(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 699 16 931 T2** 2005.04.28

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 966 126 B1**
(21) Deutsches Aktenzeichen: **699 16 931.3**
(96) Europäisches Aktenzeichen: **99 304 449.4**
(96) Europäischer Anmeldetag: **08.06.1999**
(97) Erstveröffentlichung durch das EPA: **22.12.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **06.05.2004**
(47) Veröffentlichungstag im Patentblatt: **28.04.2005**

(51) Int Cl.[7]: **H04L 9/06**
H04K 1/00

(30) Unionspriorität:
97782 **15.06.1998** **US**

(73) Patentinhaber:
Lucent Technologies Inc., Murray Hill, N.J., US

(74) Vertreter:
derzeit kein Vertreter bestellt

(84) Benannte Vertragsstaaten:
DE, FI, FR, GB, SE

(72) Erfinder:
Berenzweig, Adam L., New York, New York 10003, US; Falco, Steven Anthony, Morris Plains, New Jersey 07950, US; Mizikovsky, Semyon B., Morganville, New Jersey 07751, US; Pekrul, Winston Edward, Piscataway, New Jersey 08854, US; Rance, Robert John, Andover, Massachusetts 01810, US; Youtkus, Donald Joseph, Basking Ridge, New Jersey 07920, US

(54) Bezeichnung: **Sprachkodierer mit Verschlüsselung**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

Technisches Gebiet

[0001] Die vorliegende Erfindung betrifft allgemein Kommunikationssysteme und insbesondere in drahtlosen Kommunikationssystemen verwendete Verschlüsselungstechniken.

Allgemeiner Stand der Technik

[0002] Drahtlose Kommunikationssysteme verwenden Kryptographie zur Bereitstellung gesicherter Kommunikationsmittel für ihre Teilnehmer. Kryptographie liefert Sicherheit, so daß nur ein beabsichtigter Empfänger den Inhalt einer Nachricht, die durch einen autorisierten Sender gesendet wurde (und bei, der es sich z. B. um Sprachdaten, Benutzerdaten oder FACCH/SACCH-Nachrichten handeln kann), verstehen kann und nur der autorisierte Sender die Nachricht zu dem beabsichtigten Empfänger senden kann. Die Herausforderung der Kryptographie besteht darin, den Inhalt der Nachricht in eine Form zu verwandeln, die nur der beabsichtigte Empfänger verstehen kann. Dies muß auf eine Weise geschehen, die die sowohl für den Sender als auch für den beabsichtigten Empfänger wirtschaftlich ist. Gleichzeitig muß es (im Hinblick auf Zeit und/oder Geräte) für einen unautorisierten Empfänger (d. h. nicht den beabsichtigten Empfänger) sehr schwierig sein, den Inhalt zu verstehen. Da unautorisierte Empfänger und Sender immer intelligenter werden, wird der Notwendigkeit sicherer Kommunikation größer.

[0003] **Fig.** 1 zeigt eine Verschlüsselungssprachprozessorarchitektur, die in einen Sender **10** integriert ist, auf der Basis des wohlbekannten Standards IS-136 (einschließlich Revisionen) der TIA (Telecommunication Industrial Association) für TDMA (Time Division Multiple Access) und des Standards IS-641 für ACELP (Algebraic Code Excited Linear Prediction). Der Sender **10** umfaßt einen Sprachcodierer **12**, einen Sieben-Bit-CRC-Codierer (Sieben-Bit-CRC) **14**, einen Halbratenfaltungscodierer (½-Rate-CC) **16**, Punktierung **18**, Sprachchiffrierung **20** und einen Zweischlitzverschachtler **22**. Der Sprachcodierer **12** codiert einen Nachrichtenrahmen, der 160 16-Bit-Sprachabtastwerte umfaßt, um 148 codierte Sprachbit mit 96 Klasse-1-Bit und 52 Klasse-2-Bit zu erzeugen, wobei die Klasse-1-Bit 48 Klasse-1A-Bit und 48 Klasse-1B-Bit umfaßt. Die Klasse-1-Bit sind wichtige Bit (z. B. Bit, die Tonhöhe, Intonation usw. darstellen), die bei der Übertragung über Funkstrecken Fehlerkontrollschutz erfordern, während der Fehlerkontrollschutz unter Verwendung des CRC-Codes, der Faltungscodierung und der Bitverschachtelung bereitgestellt wird. Die Klasse-1A-Bit werden als Eingabe dem 7-Bit-CRC **14** zugeführt, um 7 Fehlerkontrollbit zu erzeugen. Die Fehlerkontrollbits, die Klasse-1-Bit und 5 Nachspannbit (die Faltungscodezustandsinformationen umfassen) werden als Eingaben dem ½-Rate-CC **16** zugeführt, um 216 Codewortbit zu erzeugen. Die Codewortbit werden dann einer Löschungseinfügung (über Punktierung **18**) unterzogen, um 208 punktierte Codewortbit zu erzeugen.

[0004] Als nächstes wird mit der Sprachchiffrierung **20** die Nachricht gesichert, so daß nur der beabsichtigte Empfänger den Inhalt der Nachricht verstehen kann. Genauer gesagt werden die punktierten Codewortbit und die Klasse-2-Bit als Eingaben der Sprachchiffrierung **20** zugeführt. Die Sprachchiffrierung **20** verschlüsselt die Eingaben unter Verwendung einer 260-Bit-Festgeheimnismaske, die dem beabsichtigten Empfänger zugeordnet ist, um 260 verschlüsselte Bit zu erzeugen. Genauer gesagt wird die Verschlüsselung durch Durchführen einer binären XOR-Operation an den punktierten Codewortbit und den Klasse-2-Bit unter Verwendung der geheimen Maske erzielt. Die verschlüsselten Bit werden (durch den Bitverschachtler **22**) bitverschachtelt, um 260 verschachtelte Bit zu erzeugen. Danach wird die Nachricht gemultiplext, moduliert und durch den Sender **10** gesendet.

[0005] Die gesendete Nachricht wird durch einen nicht gezeigten Empfänger empfangen, und im Empfänger wird die umgekehrte Funktion des Senders **10** durchgeführt. Nach dem Empfang der gesendeten Nachricht demoduliert der Empfänger die gesendete Nachricht und demultiplexiert sie, um 260 verschachtelte Bit zu erhalten. Der Bitverschachtelungsprozeß wird dann (durch einen Bitentschachtler) umgekehrt, um 260 verschlüsselte Bit zu erhalten. Die verschlüsselten Bit werden (durch einen Sprachchiffrierer) dechiffriert, um eine Ausgabe mit 208 punktierten Codewortbit und 52 Klasse-2-Bit zu erhalten. Wenn der Empfänger die von dem Sender **10** verwendete 260-Bit-Festgeheimnismaske nicht kennt (d. h. der Empfänger nicht der beabsichtigte Empfänger ist), wäre der Empfänger nicht in der Lage, die verschlüsselten Bit ordnungsgemäß zu entschlüsseln.

