels wird anhand von **Fig.** 12 beschrieben.

(Schritt S401: Attribut-Eingabeschritt)

[0091] Die Eingabeeinheit 401 nimmt den Attributparameter Γ als Eingabe entgegen.

(Schritt S402: Hauptschlüssel-Eingabeschritt)

[0092] Die Schlüsselempfangseinheit 402 empfängt den geheimen Hauptschlüssel msk.

(Schritt S403: Schritt zur Erzeugung des geheimen Benutzerschlüssels)

[0093] Die Schlüsselerzeugungseinheit 403 führt die Erzeugung des geheimen Benutzerschlüssels KeyGen der attributbasierten Verschlüsselung mit Hilfe des Attributparameters Γ und des geheimen Hauptschlüssels msk durch, wodurch der geheime Benutzerschlüssel sk_Γ erzeugt wird.

(Schritt S404: Übertragungsschritt)

[0094] Die Schlüsselübertragungseinheit 404 überträgt den erzeugten geheimen Benutzerschlüssel sk_Γ an die Entschlüsselungsvorrichtung 800.

[0095] **Fig.** 13 ist ein Flussdiagramm, das ein Beispiel für die Erzeugung eines Common-Key-Chiffretextes darstellt. Der Schritt der Erzeugung des Common-Key-Chiffretextes wird anhand von **Fig.** 13 beschrieben.

(Schritt S501: Schlüssel-Empfangsschritt)

[0096] Die Schlüsselempfangseinheit 502 empfängt den geheimen Schlüssel sk der Common-Key-Kryptografie.

(Schritt S502: Klartext-Eingabeschritt).

[0097] Die Eingabeeinheit 501 akzeptiert den Klartext M als Eingabe.

(Schritt S503: Verschlüsselungsschritt)

[0098] Die Verschlüsselungsvorrichtung 503 führt den Blockchiffrier-Counter-Modus aus, um den Klartext M zu verschlüsseln. Die Verschlüsselungsvorrichtung 503 nimmt bei der Ausführung des Counter-Modus einen Zählerwert als Hilfsinformation auxC und den Chiffretext als Common-Key-Chiffretext skC. Eine Beziehung zwischen der Hilfsinformation auxC und dem Common-Key-Chiffretext skC wird durch [Formel 1] beschrieben. Der Common-Key-Chiffretext skC ist äquivalent zum ersten Common-Key-Chiffretext. SCTRENC ist äquivalent zur Verschlüsselung nach dem ersten Common-Key-Kryptographieschema. Der geheime Schlüssel sk der Common-Key-Kryptografie ist äquivalent zu dem ersten geheimen Schlüssel. Die Hilfsinformation auxC ist äquivalent zur ersten Hilfsinformation. Der geheime Schlüssel sk und die Hilfsinformation auxC sind äquivalent zu der ersten kryptographischen Common-Key-Information.

$$\mathrm{skC} = \mathrm{SCTRENC}(\mathrm{sk},\mathrm{auxC}) + \mathrm{M} \qquad \text{[Formel 1]}$$

(Schritt S504: Übertragungsschritt)

[0099] Die Übertragungseinheit 504 überträgt den Common-Key-Chiffretext skC und die Hilfsinformationen auxC je nach Bedarf an die einzelnen Vorrichtungen.

[0100] **Fig.** 14 ist ein Flussdiagramm, das ein Beispiel für einen Umwandlungsschlüssel-Erzeugungsschritt darstellt. Der Schritt der Erzeugung des Umwandlungsschlüssels wird anhand von **Fig.** 14 beschrieben.

(Schritt S601: Schlüssel-Empfangsschritt)

[0101] Die Schlüsselempfangseinheit 601 empfängt jeweils den öffentlichen Schlüssel pk, den geheimen Schlüssel sk und die Hilfsinformationen auxC.

(Schritt S602: Eingabeschritt)

[0102] Die Eingabeeinheit 602 akzeptiert die Entschlüsselungsbedingung L als Eingabe.

(Schritt S603: Umwandlungsziel-Einstellschritt)

[0103] Die Umwandlungsziel-Einstelleinheit 603 führt die Verschlüsselung ABEENC der attributbasierten Verschlüsselung auf der Grundlage des öffentlichen Schlüssels pk und der Entschlüsselungsbedingung L aus, wie in [Formel 2] angegeben. Es sei angemerkt, dass der Public-Key-Chiffretext P ein Public-Key-Chiffretext nach Umwandlung ist und dass der Schlüssel K ein Schlüssel ist, mit dem der Public-Key-Chiffretext P verschlüsselt wird. Der Public-Key-Chiffretext P ist äquivalent zum attributbasierten Chiffretext. Der Schlüssel K ist gleichbedeutend mit dem attributbasierten Verschlüsselungsschlüssel.

$$(\mathrm{K},\mathrm{P}) = \mathrm{ABEENC}(\mathrm{pk},\mathrm{L}) \qquad \text{[Formel 2]}$$

(Schritt S604: Common-Key-Schritt zur Erzeugung geheimer Schlüssel)

[0104] Die Umwandlungsschlüssel-Erzeugungseinheit 604 wählt einen neuen Common-Key-Kryptographie-Geheimschlüssel sk' aus.

(Schritt S605: Common-Key-Geheimschlüssel-Verschlüsselungsschritt)

[0105] Die Umwandlungsschlüssel-Erzeugungseinheit 604 nimmt den Common-Key-Kryptographie-Schlüssel sk' als Klartext und den Schlüssel K als geheimen Schlüssel und führt die Common-Key-Verschlüsselung gemäß [Formel 3] durch. Man beachte, dass S1 dem dritten Common-Key-Chiffretext entspricht, SKEENC der Verschlüsselung nach dem zweiten Common-Key-Kryptographieschema und sk' dem zweiten geheimen Schlüssel entspricht.

$$S1 = \mathrm{SKEENC}(K, sk') \qquad \text{[Formel 3]}$$

(Schritt S606: Umwandlungsschlüssel-Erzeugungsschritt)

[0106] Die Umwandlungsschlüssel-Erzeugungseinheit 604 wählt eine neue Hilfsinformation auxC' aus und führt die in [Formel 4] angegebene Berechnung unter Verwendung der ausgewählten neuen Hilfsinformation auxC' durch. Die Hilfsinformation auxC' ist gleichbedeutend mit der zweiten Hilfsinformation. Der geheime Schlüssel sk' der Common-Key-Kryptographie und die Hilfsinformation auxC' entsprechen der zweiten kryptographischen Common-Key-Information.

$$S2 = \mathrm{SCTRENC}(sk, auxC) + \mathrm{SCTRENC}(sk', auxC') \qquad \text{[0066] [Formel 4]}$$

$$S = (S1, S2)$$

[0067] (Schritt S607: Lieferschritt)

[0107] Die Übertragungseinheit 605 gibt den Umwandlungsschlüssel ck (= (P, S)) an die Umwandlungsvorrichtung 700 aus.

[0108] **Fig.** 15 ist ein Flussdiagramm, das ein Beispiel für einen Umwandlungsschritt darstellt. Der Umwandlungsschritt wird anhand von **Fig.** 15 beschrieben.

(Schritt S701: Schlüssel-Empfangsschritt)

[0109] Die Schlüsselempfangseinheit 701 empfängt den öffentlichen Schlüssel pk und den Umwandlungsschlüssel ck (= (P, S (= (S1, S2)))).

(Schritt S702: Eingabeschritt)

[0110] Die Chiffretext-Empfangseinheit 702 empfängt den Common-Key-Chiffretext skC.

(Schritt S703: Konvertierungsschritt)

[0111] Die Umwandlungseinheit 703 führt eine in [Formel 5] angegebene Berechnung unter Verwendung des Common-Key-Chiffretextes skC und S2 durch. Der Common-Key-Chiffretext skC' nach Umwandlung ist äquivalent zum zweiten Common-Key-Chiffretext. Man beachte, dass S2 nach dem ersten Common-Key-Kryptographieschema erzeugt wird. Da der Common-Key-Chiffretext skC' nach Umwandlung ein exklusives ODER des Common-Key-Chiffretextes skC und S2 ist, entspricht der Common-Key-Chiffretext skC' nach Umwandlung dem ersten Common-Key-Kryptographieschema.

$$skC' = skC + S2 \qquad \text{[Formel 5]}$$

[0112] Es ist zu beachten, dass eine rechte Seite von [Formel 5] eine durch [Formel 6] angegebene Natur hat.

$$skC + S2$$
$$= SCTRENC(sk,auxC) + M + SCTRENC(sk,auxC) + SCTRENC(sk',auxC') \quad \text{[Formel 6]}$$
$$= SCTRENC(sk',auxC') + M$$

(Schritt S704: Ausgabeschritt)

[0113] Die Übertragungseinheit 704 gibt den Public-Key-Chiffretext nach Umwandlung an die Entschlüsselungsvorrichtung 800 als pkC (= (P, S1)) und den Common-Key-Chiffretext nach Umwandlung an die Entschlüsselungsvorrichtung 800 als (skC', auxC') aus.

[0114] **Fig.** 16 ist ein Flussdiagramm, das ein Beispiel für einen Entschlüsselungsschritt darstellt. Der Schritt des Entschlüsselns wird anhand von **Fig.** 16 beschrieben.

(Schritt S801: Chiffretext-Empfangsschritt)

[0115] Die Chiffretext-Empfangseinheit 801 empfängt den Public-Key-Chiffretext nach Umwandlung pkC (= (P, S1)) und den Common-Key-Chiffretext nach Umwandlung (skC', auxC').

(Schritt S802: Eingabeschritt)

[0116] Die Schlüsselempfangseinheit 802 empfängt den geheimen Benutzerschlüssel sk_Γ. Der geheime Benutzerschlüssel sk_Γ entspricht dem geheimen Benutzerschlüssel, der mit den Attributinformationen übereinstimmt, die dem attributbasierten Verschlüsselungsschlüssel entsprechen.

(Schritt S803: Entschlüsselungs-Verarbeitungsschritt)

[0117] Die Entschlüsselungseinheit 803 führt die in [Formel 7] angegebenen Berechnungen unter Verwendung der empfangenen Daten sequentiell von oben nach unten durch und entschlüsselt so den Klartext M. In [Formel 7] wird zunächst eine Entschlüsselung der attributbasierten Verschlüsselung durchgeführt, so dass der Schlüssel K entschlüsselt wird. In [Formel 7] sind die Formeln, die den Klartext M entschlüsseln, Formeln, die aus [Formel 5] und [Formel 6] stammen. Der Klartext M ist ein Klartext, der dem zweiten Common-Key-Chiffretext entspricht.

$$K = ABEDEC(sk_\Gamma, P) \quad \text{[0080] [Formel 7]}$$

$$sk' = SKEDEC(K,S1)$$

$$M = skC' + SCTRENC(sk',auxC')$$

[0081] (Schritt S804: Ausgabeschritt)

[0118] Die Ergebnisausgabeeinheit 804 gibt den Klartext M aus. In einem konkreten Beispiel gibt die Ergebnisausgabeeinheit 804 den Klartext M auf einer Anzeige aus, die der Entschlüsselungsvorrichtung 800 zur Verfügung steht.