[0006] Die punktierten Codewortbit werden einem ½-Rate-Faltungs-Decoder zugeführt, in dem die punktierten Codewortbit entfaltet werden, um eine Ausgabe mit 96 Klasse-1-Bit (einschließlich 48 Klasse-1A-Bit und 48 Klasse-1B-Bit) und 7 Fehlerkontrollbit zu erhalten. Man beachte, daß im Empfänger keine Umkehrfunktion des Löschungseinfügungsprozesses stattfindet. Der Bitverlust aufgrund der Löschungseinfügung wird in dem Entfaltungsprozeß behoben, wie in der Technik wohlbekannt ist.

[0007] Die Klasse-1A-Bit werden von einem 7-Bit-CRC im Empfänger zur Erzeugung einer zweiten Menge von 7 Fehlerkontrollbit verwendet (wobei die erste Menge von 7 Fehlerkontrollbit Teil der Ausgabe des ½-Raten-Faltungsdecodierers sind). Die

erste und die zweite Menge Fehlerkontrollbit werden (unter Verwendung einer CRC-Prüfung) verglichen, um zu bestimmen, ob in bezug auf die Übertragung der Klasse-1A-Bit ein Fehler aufgetreten ist (d. h. Bestimmung, ob ein beschädigter Rahmen existiert). Wenn kein Übertragungsfehler aufgetreten ist, werden die Klasse-1-Bit und die Klasse-2-Bit (aus dem Sprachdechiffrierer) zur Decodierung an einen Sprachdecodierer weitergeleitet. Wenn ein Übertragungsfehler aufgetreten ist (d. h. ein beschädigter Rahmen erkannt wird), können die Klasse-1A-Bit und die 32 höchstwertigen Klasse-1B-Bit verworfen und durch eine Funktion oder Interpolation der Klasse-1A-Bit und der 32 höchstwertigen Klasse-1B-Bit des letzten unbeschädigten Rahmens bzw. der letzten unbeschädigten Rahmen ersetzt und zu dem Sprachdecodierer weitergeleitet werden. Die Klasse-2-Bit (aus dem Sprachdechriffierer) und die 16 niedrigstwertigen Klasse-1B-Bit (aus dem ½-Raten-Faltungsdecodierer) werden an den Sprachdecodierer weitergeleitet und dort zusammen mit der weitergeleiteten Funktion oder Interpolation der Klasse-1A-Bit und der 32 höchstwertigen Klasse-1B-Bit des letzten unbeschädigten Rahmens bzw. der letzten unbeschädigten Rahmen decodiert. Man beachte, daß, wenn Bitfehler in den Klasse-2-Bit und den 16 niedrigstwertigen Klasse-1B-Bit vorliegen, solche Fehler eine weniger wahrnehmungsbezogene Auswirkung auf die Sprachqualität als Fehler in den übrigen Klasse-1B- und Klasse-1A-Bit aufweisen werden.

[0008] Die vorbekannte Verschlüsselungsarchitektur, die eine Sprachchiffrierung umfaßt, bietet bestimmte Vorteile. Erstens ist ein Cryptosync aus einer externen Quelle (im folgenden als „externes Cryptosync" bezeichnet) zur Synchronisierung der 260-Bit-Festgeheimnismaske an beiden Enden (d. h. im Sender und im Empfänger) erforderlich, wobei Cryptosync eine Dateneingabe ist, mit der sichergestellt wird, daß zwei kryptographische Algorithmen miteinander synchronisiert sind. Zweitens besteht keine Verschlechterung der Sprachqualität bei Anwesenheit von Übertragungsfehlern. Fehler in der Übertragung der Klasse-1A-Bit und der 32 höchstwertigen Klasse-1B-Bit können durch Verwendung einer Funktion oder Interpolation der Klasse-1A-Bit und der 32 höchstwertigen Klasse-1B-Bit des letzten unbeschädigten Rahmens bzw. der letzten unbeschädigten Rahmen maskiert werden. Die vorbekannte Verschlüsselungsarchitektur ist jedoch auf zweierlei Hinsicht für Sicherheitsprobleme anfällig. Erstens kann die 260-Bit-Festgeheimnismaske durch Verwendung von bekanntem Klartext (d. h. Eingabe in den Sprachchiffrierer) bestimmt werden, der dann dazu verwendet werden kann, die verschlüsselten Bit zu verstehen (oder zu entschlüsseln), so daß die Sicherheit der übertragenen Nachricht kompromittiert wird. Zweitens wird auch bei Abwesenheit von bekanntem Klartext lediglich durch XOR-Verknüpfung benachbarter 260-Bit-Rahmen die Festgeheimnismaske eliminiert, und es werden Informationen darüber erhalten, wie sich die Parameter des ACELP-Sprachalgorithmus ändern. Folglich wird eine Sprachprozessorarchitektur benötigt, die verbesserte Sicherheit ohne Verwendung von externem Cryptosync und mit minimaler Sprachverschlechterung ergibt.

[0009] Aus US-A-5 694 473 ist ein Verfahren zum Entschlüsseln erneut gesendeter Teile einer Nachricht bekannt, umfassend: Empfangen einer Nachricht mit Verschlüsselungssynchronisation und mehrerer verschlüsselter Blöcke. Bis ein erster Block der mehreren verschlüsselten Blöcke mit Fehler empfangen wird, wird ein erster Schlüsselstrom aus der Verschlüsselungssynchronisation und mindestens einem der mehreren verschlüsselten Blöcke erzeugt, und unter Verwendung des ersten Schlüsselstroms werden die mehreren verschlüsselten Blöcke, die ohne Fehler empfangen werden, bevor der erste Block der mehreren verschlüsselten Blöcke mit Fehler empfangen wird, entschlüsselt. Aus der Nachricht wird ein Primblock bestimmt. Wenn der erste Block der mehreren verschlüsselten Blöcke mit Fehler empfangen wird, wird eine zweite Nachricht gesendet, die eine erneute Übertragung des ersten Blocks anfordert. Nach dem Empfang der erneuten Übertragung des ersten Blocks ohne Fehler wird ein zweiter Schlüsselstrom aus dem Primblock und der erneuten Übertragung des ersten Blocks erzeugt, und das Entschlüsseln der erneuten Übertragung des ersten Blocks wird unter Verwendung des zweiten Schlüsselstroms entschlüsselt.