[0082] *** Beschreibung der Wirkung der Ausführungsform 1***

[0119] Wie oben beschrieben, kann ein Benutzer gemäß der vorliegenden Ausführungsform eine Summe innerer Produkte nur dann berechnen, wenn ein Entschlüsselungsschlüssel mit Hilfe eines Entschlüsselungs-Tokens erworben wird, selbst wenn der Benutzer über einen geheimen Benutzerschlüssel verfügt. Daher ist die Information eines Vektors x in Verbindung mit einzelnen Chiffretexten im Stand der Technik nicht einfach zu analogisieren. Daher kann das Chiffretext-Umwandlungssystem 100 gemäß der vorliegenden Ausführungsform wesentlich sicherer realisiert werden.

[0120] Außerdem kann ein durch das Common-Key-Kryptographieschema verschlüsselter Chiffretext in einen auf dem Public-Key-Kryptographieschema basierenden Chiffretext umgewandelt werden, ohne dass der Chiffretext durch ein beliebiges Schema wie das Public-Key-Kryptographieschema, ein funktionales Kryptographieschema, mit dem ein Zugriffsbereich festgelegt werden kann, und das attributbasierte Verschlüsselungsschema entschlüsselt werden muss. Daher kann gemäß der vorliegenden Ausführungsform beispiels-

weise die Umwandlung eines durch das Common-Key-Kryptographieschema verschlüsselten Chiffretextes in einen auf dem Public-Key-Kryptographieschema basierenden Chiffretext, die Übermittlung des umgewandelten Chiffretextes usw. unter Verwendung einer ressourcensparenden Vorrichtung durchgeführt werden, die keine Berechnung der Public-Key-Verschlüsselung ausführen kann, was zu einer Verbesserung des Komforts führt.

[0083] *** Andere Konfigurationen ***

< Modifikation 1 >

[0121] Fig. 17 zeigt ein Beispiel für die Hardwarekonfiguration jeder Vorrichtung, mit der ein Chiffretext-Umwandlungssystem 100 gemäß der vorliegenden Änderung ausgestattet ist.

[0122] Jede Vorrichtung des Chiffretext-Umwandlungssystems 100 ist mit einer Verarbeitungsschaltung 18 anstelle eines Prozessors 11, eines Prozessors 11 und eines ROM 13, eines Prozessors 11 und eines RAM 14 oder eines Prozessors 11, eines ROM 13 und eines RAM 14 ausgestattet.

[0123] Bei der Verarbeitungsschaltung 18 handelt es sich um Hardware, die zumindest einige der Einheiten implementiert, mit denen jede Vorrichtung des Chiffretext-Umwandlungssystems 100 ausgestattet ist.

[0124] Bei der Verarbeitungsschaltung 18 kann es sich um dedizierte Hardware oder einen Prozessor handeln, der ein im ROM 13 oder im RAM 14 gespeichertes Programm ausführt.

[0125] Handelt es sich bei der Verarbeitungsschaltung 18 um dedizierte Hardware, so ist die Verarbeitungsschaltung 18 in einem spezifischen Beispiel eine aus oder durch eine Kombination von einer einzelnen Schaltung, einer zusammengesetzten Schaltung, einem programmierten Prozessor, einem parallel programmierten Prozessor, einer anwendungsspezifischen integrierten Schaltung (ASIC) und einem Field Programmable Gate Array (FPGA).

[0126] Jede Vorrichtung, mit der das Chiffretext-Umwandlungssystem 100 ausgestattet ist, kann mit einer Vielzahl von Verarbeitungsschaltungen versehen sein, die die Verarbeitungsschaltung 18 ersetzen. Die Vielzahl von Verarbeitungsschaltungen teilen sich die Funktionen der Verarbeitungsschaltung 18.

[0127] In jeder Vorrichtung, mit der das Chiffretext-Umwandlungssystem 100 ausgestattet ist, können einige Funktionen durch spezielle Hardware implementiert werden, während die übrigen Funktionen durch Software oder Firmware implementiert werden können.

[0128] In einem bestimmten Beispiel wird die Verarbeitungsschaltung 18 durch eine der folgenden Komponenten oder durch eine Kombination aus Hardware, Software und Firmware implementiert.

[0129] Der Prozessor 11, das ROM 13, das RAM 14 und die Verarbeitungsschaltung 18 werden zusammen als „Verarbeitungsschaltung“ bezeichnet. Das heißt, eine Funktion jedes funktionsbestimmenden Elements jeder Vorrichtung, mit der das Chiffretext-Umwandlungssystem 100 ausgestattet ist, wird durch einen Verarbeitungsschaltkreis realisiert.

*** Weitere Ausführungsformen ***

[0130] Nach der Beschreibung von Ausführungsform 1 kann eine Vielzahl von Teilen der vorliegenden Ausführungsform durch Kombination ausgeführt werden. Alternativ kann die vorliegende Ausführungsform auch in Teilen umgesetzt werden. An der vorliegenden Ausführungsform können nach Bedarf verschiedene Änderungen vorgenommen werden. Die vorliegende Ausführungsform kann als Ganzes oder teilweise durch eine beliebige Kombination umgesetzt werden. Jede in der vorliegenden Spezifikation beschriebene Einheit kann durch eine der folgenden Komponenten oder durch eine Kombination aus Firmware, Software und Hardware implementiert werden.

[0131] Die oben beschriebene Ausführungsform ist ein im Wesentlichen bevorzugtes Beispiel und soll die vorliegende Offenbarung, ein Anwendungsprodukt der vorliegenden Offenbarung und einen Anwendungsbereich der vorliegenden Offenbarung nicht einschränken. Die mit Hilfe von Flussdiagrammen oder ähnlichem beschriebenen Verfahren können bei Bedarf geändert werden.

BEZUGSZEICHENLISTE

[0132] 11: Prozessor; 12: Bus; 13: ROM; 14: RAM; 15: Kommunikationsplatine; 18: Verarbeitungsschaltung; 20: Magnetplattenvorrichtung; 21: Betriebssystem; 22: Programme; 23: Dateien; 51: Anzeige; 52: Tastatur; 53: Maus; 54: Laufwerk; 100: Chiffretext-Umwandlungssystem; 101: Netzwerk; 200: Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtung; 201: Eingabeeinheit; 202: Common-Key-Kryptographie-Schlüsselerzeugungseinheit; 203: Übertragungseinheit; 290: Common-Key-Kryptographie-Geheimschlüssel-Erzeugungsvorrichtungsgruppe; 300: Parametererzeugungsvorrichtung; 301: Eingabeeinheit; 302: Gemeinsame-Parameter-Erzeugungsvorrichtung; 303: Übertragungseinheit; 400: Benutzergeheimschlüssel-Erzeugungsvorrichtung; 401: Eingabeeinheit; 402: Schlüsselempfangseinheit; 403: Schlüsselerzeugungseinheit; 404: Schlüsselübertragungseinheit; 490: Benutzergeheimschlüssel-Erzeugungsvorrichtungsgruppe; 500: Common-Key-Chiffretext-Erzeugungsvorrichtung; 501: Eingabeeinheit; 502: Schlüsselempfangseinheit; 503: Verschlüsselungsvorrichtung; 504: Übertragungseinheit; 600: Umwandlungsschlüssel-Erzeugungsvorrichtung; 601: Schlüsselempfangseinheit; 602: Eingabeeinheit; 603: Umwandlungsziel-Einstelleinheit; 604: Umwandlungsschlüssel-Erzeugungseinheit; 605: Übertragungseinheit; 700: Umwandlungsvorrichtung; 701: Schlüsselempfangseinheit; 702: Chiffretext-Empfangseinheit; 703: Umwandlungseinheit; 704: Übertragungseinheit; 800: Entschlüsselungsvorrichtung; 801: Chiffretext-Empfangseinheit; 802: Schlüsselempfangseinheit; 803: Entschlüsselungseinheit; 804: Ergebnisausgabeeinheit; auxC, auxC': Hilfsinformationen; K: Schlüssel; L: Entschlüsselungsbedingung; M: Klartext; P: Public-Key-Chiffretext; ck: Umwandlungsschlüssel; pk: öffentlicher Schlüssel; pkC: Public-Key-Chiffretext nach Umwandlung; msk: geheimer Hauptschlüssel; sk, sk': Common-Key-Kryptographie-Geheimschlüssel; skC: Common-Key-Chiffretext; skC': Common-Key-Chiffretext nach Umwandlung; sk_Γ: geheimer Benutzerschlüssel; Γ: Attributparameter.

Patentansprüche

1. Chiffretext-Umwandlungssystem (100), umfassend:
eine Umwandlungsschlüssel-Erzeugungsvorrichtung (600), umfassend
eine Umwandlungsziel-Einstelleinheit (603) zum Erzeugen eines attributbasierten Verschlüsselungsschlüssels und eines attributbasierten Chiffretextes, der mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird, gemäß einem attributbasierten Verschlüsselungsschema; und
eine Umwandlungsschlüssel-Erzeugungseinheit (604)
zum Erzeugen eines Umwandlungsschlüssels, der einen ersten Common-Key-Chiffretext in einen zweiten Common-Key-Chiffretext umwandelt, der ein Chiffretext ist, der mit einem ersten Common-Key-Kryptographieschema übereinstimmt und der sich von dem ersten Common-Key-Chiffretext unterscheidet, auf der Grundlage einer ersten kryptographischen Common-Key-Information, die beim Erzeugen des ersten Common-Key-Chiffretextes verwendet wird, durch Verschlüsseln eines Klartextes mit einem ersten geheimen Schlüssel gemäß dem ersten Common-Key-Kryptographieschema, und
zum Erzeugen eines dritten Common-Key-Chiffretextes gemäß einem zweiten Common-Key-Kryptographieschema zu erzeugen, indem ein zweiter geheimer Schlüssel, der zum Entschlüsseln des zweiten Common-Key-Chiffretextes verwendet wird, mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird.

2. Chiffretext-Umwandlungssystem (100) nach Anspruch 1, wobei das erste Common-Key-Kryptographieschema ein Blockchiffrier-Counter-Mode-Schema ist.

3. Chiffretext-Umwandlungssystem (100) nach Anspruch 2, wobei die erste kryptographische Common-Key-Information aus dem ersten geheimen Schlüssel und einer ersten Hilfsinformation besteht, die bei der Verschlüsselung nach dem Blockchiffrier-Counter-Mode-Schema verwendet wird.

4. Chiffretext-Umwandlungssystem (100) nach Anspruch 3, wobei die Umwandlungsschlüssel-Erzeugungseinheit (604) den Umwandlungsschlüssel unter Verwendung der ersten kryptographischen Common-Key-Information und der zweiten kryptographischen Common-Key-Information erzeugt, die aus dem zweiten geheimen Schlüssel und der zweiten Hilfsinformation besteht, die bei der Verschlüsselung nach dem Blockchiffrier-Counter-Mode-Schema verwendet werden.

5. Chiffretext-Umwandlungssystem (100) nach Anspruch 4, wobei die Umwandlungsschlüssel-Erzeugungseinheit (604) als den Umwandlungsschlüssel ein exklusives ODER eines Ergebnisses der Ausführung des ersten Common-Key-Kryptographieschemas unter Verwendung der ersten kryptographischen Common-Key-Information und eines Ergebnisses der Ausführung des ersten Common-Key-Kryptographieschemas unter Verwendung der zweiten kryptographischen Common-Key-Information berechnet.