Kurze Darstellung der Erfindung

[0010] Ein Verfahren gemäß der Erfindung wird in dem unabhängigen Anspruch definiert. Bevorzugte Formen werden in abhängigen Ansprüchen definiert.

[0011] Die vorliegende Erfindung ist eine verschlüsselnde Sprachprozessorarchitektur, die ohne Verwendung eines externen Cryptosync und mit minimaler Sprachverschlechterung verbesserte Sicherheit liefert. Dies wird erreicht durch Integrieren eines Blockverschlüsselers und eines Schlüsselstromgenerators (anstelle eines Festgeheimmaskenverschlüsselungsschemas, wie z. B. des im Sprachchiffrierer implementierten), um Blöcke codierter Sprachbit auf einer Senderseite zu verschlüsseln. Der Blockverschlüsseler verwendet einen invertierbaren kryptographischen Algorithmus und ein internes Cryptosync zum Umsetzen eines ersten Blocks codierter Sprachbit in einen ersten Chiffretextblock, wobei der erste Block codierter Sprachbit Bit der ersten Ebene enthält, die eine signifikante wahrnehmungsbezogene Verschlechterung der Sprachqualität verursachen würden, wenn während ihrer Übertragung ein Fehler aufträte (und die verfälschten Bit anstelle einer Funktion oder Interpolation von Bit aus vorherigen unbe-

schädigten Rahmen verwendet würden).

[0012] Der erste Chiffretextblock wird dann als Eingabe dem Schlüsselstromgenerator und einer CRC-Prüfung zugeführt. Der Schlüsselstromgenerator verwendet einen invertierbaren kryptographischen Algorithmus, der als Schlüssel-Einwegfunktion verwendet wird, und ein internes Cryptosync zur Umsetzung des ersten Chiffretextblocks in einen Schlüsselstrom, der verschlüsselte erste Chiffretextblöcke umfaßt. Der Schlüsselstrom wird anschließend zur Verschlüsselung eines zweiten und eines dritten Blocks codierter Sprachbit verwendet, um einen zweiten Chiffretextblock bzw. einen dritten Chiffretextblock zu erzeugen, wobei der dritte Block codierter Sprachbit Bit der zweiten Ebene enthält, die eine geringfügige oder keine wahrnehmungsbezogene Verschlechterung der Sprachqualität verursachen, wenn während der Übertragung des ersten Chiffretextblocks ein Fehler auftritt, und der zweite Block codierter Sprachbit Bit der ersten und der zweiten Ebene enthält.

[0013] Bei der CRC-Prüfung wird der erste Chiffretextblock zur Erzeugung von Fehlerkontrollbit verwendet, mit denen erkannt werden kann, ob bei der Übertragung des ersten Chiffretextblocks ein Fehler aufgetreten ist, d. h. der erste Chiffretextblock wird durch eine bestimmte Art von Übertragungsfehlerdetektionsmechanismus geschützt. Der erste, der zweite und der dritte Chiffretextblock und die Fehlerkontrollbit werden danach verarbeitet und übertragen.

[0014] Auf der Empfängerseite wird mit den Fehlerkontrollbit und dem empfangenen ersten Chiffretextblock bestimmt, ob bei der Übertragung des ersten Chiffretextblocks ein Fehler aufgetreten ist. Wenn kein Fehler erkannt wird, wird der empfangene erste Chiffretextblock durch einen Blockentschlüsseler entschlüsselt und zur Entschlüsselung des empfangenen zweiten und dritten Chiffretextblocks (über einen mit dem Schlüsselstromgenerator auf der Senderseite identischen Schlüsselstromgenerator) verwendet. Wenn ein Fehler erkannt wird, werden die Bit der ersten Ebene (in dem ersten und dem zweiten Chiffretextblock) unter Verwendung einer Funktion oder Interpolation der Bit der ersten Ebene (in dem ersten und dem zweiten Chiffretextblock) unter Verwendung einer bestimmten Funktion oder Interpolation der Bit der ersten Ebene in einem oder mehreren letzten unbeschädigten Rahmen maskiert. Die Bit der zweiten Ebene (in dem zweiten und dem dritten Chiffretextblock) können direkt zu einem Sprachdecodierer weitergeleitet werden, anstatt (falscherweise) entschlüsselt zu werden, um Verarbeitungszyklen zu sparen.

[0015] Vorteilhafterweise verlängert diese Ausführungsform der vorliegenden Erfindung keine Fehler in und aus den Bit der ersten Ebene. Genauer gesagt verlängert sich, wenn ein Fehler an einem beliebigen Bit in dem empfangenen ersten Chiffretextblock aufgetreten ist, ein solcher Fehler zu keinem anderen Bit der ersten Ebene, da alle Bit der ersten Ebene durch eine bestimmte Funktion oder Interpolation der Bit der ersten Ebene in einem oder mehreren letzten unbeschädigten Rahmen maskiert werden. Obwohl sich ein an einem beliebigen Bit in dem empfangenen ersten Chiffretextblock auftretender Fehler zu dem Bit der zweiten Ebene verlängert, hat ein solcher Fehler nur wenig oder gar keine wahrnehmungsbezogene Wirkung auf die Sprachqualität. Wenn an keinem Bit in dem empfangenen ersten Chiffretextblock Fehler bestehen, werden insbesondere keine Fehler zu irgendwelchen anderen Bit der ersten Ebene oder zweiten Ebene verlängert. Außerdem ist zu beachten, daß aufgrund der Schlüsselstromgeneratorarchitektur, bei der der Schlüsselstrom mit dem Klartext XOR-verknüpft wird, sich keine Fehler in dem zweiten oder dritten empfangenen Chiffretextblock zu anderen Bit verlängern.

[0016] Ferner verwenden der Blockverschlüsseler und der Schlüsselstromgenerator vorteilhafterweise kryptographische Algorithmen (oder Schlüssel-Einwegfunktionen), die kryptographisch wesentlich sicherer als die 260-Bit-Festgeheimnismaske sind, die im Stand der Technik von Sprachchiffrierern verwendet wird. Somit ist die verschlüsselnde Sprachprozessorarchitektur der vorliegenden Erfindung kryptographisch wesentlich sicherer als der Stand der Technik. Außerdem wird internes Cryptosync verwendet, um verschlüsselnde und entschlüsselnde kryptographische Algorithmen zu synchronisieren. Somit ist kein externes Cryptosync erforderlich.