6. Chiffretext-Umwandlungssystem (100) nach Anspruch 4 oder 5, ferner umfassend:
eine Entschlüsselungseinrichtung (800), umfassend:
eine Entschlüsselungseinheit (803)
zum Entschlüsseln des attributbasierten Chiffretextes mit Hilfe eines geheimen Benutzerschlüssels zu entschlüsseln, der mit den Attributinformationen übereinstimmt, die dem attributbasierten Verschlüsselungsschlüssel entsprechen, wodurch der attributbasierte Verschlüsselungsschlüssel erhalten wird,
zum Entschlüsseln des dritten Common-Key-Chiffretextes unter Verwendung des erworbenen attributbasierten Verschlüsselungsschlüssels, wodurch der zweite geheime Schlüssel erhalten wird, und
zum Finden, als den Klartext, eines exklusiven ODER eines Ergebnisses der Verschlüsselung der zweiten Hilfsinformation mit dem zweiten geheimen Schlüssel und des zweiten Common-Key-Chiffretextes.

7. Chiffretext-Umwandlungssystem (100) nach einem der Ansprüche 1 bis 6, ferner umfassend:
eine Umwandlungsvorrichtung (700) umfassend
eine Umwandlungseinheit (703), um als den zweiten Common-Key-Chiffretext ein exklusives ODER des ersten Common-Key-Chiffretext und des Umwandlungsschlüssels zu berechnen.

8. Verfahren zur Erzeugung eines Umwandlungsschlüssels, umfassend:
Erzeugen, durch einen Computer, eines attributbasierten Verschlüsselungsschlüssels und eines attributbasierten Chiffretextes, der mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird, gemäß einem attributbasierten Verschlüsselungsschema;
Erzeugen, durch den Computer, eines Umwandlungsschlüssels, der einen ersten Common-Key-Chiffretext in einen zweiten Common-Key-Chiffretext umwandelt, der ein Chiffretext ist, der mit einem ersten Common-Key-Kryptographieschema übereinstimmt und der sich von dem ersten Common-Key-Chiffretext unterscheidet, auf der Grundlage einer ersten kryptographischen Common-Key-Information, die beim Erzeugen des ersten Common-Key-Chiffretextes verwendet wird, durch Verschlüsseln eines Klartextes mit einem ersten geheimen Schlüssel gemäß dem ersten Common-Key-Kryptographieschema; und
Erzeugen, durch den Computer, eines dritten Common-Key-Chiffretextes gemäß einem zweiten Common-Key-Kryptographieschema zu erzeugen, indem ein zweiter geheimer Schlüssel, der zum Entschlüsseln des zweiten Common-Key-Chiffretextes verwendet wird, mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird.

9. Konvertierungsschlüssel-Erzeugungsprogramm, das eine Umwandlungsschlüssel-Erzeugungsvorrichtung (600), die ein Computer ist, dazu veranlasst:
einen Umwandlungsziel-Einstellprozess zum Erzeugen eines attributbasierten Verschlüsselungsschlüssels und eines attributbasierten Chiffretextes, der mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird, gemäß einem attributbasierten Verschlüsselungsschema; und
einen Umwandlungsschlüssel-Erzeugungsprozess des
Erzeugens eines Umwandlungsschlüssels, der einen ersten Common-Key-Chiffretext in einen zweiten Common-Key-Chiffretext umwandelt, der ein Chiffretext ist, der mit dem ersten Common-Key-Kryptographieschema übereinstimmt und der sich von dem ersten Common-Key-Chiffretext unterscheidet, auf der Grundlage einer ersten kryptographischen Common-Key-Information, die beim Erzeugen des ersten Common-Key-Chiffretextes verwendet wird, durch Verschlüsseln eines Klartextes mit einem ersten geheimen Schlüssel gemäß einem ersten Common-Key-Kryptographieschema; und
Erzeugens eines dritten Common-Key-Chiffretextes gemäß einem zweiten Common-Key-Kryptographieschema zu erzeugen, indem ein zweiter geheimer Schlüssel, der zum Entschlüsseln des zweiten Common-Key-Chiffretextes verwendet wird, mit dem attributbasierten Verschlüsselungsschlüssel verschlüsselt wird.

Es folgen 17 Seiten Zeichnungen

Anhängende Zeichnungen

Fig. 1

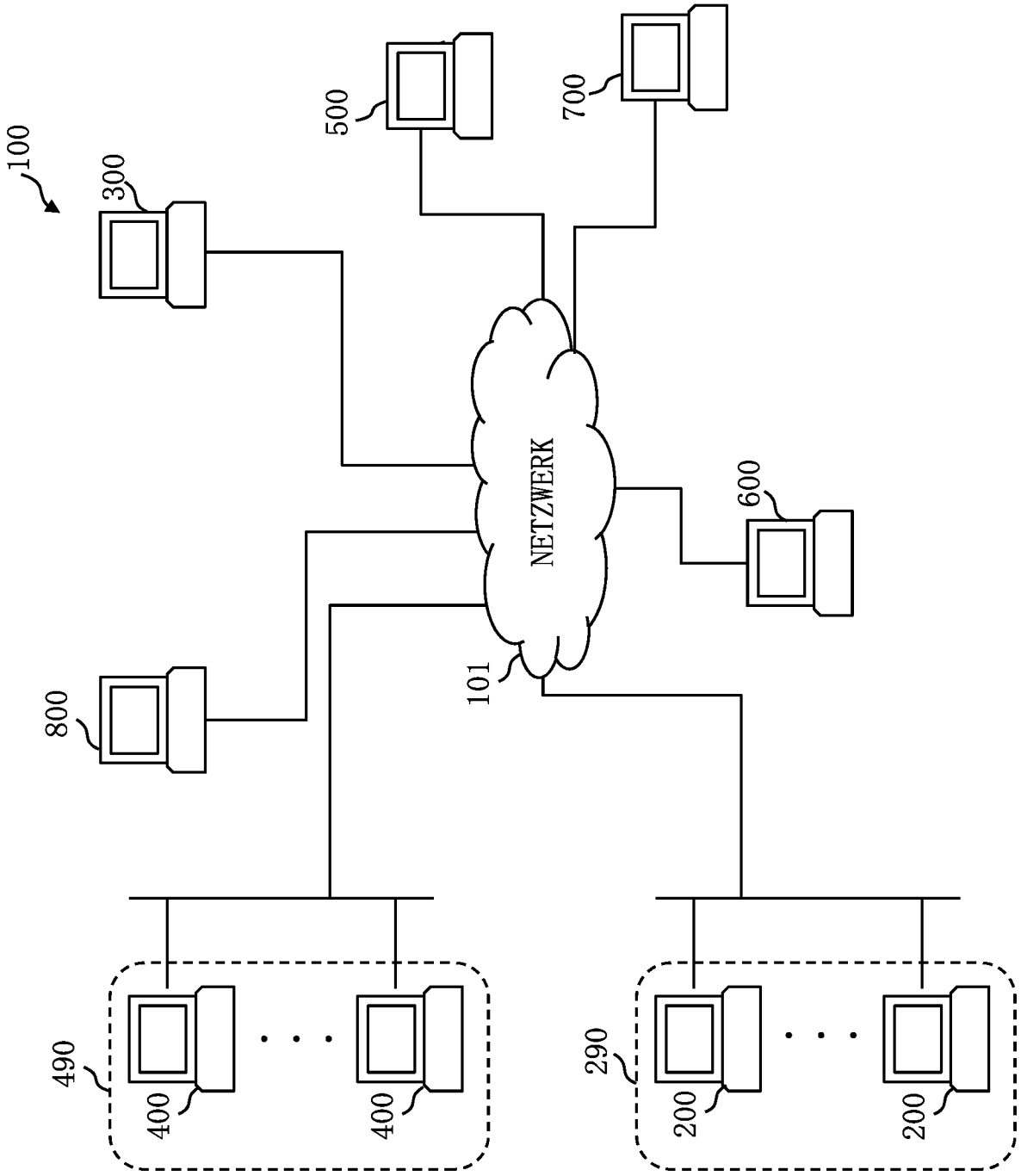


Fig. 2

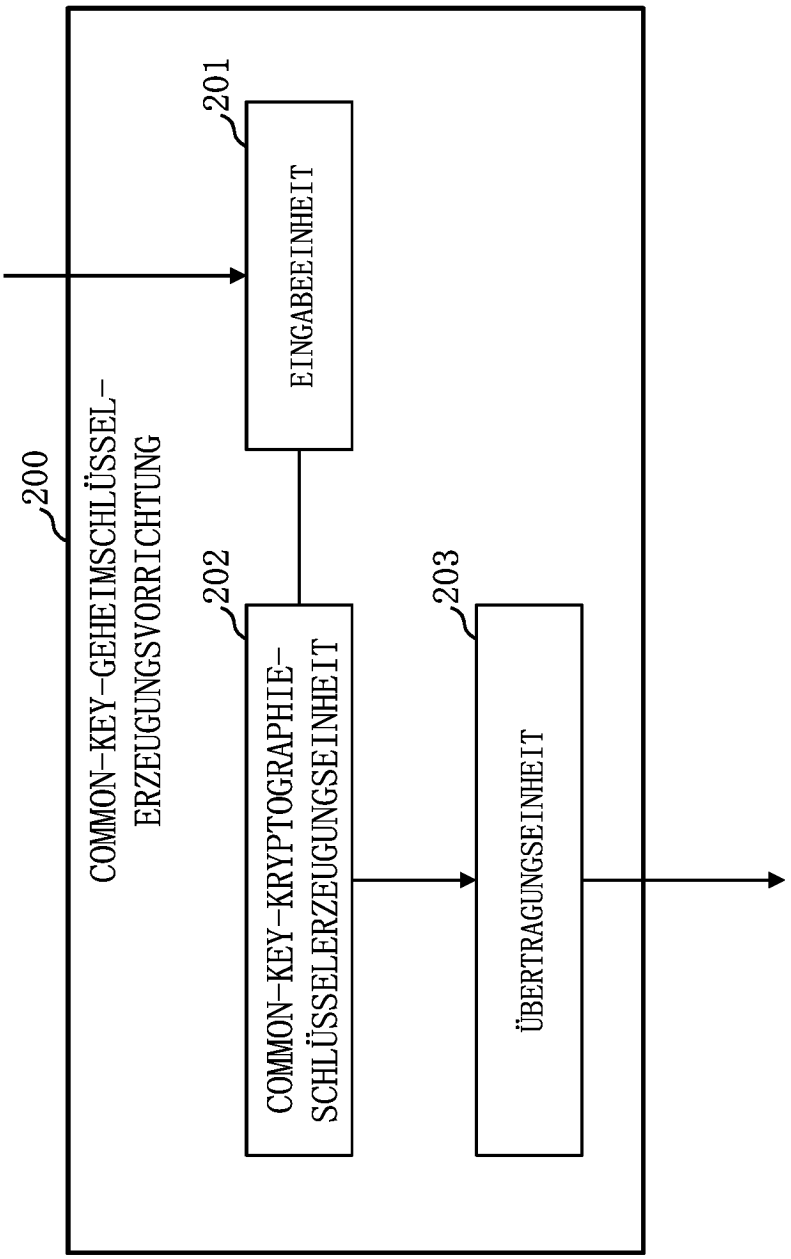

200
COMMON-KEY-GEHEIMSCHLÜSSEL-ERZEUGUNGSVORRICHTUNG
201
EINGABEEINHEIT
202
COMMON-KEY-KRYPTOGRAPHIE-SCHLÜSSELERZEUGUNGSEINHEIT
203
ÜBERTRAGUNGSEINHEIT