Kurze Beschreibung der Zeichnungen

[0017] Die Merkmale, Aspekte und Vorteile der vorliegenden Erfindung werden mit Bezug auf die folgende Beschreibung, die angefügten Ansprüche und die beigefügten Zeichnungen besser verständlich. Es zeigt:

[0018] Fig. 1 eine vorbekannte Architektur von Sprachprozessor, Fehlerschutz und Sprachchiffrierung;

[0019] Fig. 2 eine in einen gemäß der vorliegenden Erfindung verwendeten Sender integrierte Sprachprozessorarchitektur;

[0020] Fig. 3 ein repräsentatives Diagramm, das die codierten Sprachbit, die in der vorliegenden Anmeldung charakterisiert werden, beschreibt;

[0021] Fig. 4 ein Funktionsblockschaltbild eines Blockverschlüsselers, der die ECMEA-Algorithmen (erweiterte Verschlüsselungsalgorithmen für zellulare Nachrichten) zur Verschlüsselung von 48-Bit-Blöcken Klartext zu Chiffretext gemäß einer Ausfüh-

rungsform der vorliegenden Erfindung verwendet;

[0022] **Fig.** 5 ein Funktionsblockschaltbild eines 48-Bit-Blockentschlüsselers zur Durchführung der umgekehrten Funktion des in **Fig.** 4 abgebildeten Blockverschlüsselers;

[0023] **Fig.** 6 ein Funktionsblockschaltbild eines Schlüsselstromgenerators, der ECMEA verwendet, gemäß einer Ausführungsform der vorliegenden Erfindung;

[0024] **Fig.** 7 eine Sprachprozessorarchitektur, die in einen gemäß der vorliegenden Erfindung verwendeten Empfänger integriert ist;

[0025] **Fig.** 8 ein Funktionsblockschaltbild eines ECMEA verwendenden 40-Bit-Blockverschlüsselers gemäß einer Ausführungsform der vorliegenden Erfindung;

[0026] **Fig.** 9 ein Funktionsblockschaltbild eines 40-Bit-Blockentschlüsselers zur Durchführung der umgekehrten Funktion des in **Fig.** 8 abgebildeten Blockverschlüsselers; und

[0027] **Fig.** 10 ein Funktionsblockschaltbild eines RC5 verwendenden 48-Bit-Blockverschlüsselers gemäß einer Ausführungsform der vorliegenden Erfindung.

Ausführliche Beschreibung

[0028] FIG. zeigt eine in einen gemäß der vorliegenden Erfindung verwendeten Sender **30** integrierte Sprachprozessorarchitektur. Zur Veranschaulichung wird die vorliegende Erfindung hier mit Bezug auf eine Sprachprozessorarchitektur beschrieben, die auf dem wohlbekannten Standard IS-136 (einschließlich Revisionen) für TMDA (Time Division Multiple Access) und dem Standard IS-641 für ACELP (Algebraic Code Excited Linear Prediction) basiert. Dies sollte jedoch auf keinerlei Weise als Einschränkung der vorliegenden Erfindung aufgefaßt werden.

[0029] Der Sender **30** umfaßt eine Sprachprozessorarchitektur mit Sprachcodierer **32**, Blockverschlüsseler **34**, Schlüsselstromgenerator **36**, XOR-Operatoren **38**, **40**, Sieben-Bit-CRC-Codierer (7-Bit-CRC) **42**, Halbratenfaltungscodierer (½-Rate-CC) **44**, Punktierung **46** und Zweischlitzverschachteler **48**. Die Sprachprozessorarchitektur kann als Software implementiert werden, die auf einem Computerprozessor, einem anwendungsspezifischen integrierten Chip usw. ausgeführt wird. Der Sprachcodierer **32**, die XOR-Operatoren **38**, **40**, der 7-Bit-CRC **42**, der ½-Rate-CC **44**, die Punktierung **46** und der Zweischlitzverschachteler **48** sind in der Technik wohlbekannt. Der Blockverschlüsseler **34** und der Schlüsselstromgenerator **36** werden hier beschrieben.

[0030] Der Sprachcodierer **32** empfängt einen zu übertragenden Nachrichtenrahmen, der 160 16-Bit-Sprachabtastwerte umfaßt. Für die Zwecke der vorliegenden Anmeldung soll der Begriff „Sprachabtastwerte" ohne Einschränkung u. a. Sprachdaten, Benutzerdaten oder Steuerkanalnachrichten umfassen. Der Rahmen wird durch den Sprachcodierer **32** codiert, um $output_{32}$, umfassend 148 codierte Sprachbit mit auf erster und auf zweiter Ebene codierten Sprachbit, zu erzeugen, wobei die Bit der ersten Ebene (codierte Sprache) Spracheigenschaften darstellen, die die Sprachqualität wahrnehmbar verschlechtern werden, wenn in beliebigen Bits des ersten Blocks ein Übertragungsfehler auftritt, und die Bit der zweiten Ebene (codierte Sprache) Spracheigenschaften darstellen, die die Sprachqualität nicht wahrnehmbar verschlechtern werden, wenn in beliebigen Bit des ersten Blocks ein Übertragungsfehler auftritt. Siehe **Fig.** 3, worin eine Tabelle 45 abgebildet ist, die die codierten Sprachbit, die in der vorliegenden Anmeldung charakterisiert werden, beschreibt.

[0031] Die codierten Sprachbit werden danach portioniert und in drei Blöcken verarbeitet. Der erste Block (der hier auch als Klasse-1A-Bit oder $output_{32-1}$ bezeichnet wird) enthält 48 Bit der ersten Ebene, der zweite Block (der hier auch als Klasse-1B-Bit oder $output_{32-2}$ bezeichnet wird) enthält 32 Bit der ersten Ebene und 16 Bit der zweiten Ebene, und der dritte Block (der hier auch als Klasse-2-Bit oder $output_{32-3}$ bezeichnet wird) enthält 52 Bit der zweiten Ebene. Genauer gesagt sind mit Bezug auf den zweiten Block die Bit der ersten Ebene die 32 höchstwertigen Bit und die Bit der zweiten Ebene die 16 niedrigstwertigen Bit. Man beachte, daß die vorliegende Erfindung nicht auf die Anzahl von Blöcken, auf die die codierten Sprachbit portioniert werden, oder auf die Anzahl von Bit in jedem Block begrenzt werden sollte. Da die Bit der ersten Ebene die Sprachqualität wahrnehmbar verschlechtern werden, wenn ein Übertragungsfehler auftritt, wird Fehlerkontrollschutz auf so viele dieser Bit wie möglich angewandt, wobei Fehlerkontrollschutz z. B. über CRC-Code und Faltungscodierung bereitgestellt wird.

[0032] Aus dem Sprachcodierer **32** werden die Klasse-1A-Bit (erster Block) als Eingabe dem Blockverschlüsseler **34**, die Klasse-1B-Bit (zweiter Block) als Eingabe dem XOR-Operator **38** und die Klasse-2-Bit (dritter Block) als Eingabe dem XOR-Operator **40** zugeführt. Der Blockverschlüsseler **34** verwendet einen invertierbaren kryptographischen Algorithmus mit einem dem beabsichtigten Empfänger zugeordneten Schlüssel zum Verschlüsseln von Klartextblöcken zu Chiffretext. Solche kryptographischen Algorithmen sind z. B. RC5 und ECMEA (Enhanced Cellular Messaging Encryption Algorithm). RC5 wurde von Ron Rivest entwickelt und ist in der Technik

wohlbekannt. ECMEA wurde von Robert Rance, Daniel Heer, Semyon Mizikovsky et al. entwickelt und am 28.10.1997 bei dem TIA TR45 Ad-Hoc Authentication Group Meeting offengelegt, an dem Mitglieder der TIA teilnahmen, und ist für begrenzte und geregelte Distribution durch die TIA unter Berücksichtigung der Exportgesetze des United States Department of Commerce, spezifiziert in den Exportadministrationsregeln (Titel 15, CFR, Teile 730 bis einschließlich 774) verfügbar.

[0033] In dem Blockverschlüsseler **34** werden die Klasse-1A-Bit verschlüsselt, um $output_{34}$, umfassend 48 Klasse-1A-Chiffretextbit (oder einen ersten Chiffretextblock), zu erzeugen. **Fig.** 4 zeigt ein Funktionsblockschaltbild des Blockverschlüsselers **34**, der ECMEA zur Verschlüsselung von 48-Bit-Blöcken Klartext zu Chiffretext verwendet, gemäß einer Ausführungsform der vorliegenden Erfindung. Der Blockverschlüsseler umfaßt einen ersten, einen zweiten und einen dritten Funktionsaufruf **52**, **54** und **58** (Betrieb im Verschlüsselungsmodus zum Verschlüsseln ihrer Eingaben) und den XOR-Operator **56**. Ein erster und ein zweiter 16-Bit-Teil der Klasse-1A-Bit (der im folgenden als erster bzw. zweiter Klasse-1A-Teil bezeichnet wird) werden als Angaben dem ersten und dem zweiten ECMEA-Funktionsaufruf **52**, **54** zugeführt. Der erste EDMEA-Funktionsaufruf **52** verschlüsselt den ersten Klasse-1A-Teil unter Verwendung des zweiten Klasse-1A-Teils als Cryptosync-Eingabe, um $output_{52}$ (16 Bit) zu erzeugen.

[0034] Wie in der Technik wohlbekannt ist, dient Cryptosync zur Sychronisierung kryptographischer Verschlüsselungs- und Entschlüsselungsalgorithmen. Bei ECMEA dient insbesondere Cryptosync jedoch auch als Schlüsselbit zum Zwecke des Verbesserns der kryptographischen Stärke von ECMEA. In dieser Rolle wird ECMEA als eine Schlüssel-Hash-Funktion verwendet, um sowohl die Entropie des ersten und des zweiten Klasse-1A-Teils zu konzentrieren als auch die gesamte kryptographische Stärke des 48-Bit-Blockverschlüsselers zu erhöhen.

[0035] $output_{52}$ wird mit einem dritten 16-Bit-Teil der Klasse-1A-Bit (der im folgenden als dritter Klasse-1A-Teil bezeichnet wird) in dem XOR-Operator 56 XOR-verknüpft, um $output_{56}$ (16 Bit) zu erzeugen.

[0036] $output_{56}$ wird als Eingaben einem zweiten und einem dritten ECMEA-Funktionsaufruf **54**, **58** zugeführt. Der zweite ECMEA-Funktionsaufruf **54** verwendet $output_{56}$ als Cryptosync zur Verschlüsselung des ersten und des zweiten Klasse-1A-Teils und zur Erzeugung von $output_{54\text{-}1}$ (16 Bit) bzw. $output_{54\text{-}2}$ (16 Bit). Der dritte ECMEA-Funktionsaufruf **58** verschlüsselt $output_{56}$ und $output_{54\text{-}1}$ unter Verwendung von $output_{54\text{-}2}$ als Cryptosync, um $output_{58}$ (32 Bit) zu erzeugen. **Fig.** 5 zeigt ein Funktionsblockschaltbild eines 48-Bit-Entschlüsselers **35** zur Durchführung der umgekehrten Funktion des in **Fig.** 4 abgebildeten Blockverschlüsselers **34**.

[0037] $output_{58}$ und $output_{54\text{-}2}$ umfassen zusammen $output_{34}$ des Blockverschlüsselers **34**. $Output_{34}$ wird als Eingaben dem 7-Bit-CRC **42**, dem ½-Rate-CC **44** und dem Schlüsselstromgenerator **36** zugeführt. In dem 7-Bit-CRC **42** wird mit $output_{34}$ das 7 Fehlerkontrollbit umfassende $output_{42}$ erzeugt. $Output_{42}$ wird danach als Eingabe dem ½-Rate-CC **44** zugeführt.

[0038] Der Schlüsselstromgenerator **36** verwendet entweder einen invertierbaren kryptographischen Algorithmus, wie z. B. RC5 und ECMEA, oder eine geeignete nichtinvertierbare Schlüssel-Einwegfunktion, wobei dem beabsichtigten Empfänger ein Schlüssel zur Ausgabe eines Bitschlüsselstroms zugeordnet ist. Man beachte, daß eine Einwegfunktion eine allgemeine Art von kryptographischer Operation ist und tatsächlich invertierbare kryptographische Algorithmen als Subklasse enthält. Eine Person, die die Ausgabe einer Schlüssel-Einwegfunktion beobachtet, kann weder auf den Schlüssel noch auf die Eingabe schließen.