Fig. 3

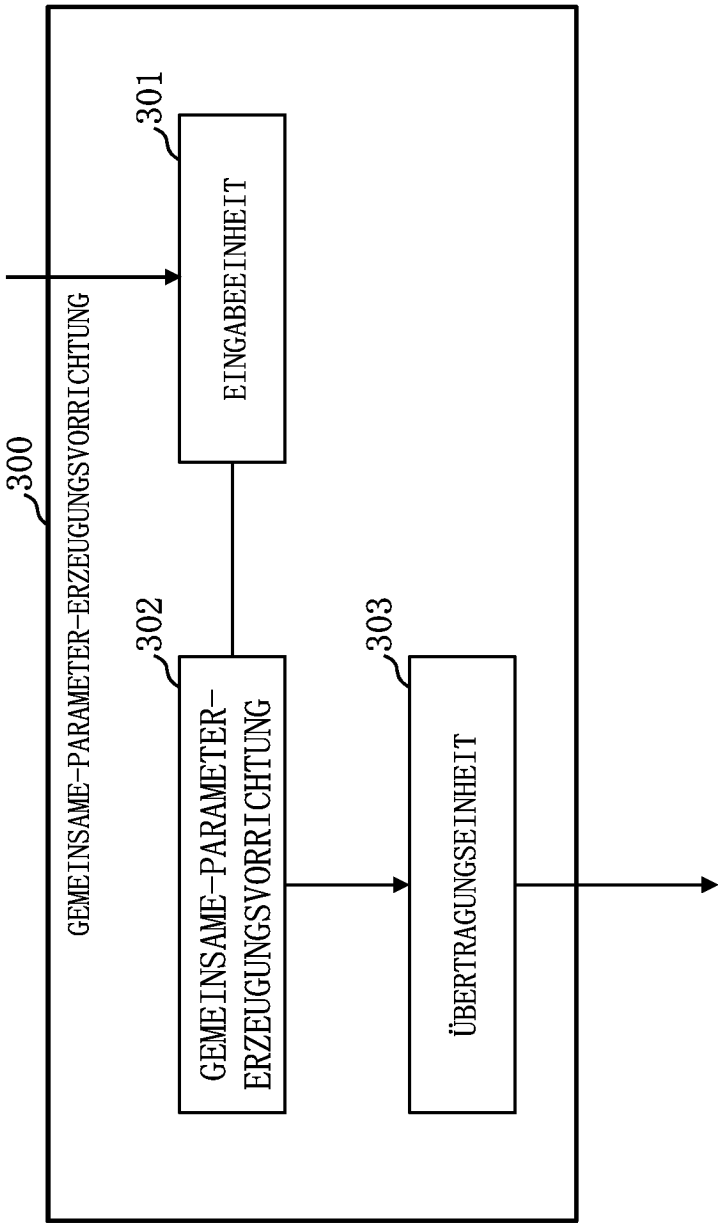

300
GEMEINSAME-PARAMETER-ERZEUGUNGSVORRICHTUNG
301
EINGABEEINHEIT
302
GEMEINSAME-PARAMETER-ERZEUGUNGSVORRICHTUNG
303
ÜBERTRAGUNGSEINHEIT

Fig. 4

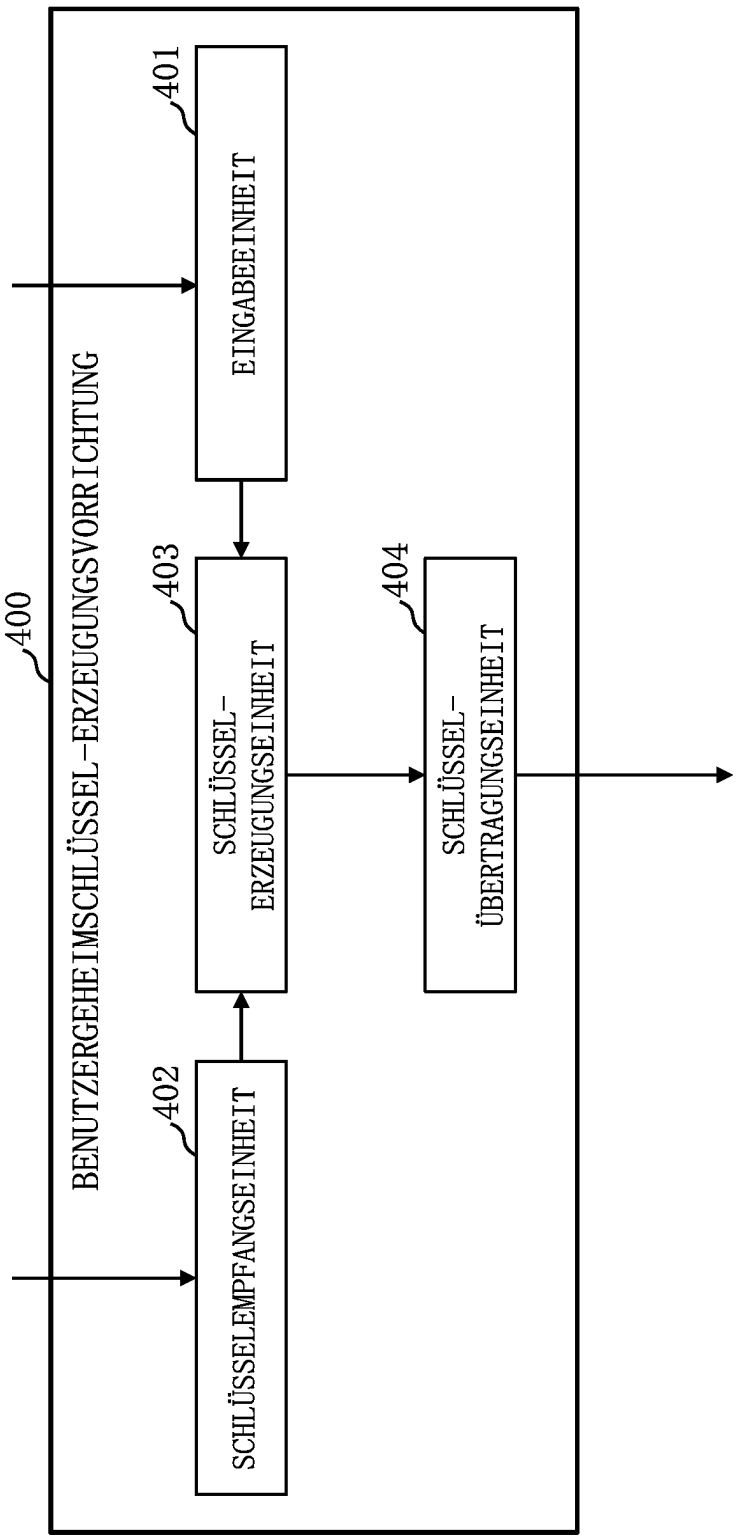

400
BENUTZERGEHEIMSCHLÜSSEL-ERZEUGUNGSVORRICHTUNG
401
EINGABEEINHEIT
402
SCHLÜSSELEMPFANGSEINHEIT
403
SCHLÜSSEL-ERZEUGUNGSEINHEIT
404
SCHLÜSSEL-ÜBERTRAGUNGSEINHEIT

Fig. 5

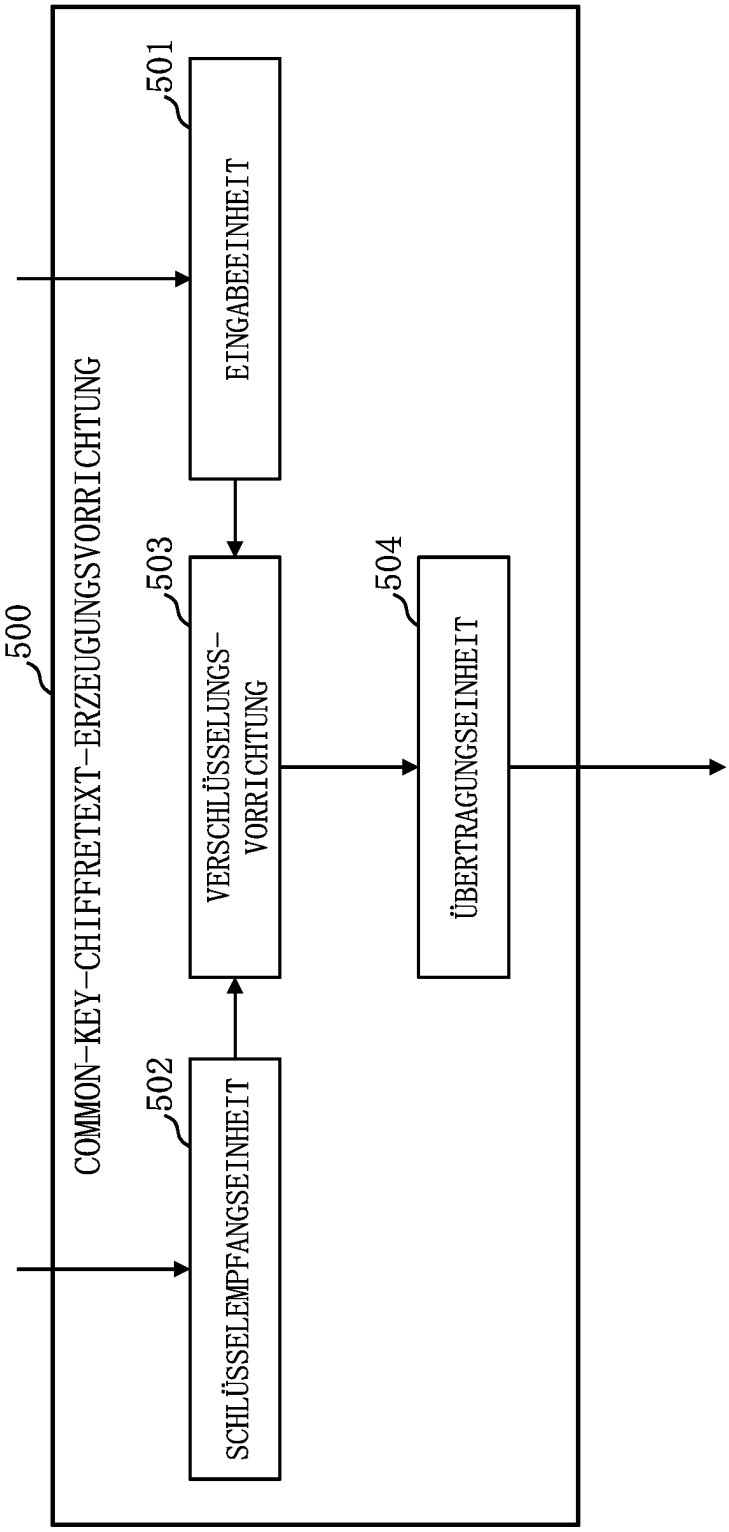

500
COMMON-KEY-CHIFFRETEXT-ERZEUGUNGSVORRICHTUNG
501
EINGABEEINHEIT
502
SCHLÜSSELEMPFANGSEINHEIT
503
VERSCHLÜSSELUNGS-VORRICHTUNG
504
ÜBERTRAGUNGSEINHEIT

Fig. 6

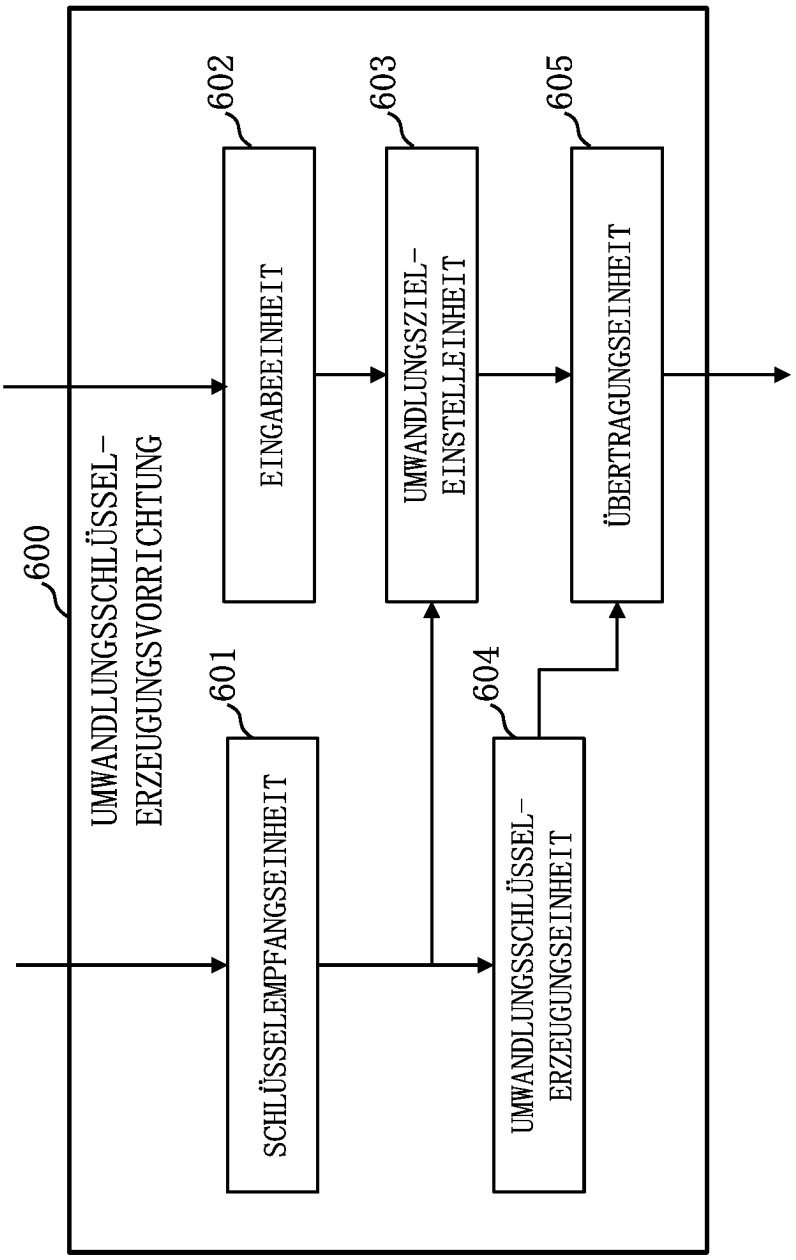

600
UMWANDLUNGSSCHLÜSSEL-ERZEUGUNGSVORRICHTUNG
601
SCHLÜSSELEMPFANGSEINHEIT
602
EINGABEEINHEIT
603
UMWANDLUNGSZIEL-EINSTELLEINHEIT
604
UMWANDLUNGSSCHLÜSSEL-ERZEUGUNGSEINHEIT
605
ÜBERTRAGUNGSEINHEIT

Fig. 7

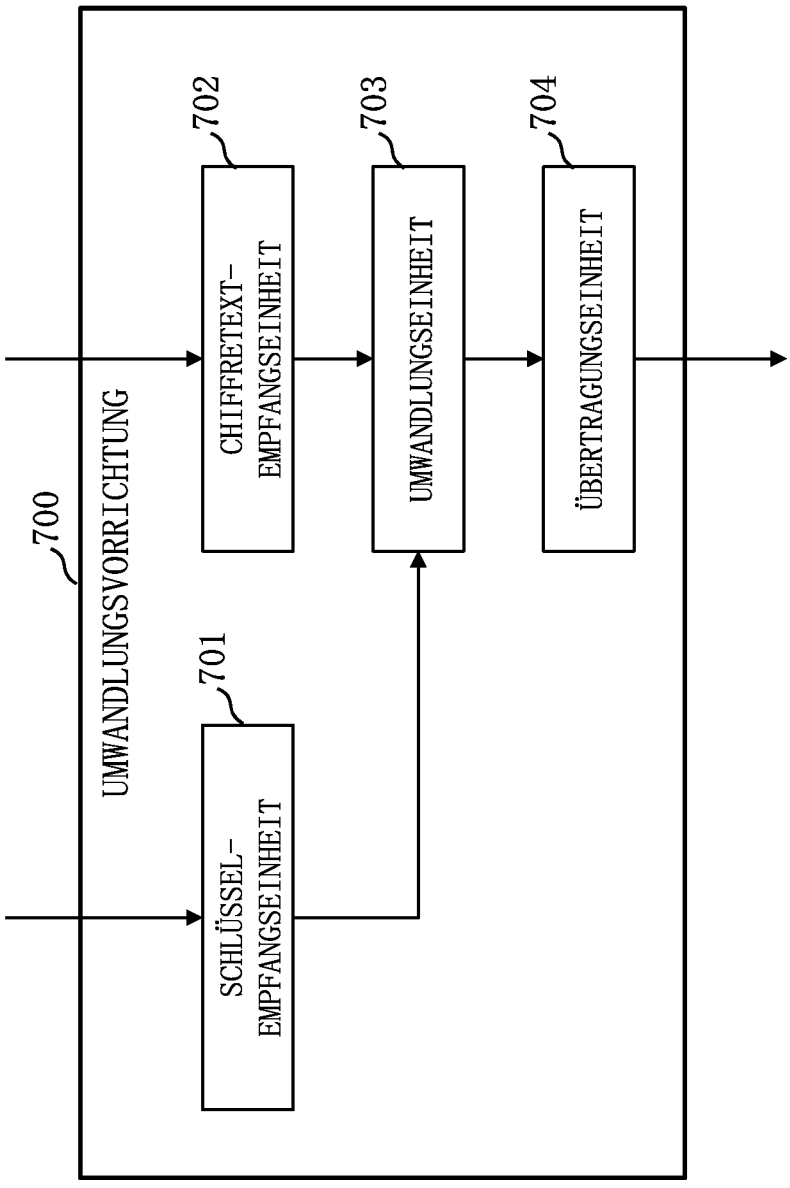

700
UMWANDLUNGSVORRICHTUNG
701
SCHLÜSSEL-EMPFANGSEINHEIT
702
CHIFFRETEXT-EMPFANGSEINHEIT
703
UMWANDLUNGSEINHEIT
704
ÜBERTRAGUNGSEINHEIT

Fig. 8

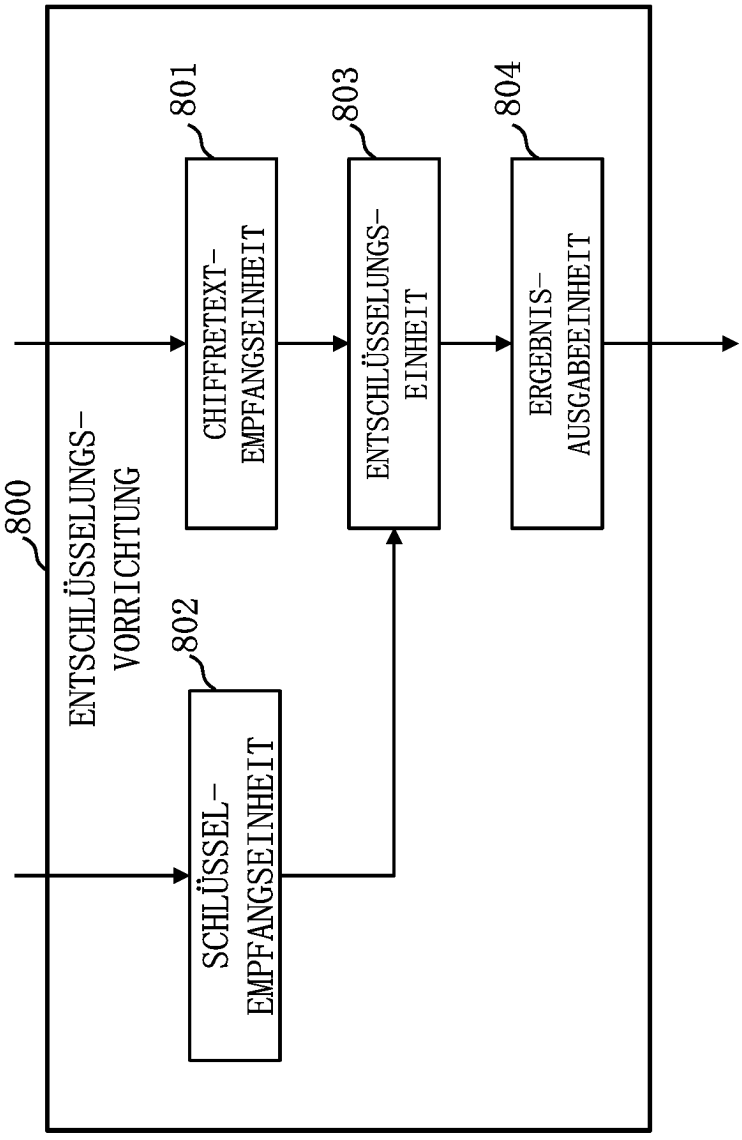

800
ENTSCHLÜSSELUNGS-
VORRICHTUNG
801
CHIFFRETEXT-
EMPFANGSEINHEIT
802
SCHLÜSSEL-
EMPFANGSEINHEIT
803
ENTSCHLÜSSELUNGS-
EINHEIT
804
ERGEBNIS-
AUSGABEEINHEIT