[0039] Der Schlüsselstromgenerator **36** wird durch die 48 Klasse-1A-Chiffretextbit (d. h. $output_{34}$) angesteuert, die an dem Eingang des Schlüsselstromgenerators **34** oft genug wiederholt werden, um einen 104-Bit-Block zu füllen. In dem Schlüsselstromgenerator **36** werden die Klasse-1A-Chiffretextbit verschlüsselt, um $output_{36}$ des Schlüsselstroms, umfassend 100 Bit verschlüsselter Klasse-1A-Chiffretextbit, zu erzeugen. Genauer gesagt wird $output_{36}$ erzeugt, indem der (von dem Schlüsselstromgenerator **36** verwendete) kryptographische Algorithmus durch Verschlüsseln öffentlich bekannter Pseudozufallsdaten ausgeführt wird, bei denen es sich tatsächlich um die Klasse-1A-Chiffretextbit handelt. Man beachte, daß 4 der Klasse-1A-Chiffretextbit (die den 104-Bit-Block umfassen) verworfen werden, da ECMEA (und die meisten anderen Blockalgorithmen) nur eine ganze Anzahl von Byte verschlüsseln.

[0040] **Fig.** 6 zeigt ein Funktionsblockschaltbild des Schlüsselstromgenerators **36**, der ECMEA verwendet, gemäß einer Ausführungsform der vorliegenden Erfindung. Der Schlüsselstromgenerator **36** umfaßt den ECMEA-Funktionsaufruf **62**, der die 104-Bit-Blockeingabe, umfassend wiederholt $output_{34}$ (aus dem Blockverschlüsseler **34**), empfängt. Man beachte, daß die Ausgabe des Blockverschlüsselers **34** an sich selbst angehängt oder mit sich selbst verkettet wird, um 96 Bit zu erhalten, und dann teilweise ein weiteres Mal angehängt wird, um eine 104-Bit-Blockeingabe für den Schlüsselstromgenerator zu erhalten. Die 104-Bit-Blockeingabe wird durch den ECMEA-Funktionsaufruf **62** unter Verwendung der 16 höchstwertigen Bit von $output_{34}$ (d. h. der

16 höchstwertigen Bit der 48 Klasse-1A-Chiffretext-Bit) als Cryptosync verschlüsselt, um $output_{36}$ zu erzeugen.

[0041] $Output_{36}$ wird als Eingaben den XOR-Operatoren **38** und **40** zugeführt. Genauer gesagt wird ein 48-Bit-Teil von $output_{36}$ als Eingabe dem XOR-Operator **38** und ein 52-Bit-Teil von $output_{36}$ als Eingabe dem XOR-Operator **40** zugeführt. In dem XOR-Operator **38** werden die Klasse-1B-Bit (d. h. der zweite Block) mit dem 48-Bit-Teil von $output_{36}$ XOR-verknüpft, um output **38**, umfassend 48 Klasse-1B-Chiffretextbit (d. h. den zweiten Chiffretextblock), zu erzeugen. $Output_{38}$ wird dann als Eingabe dem ½-Rate-CC **44** zugeführt. Ähnlich werden in dem XOR-Operator **40** die Klasse-2-Bit (d. h. der dritte Block) mit dem 52-Bit-Teil von $output_{36}$ XOR-verknüpft, um $output_{40}$, umfassend 52 Klasse-2-Chiffretextblockbit (d. h. den dritten Chiffretextblock), zu erzeugen. $Output_{40}$ wird dann als Eingabe dem Zweischlitzverschachteler **48** zugeführt.

[0042] In dem ½-Rate-CC **44** werden $output_{42}$, $output_{34}$ und $output_{38}$ zusammen mit 5 Nachspannbit (die Faltungscodezustandsinformationen umfassen) zur Erzeugung von $output_{44}$ (umfassend 216 Codewortbit) verwendet. $Output_{44}$ wird der Punktierung **46** zugeführt, um $output_{46}$, umfassend 208 punktierte Codewortbit, zu erzeugen. $Output_{46}$ wird dann dem Zweischlitzverschachteler **48** zugeführt und dort mit $output_{40}$ bitverschachtelt, um $output_{48}$, umfassend 260 verschachtelte Bit, zu erzeugen. $Output_{48}$ wird anschließend gemultiplext, moduliert und durch den Sender **30** gesendet.

[0043] Die gesendete Nachricht wird durch einen Empfänger empfangen, in dem die umgekehrte Funktion des Senders **10** durchgeführt wird. **Fig.** 7 zeigt eine Sprachprozessorarchitektur, die in einen gemäß der vorliegenden Erfindung verwendeten Empfänger **70** integriert ist. Der Empfänger **70** umfaßt eine Sprachprozessorarchitektur mit dem Sprachdecodierer **72**, dem Blockentschlüsseler **74**, dem Schlüsselstromgenerator **76**, XOR-Operatoren **78**, **80**, dem 7-Bit-CRC **82**, dem ½-Rate-Faltungsdecodierer **84** und dem Zweischlitzbitentschachteler **86**. Die Sprachprozessorarchitektur kann als Software implementiert werden, die auf einem Computerprozessor, einem anwendungsspezifischen integrierten Chip usw. ausgeführt wird. Der Spachdecodierer **72**, die XOR-Operatoren **78**, **80**, der 7-Bit-CRC **82**, der ½-Rate-Faltungsdecodierer **84** und der Zweischlitzbitentschachtler **86** sind alle in der Technik wohlbekannt. Der Blockverschlüsseler **74** und der Schlüsselstromgenerator **76** werden hier beschrieben.

[0044] Nach dem Empfang der gesendeten Nachricht führt der Empfänger ein Demodulieren und Demultiplexen der gesendeten Nachricht durch, um $output_{48'}$ (d. h. 260 verschachtelte Bit) zu erhalten, wobei die Apostrophnotation eine empfangene Version der entsprechenden gesendeten Version bedeuten soll. Der Zweischlitzbitentschachtler **86** verwendet $output_{48'}$ zur Erzeugung von $output_{46'}$ (d. h. 208 punktierten Codewortbit und 52 Klasse-2-Chiffretextbit oder dem dritten Chiffretextblock). Die 208 punktierten Codewortbit werden dann durch den ½-Rate-Faltungsdecodierer **84** entfaltet, um 5 Nachspannbit, $output_{42'}$ (d. h. 7 Fehlerkontrollbit) , $output_{34'}$ (d. h. 48 Klasse-1A-Chiffretextbit oder den ersten Chiffretextblock) und $output_{38'}$ (d. h. 48 Klasse-1B-Chiffretextbit oder den zweiten Chiffretextblock) zu erhalten. Man beachte, daß in dem Empfänger **80** keine Operation zum Umkehren des Löschungseinfügungsprozesses der Punktierung **46** stattfindet. Die aufgrund der Löschungseinfügung verlorenen Bit werden im Empfänger durch den ½-Rate-Faltungsdecodierer **84** wiederhergestellt.