Fig. 9

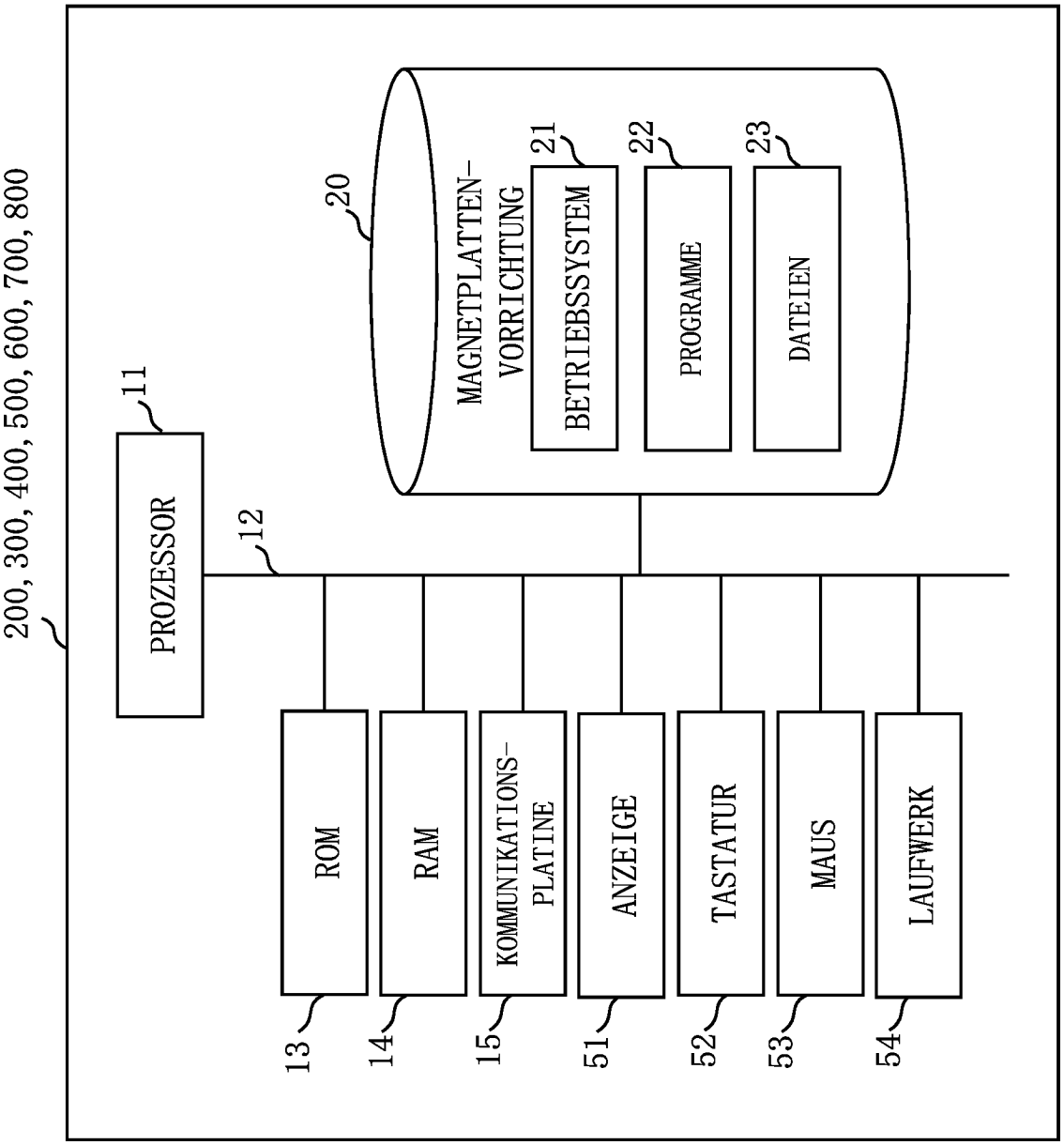

200, 300, 400, 500, 600, 700, 800
PROZESSOR
11
12
20
MAGNETPLATTEN-VORRICHTUNG
21
BETRIEBSSYSTEM
22
PROGRAMME
23
DATEIEN
ROM
RAM
KOMMUNIKATIONS-PLATINE
ANZEIGE
TASTATUR
MAUS
LAUFWERK
13
14
15
51
52
53
54

Fig. 10

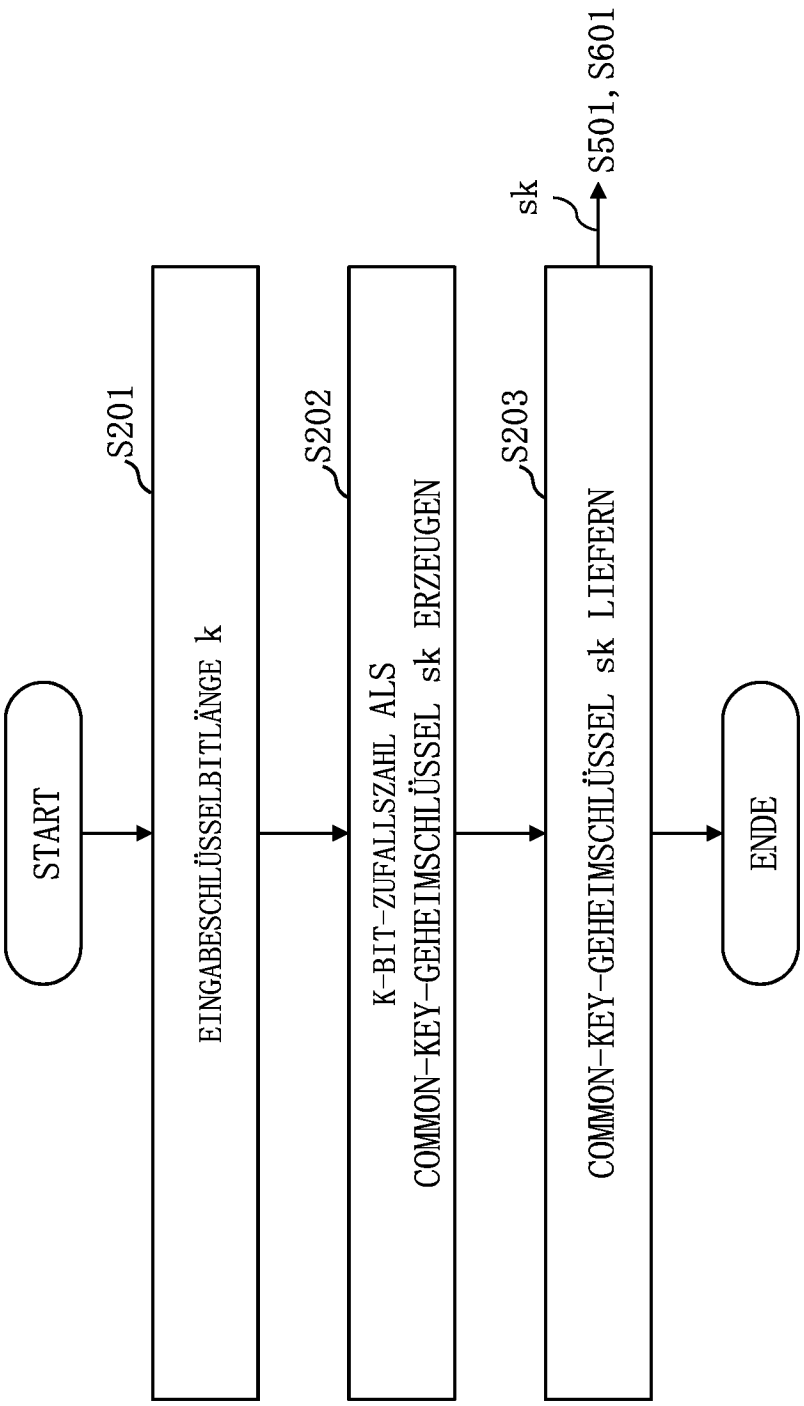

START
S201
EINGABESCHLÜSSELBITLÄNGE k
S202
K-BIT-ZUFALLSZAHL ALS
COMMON-KEY-GEHEIMSCHLÜSSEL sk ERZEUGEN
S203
COMMON-KEY-GEHEIMSCHLÜSSEL sk LIEFERN
sk
S501, S601
ENDE

Fig. 11

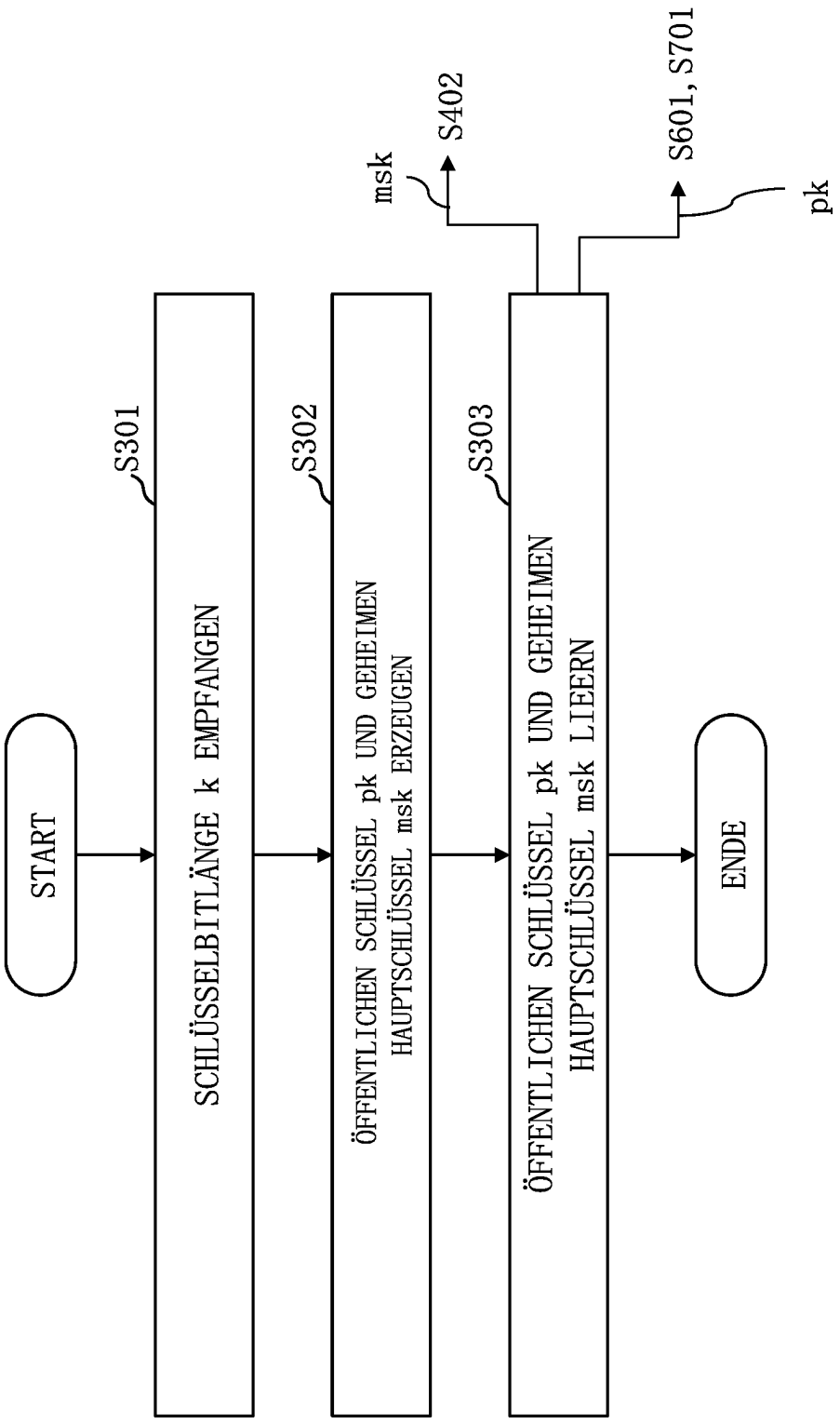

START
S301
SCHLÜSSELBITLÄNGE k EMPFANGEN
S302
ÖFFENTLICHEN SCHLÜSSEL pk UND GEHEIMEN HAUPTSCHLÜSSEL msk ERZEUGEN
S303
ÖFFENTLICHEN SCHLÜSSEL pk UND GEHEIMEN HAUPTSCHLÜSSEL msk LEERN
ENDE
msk
S402
S601, S701
pk