[0045] $Output_{34'}$ wird als Eingabe dem 7-Bit-CRC **82** zugeführt, um eine zweite Menge von 7 Fehlerkontrollbit zu erzeugen (wobei die erste Menge von 7 Fehlerkontrollbit zusammen $output_{42'}$ umfaßt, was die 7 Fehlerkontrollbit sind, die durch den ½-Rate-Faltungsdecodierer ausgegeben werden). Die erste und die zweite Menge von Fehlerkontrollbit werden untersucht, um zu bestimmen, ob ein Fehler in der Übertragung des ersten Chiffretextblocks (d. h. der Klasse-1A-Chiffretextbit) vorlag (d. h. Bestimmung ob ein beschädigter Rahmen existiert). Wenn kein Übertragungsfehler aufgetreten ist, wird $output_{34'}$ (d. h. Klasse-1A-Chiffretextbit) an den Blockentschlüsseler **74** und den Schlüsselstromgenerator **76** weitergeleitet. Der Blockentschlüsseler ist betreibbar, um die umgekehrte Funktion des Blockverschlüsselers **34** durchzuführen.

[0046] Siehe **Fig.** 5, worin ein Funktionsblockschaltbild eines 48-Bit-Entschlüsselers **35** zur Durchführung der umgekehrten Funktion des in **Fig.** 4 abgebildeten Blockverschlüsselers **34** abgebildet ist. Der Schlüsselstromgenerator **76** ist mit dem Schlüsselstromgenerator **36** identisch.

[0047] In dem Blockentschlüsseler **74** wird $output_{34'}$ entschlüsselt, um $output_{32\text{-}1'}$ (d. h. 48 Klasse-1A-Bit) zu erhalten. In dem Schlüsselstromgenerator **76** wird mit $output_{34'}$ $output_{36'}$ des Schlüsselstroms (d. h. 100 verschlüsselte Klasse-1A-Chiffretextbit) erzeugt. Mit dem Schlüsselstrom wird dann $output_{38'}$ (d. h. Klasse-1B-Chiffretextbit) und $output_{40'}$ (d. h. Klasse-2-Chiffretextbit) XOR-verknüpft, um $output_{32\text{-}2'}$ (d. h. Klasse-1B-Bit) und $output_{32\text{-}3'}$ (d. h. Klasse-2-Bit) zu erhalten. $Output_{32\text{-}1'}$, $output_{32\text{-}2'}$ und $output_{32\text{-}3'}$ (d. h. Klasse-1A-Bit, Klasse-1B-Bit und Klasse-2-Bit) werden durch den Sprachdecodierer **72** decodiert, um den ursprünglichen Nachrichtenrahmen zu erhalten.

[0048] Wenn ein Übertragungsfehler aufgetreten ist, werden die Bit der ersten Ebene (d. h. die Klas-

se-1A-Bit und die 32 höchstwertigen Klasse-1B-Bit) verworfen und mit einer Funktion oder Interpolation der Bit der ersten Ebene eines oder mehrerer vorheriger unbeschädigter Rahmen ersetzt (wie in dem wohlbekannten Standard IS-641 beschrieben) und an den Sprachdecodierer **72** weitergeleitet. Eine Blockentschlüsselung der Klasse-1A-Bit oder eine Erzeugung eines Schlüsselstroms (unter Verwendung des Schlüsselstromgenerators **76**) wäre nicht notwendig, da diese Daten im Fall eines versagenden CRC irrelevant wären. Somit ist es nicht möglich, die Bit der zweiten Ebene (d. h. die Klasse-2-Bit und die 16 niedrigstwertigen Klasse-1B-Bit) zu entschlüsseln. Die Vermeidung dieser Aufgaben spart Prozessorzyklen. Die Verschlechterung der Sprachqualität aufgrund des Verschlüsseltbleibens dieser Bit der zweiten Ebene wird nur wenig oder keine wahrnehmungsbezogene Auswirkung aufweisen.

[0049] Man beachte, daß die vorliegende Erfindung auf ähnliche Weise wie Sprachvertraulichkeit FACCH- und SACCH-Verschlüsselung bereitstellt, wobei der Ursprung des Cryptosync statt extern intern ist. Das erste Wort jeder FACCH- und SACCH-Nachricht enthält einen 8-Bit-Nachrichtentyp, der unverschlüsselt bleiben muß. Somit würde das erste Wort jeder FACCH- und SACCH-Nachricht einen 40-Bit-Blockverschlüsseler **80** (und -entschlüsseler **90**) verwenden, wie in **Fig.** 8 (und in **Fig.** 9) gezeigt, und die übrigen Wörter würden den 48-Bit-Blockverschlüsseler von **Fig.** 4 benutzen.

[0050] Obwohl die vorliegende Erfindung in großem Detail mit Bezug auf bestimmte Ausführungsformen beschrieben wurde, sind andere Versionen möglich. Zum Beispiel sind andere Verschlüsseler und Entschlüsseler möglich. Siehe **Fig.** 10, worin ein 48-Bit-Blockverschlüsseler **100**, der RC5 verwendet, abgebildet ist. Für Durchschnittsfachleute ist ersichtlich, daß das Konzept der vorliegenden Erfindung auf Sprachprozessorarchitekturen angewandt werden kann, die andere Arten von Sprachcodierern, Fehlerkontrollmechanismen und Verschlüsselungs- und/oder kryptographischen Algorithmen verwenden.

Patentansprüche

1. Verfahren zum Verschlüsseln eines Nachrichtenrahmens, wobei der Nachrichtenrahmen einen ersten Block mit auf erster Ebene codierten Sprachbit und einen zweiten Block mit auf zweiter Ebene codierten Sprachbit aufweist, wobei auf erster Ebene codierte Sprachbit Spracheigenschaften darstellen, die die Sprachqualität wahrnehmbar verschlechtern werden, wenn ein Übertragungsfehler auftritt, und auf zweiter Ebene codierte Sprachbit Spracheigenschaften darstellen, die die Sprachqualität nicht wahrnehmbar verschlechtern werden, wenn ein Übertragungsfehler auftritt, gekennzeichnet durch die folgenden Schritte:
Verschlüsseln des ersten Blocks (**32-1**) unter Verwendung eines Blockchiffreverschlüsselungsalgorithmus (**34**), um einen ersten Chiffretextblock (**34**) zu erzeugen;
Erzeugen eines Schlüssel-Bitstroms (**36**) unter Verwendung des ersten Chiffretextblocks;
Verschlüsseln des zweiten Blocks (**32-2**) unter Verwendung des Schlüssel-Bitstroms, um einen zweiten Chiffretextblock (**38**) zu erzeugen; und
Erzeugen von Fehlersteuerbit (**42**) unter Verwendung des ersten Chiffretextblocks.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der zweite Block weiterhin auf erster Ebene codierte Sprachbit enthält.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der erste Block 48 Bit der ersten Ebene umfaßt.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der erste Block 52 Bit der ersten Ebene umfaßt.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Nachrichtenrahmen weiterhin einen dritten Block (**32-3**) mit auf erster Ebene codierten Sprachbit und auf zweiter Ebene codierten Sprachbit enthält, wobei das Verfahren weiterhin durch den folgenden zusätzlichen Schritt gekennzeichnet ist:
Verschlüsseln des dritten Blocks unter Verwendung des Schlüssel-Bitstroms, um einen dritten Chiffretextblock (**40**) zu erzeugen.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Schritt des Erzeugens des Schlüssel-Bitstroms die folgenden Schritte umfaßt:
Wiederholen des ersten Chiffretextblocks, um einen wiederholten ersten Chiffretextblock zu erzeugen; und
Verschlüsseln des wiederholten ersten Chiffretextblocks unter Verwendung eines Teils des ersten Chiffretextblocks, um den Schlüssel-Bitstrom zu erzeugen.