Fig. 12

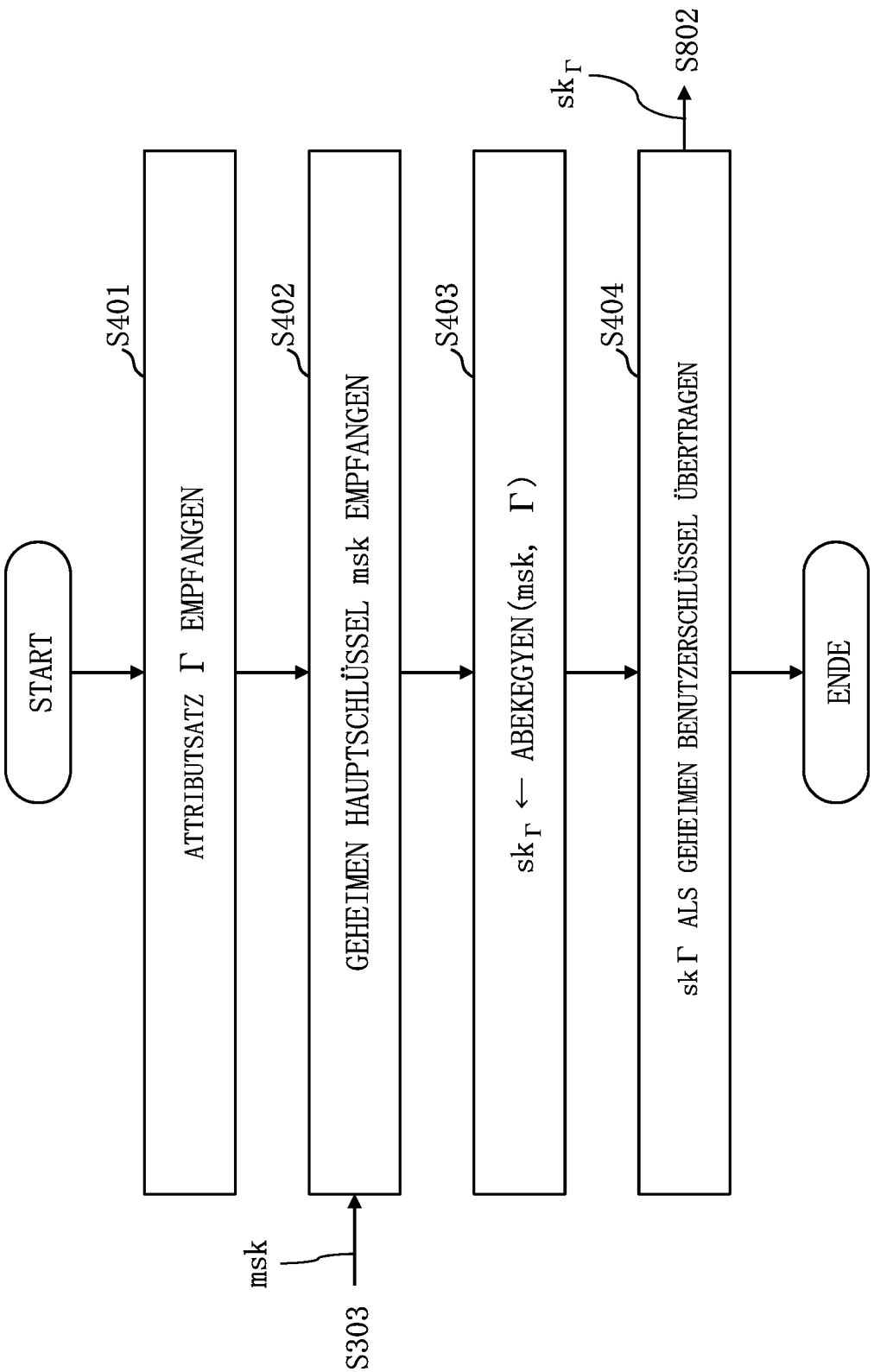

START
S401
ATTRIBUTSATZ Γ EMPFANGEN
S402
GEHEIMEN HAUPTSCHLÜSSEL msk EMPFANGEN
S303
msk
S403
$sk_\Gamma \leftarrow$ ABEKEGYEN(msk, Γ)
S404
sk_Γ
S802
sk Γ ALS GEHEIMEN BENUTZERSCHLÜSSEL ÜBERTRAGEN
ENDE

Fig. 13

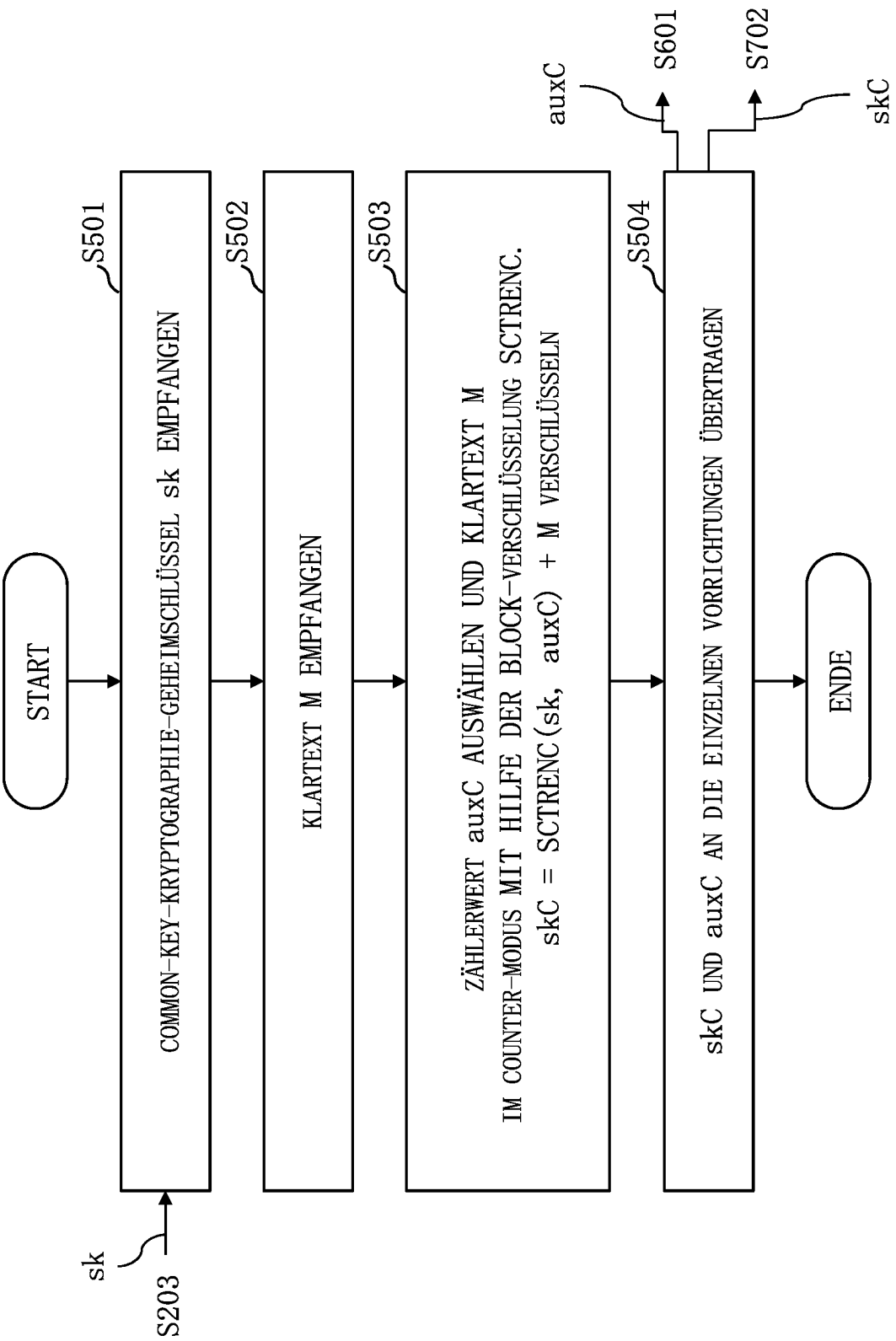

START
S501
COMMON-KEY-KRYPTOGRAPHIE-GEHEIMSCHLÜSSEL sk EMPFANGEN
S502
KLARTEXT M EMPFANGEN
S503
ZÄHLERWERT auxC AUSWÄHLEN UND KLARTEXT M
IM COUNTER-MODUS MIT HILFE DER BLOCK-VERSCHLÜSSELUNG SCTRENC.
skC = SCTRENC(sk, auxC) + M VERSCHLÜSSELN
S504
skC UND auxC AN DIE EINZELNEN VORRICHTUNGEN ÜBERTRAGEN
ENDE
sk
S203
auxC
S601
skC
S702

Fig. 14

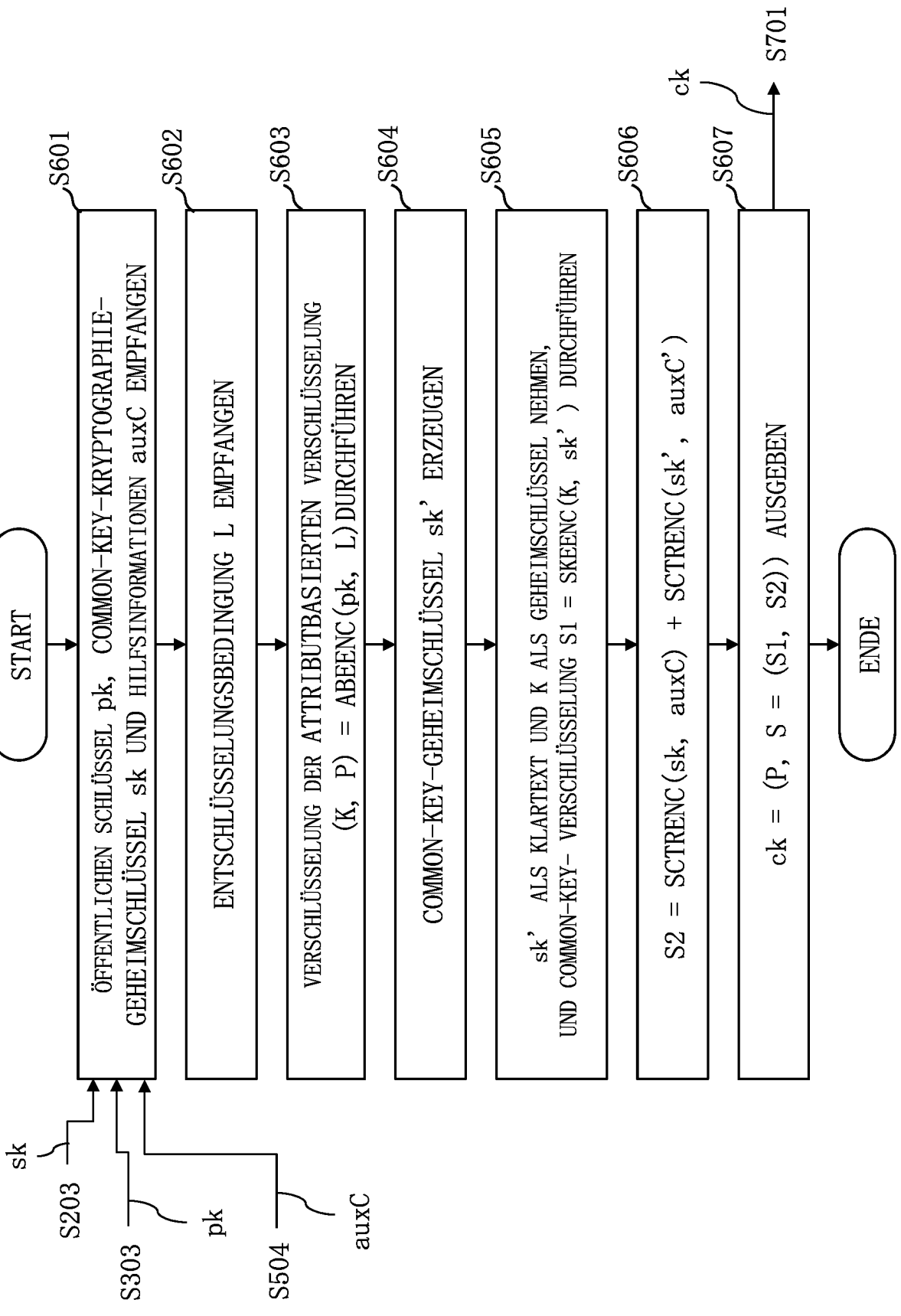

START
S601
ÖFFENTLICHEN SCHLÜSSEL pk, COMMON-KEY-KRYPTOGRAPHIE-GEHEIMSCHLÜSSEL sk UND HILFSINFORMATIONEN auxC EMPFANGEN
S602
ENTSCHLÜSSELUNGSBEDINGUNG L EMPFANGEN
S603
VERSCHLÜSSELUNG DER ATTRIBUTBASIERTEN VERSCHLÜSSELUNG (K, P) = ABEENC(pk, L) DURCHFÜHREN
S604
COMMON-KEY-GEHEIMSCHLÜSSEL sk' ERZEUGEN
S605
sk' ALS KLARTEXT UND K ALS GEHEIMSCHLÜSSEL NEHMEN, UND COMMON-KEY- VERSCHLÜSSELUNG S1 = SKEENC(K, sk') DURCHFÜHREN
S606
S2 = SCTRENC(sk, auxC) + SCTRENC(sk', auxC')
S607
ck
S701
ck = (P, S = (S1, S2)) AUSGEBEN
ENDE
sk
S203
S303
pk
S504
auxC

Fig. 15

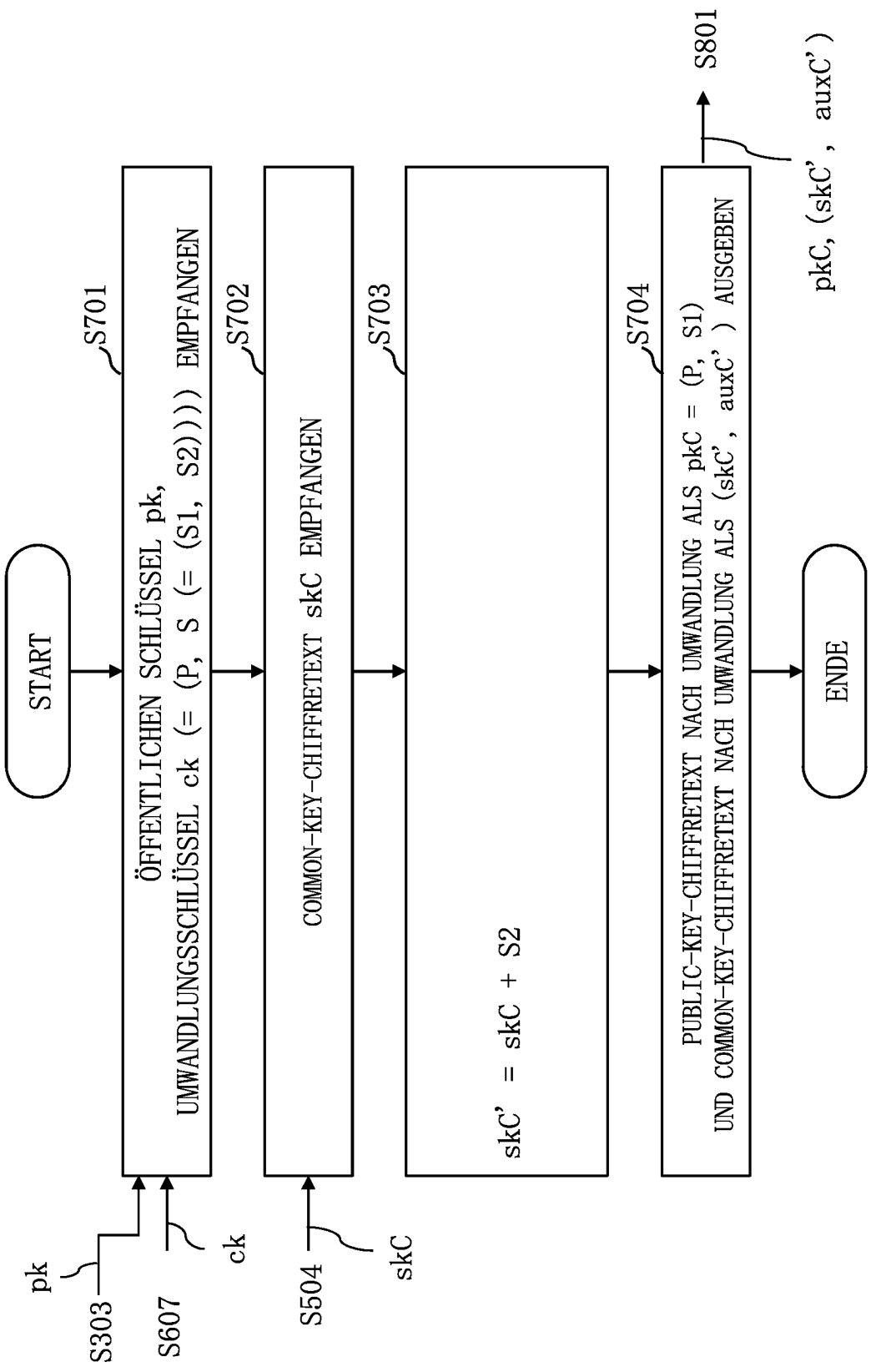

START
S701
ÖFFENTLICHEN SCHLÜSSEL pk,
UMWANDLUNGSSCHLÜSSEL ck (= (P, S (= (S1, S2)))) EMPFANGEN
S702
COMMON-KEY-CHIFFRETEXT skC EMPFANGEN
S703
skC' = skC + S2
S704
PUBLIC-KEY-CHIFFRETEXT NACH UMWANDLUNG ALS pkC = (P, S1)
UND COMMON-KEY-CHIFFRETEXT NACH UMWANDLUNG ALS (skC', auxC') AUSGEBEN
S801
pkC, (skC', auxC')
ENDE
pk
S303
S607
ck
S504
skC

Fig. 16

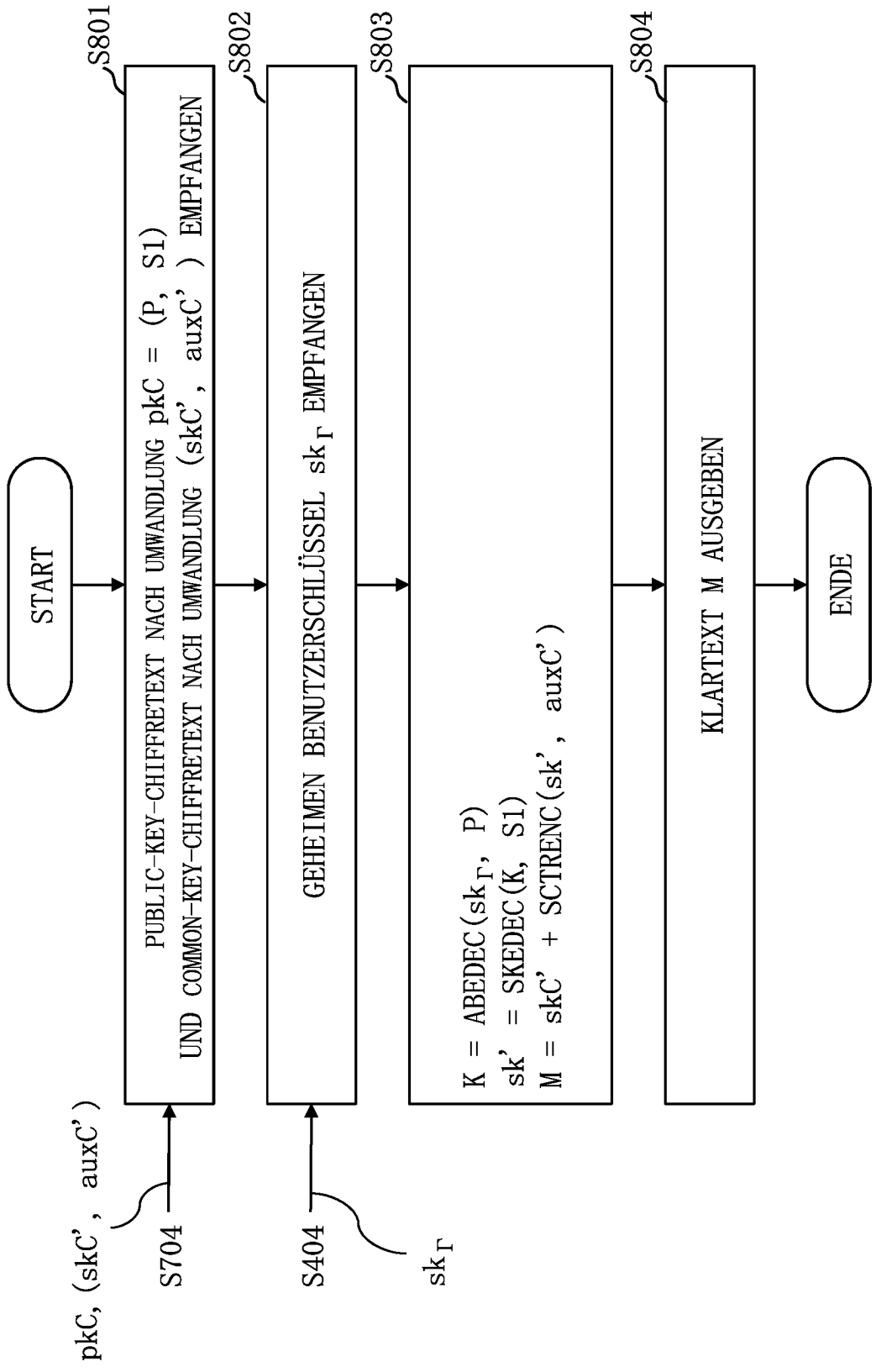

START
S801
PUBLIC-KEY-CHIFFRETEXT NACH UMWANDLUNG pkC = (P, S1)
UND COMMON-KEY-CHIFFRETEXT NACH UMWANDLUNG (skC', auxC') EMPFANGEN
S802
GEHEIMEN BENUTZERSCHLÜSSEL skΓ EMPFANGEN
S803
K = ABEDEC(skΓ, P)
sk' = SKEDEC(K, S1)
M = skC' + SCTRENC(sk', auxC')
S804
KLARTEXT M AUSGEBEN
ENDE
pkC, (skC', auxC')
S704
S404
skΓ

Fig. 17