7. Verfahren nach Anspruch 1, gekennzeichnet durch den folgenden zusätzlichen Schritt:
Erzeugen von Fehlersteuerbit unter Verwendung des ersten Chiffretextblocks.

8. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Schritt des Verschlüsselns des ersten Blocks die folgenden Schritte umfaßt:
Verschlüsseln eines ersten Teils des ersten Blocks unter Verwendung eines zweiten Teils des ersten Blocks als Cryptosync, um eine erste Ausgabe (**52**) zu erzeugen;
Verknüpfen der ersten Ausgabe mit einem dritten Teil des ersten Chiffretextblocks unter Verwendung einer

binären Operation, um eine zweite Ausgabe (**54**) zu erzeugen;
Verschlüsseln des ersten und des zweiten Teils des ersten Chiffretextblocks unter Verwendung der zweiten Ausgabe als Cryptosync, um eine dritte Ausgabe (**54**) mit einem ersten Teil und einem zweiten Teil zu erzeugen;
Verschlüsseln der zweiten Ausgabe und des ersten Teils der dritten Ausgabe unter Verwendung des zweiten Teils der dritten Ausgabe als Cryptosync, um eine vierte Ausgabe (**58**) mit einem ersten Teil und einem zweiten Teil zu erzeugen; und
Verschlüsseln des ersten Teils der vierten Ausgabe und des zweiten Teils der dritten Ausgabe unter Verwendung des ersten Teils der vierten Ausgabe als Cryptosync, um eine fünfte Ausgabe (**60**) zu erzeugen

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

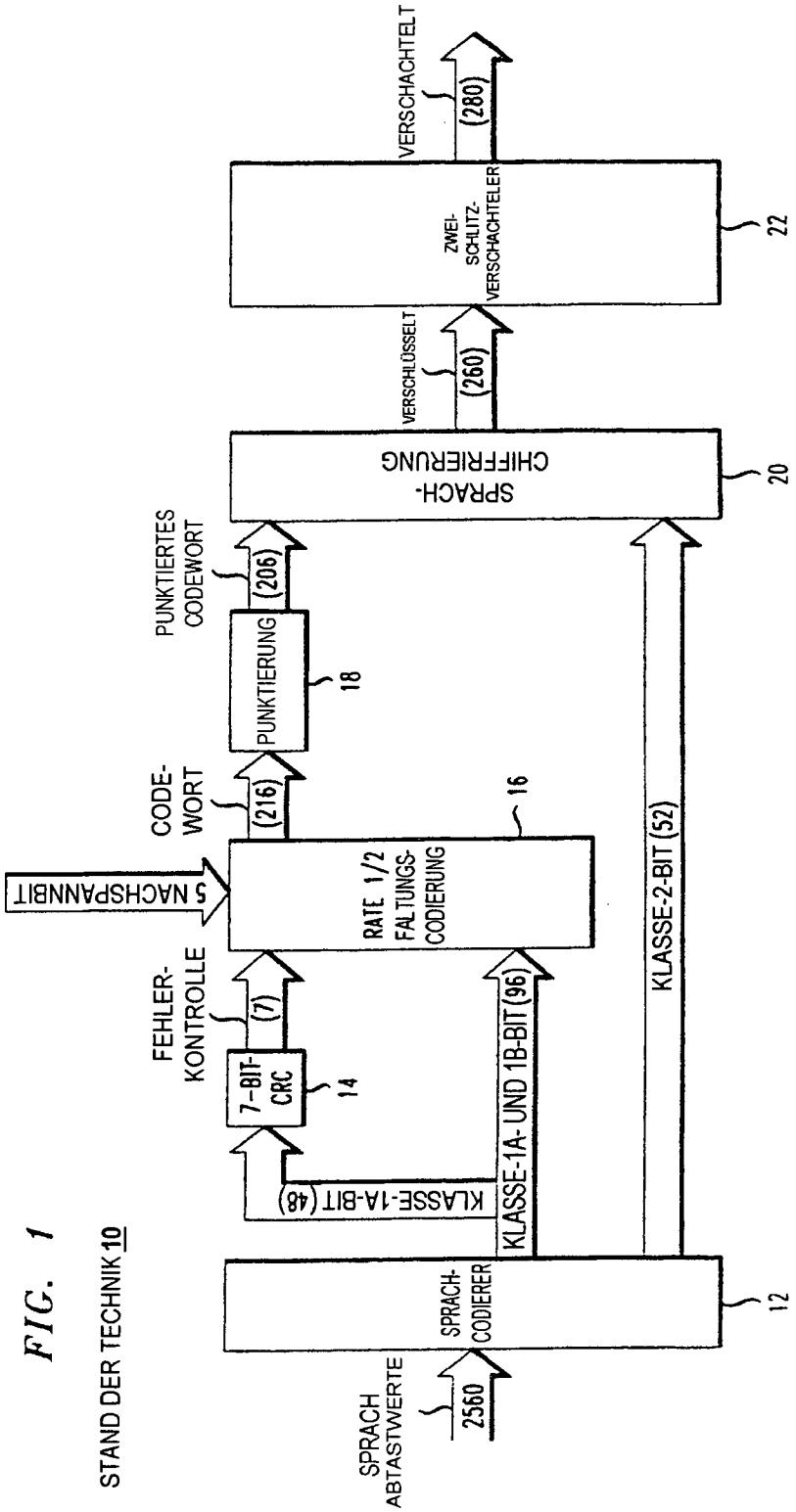


FIG. 1

STAND DER TECHNIK 10

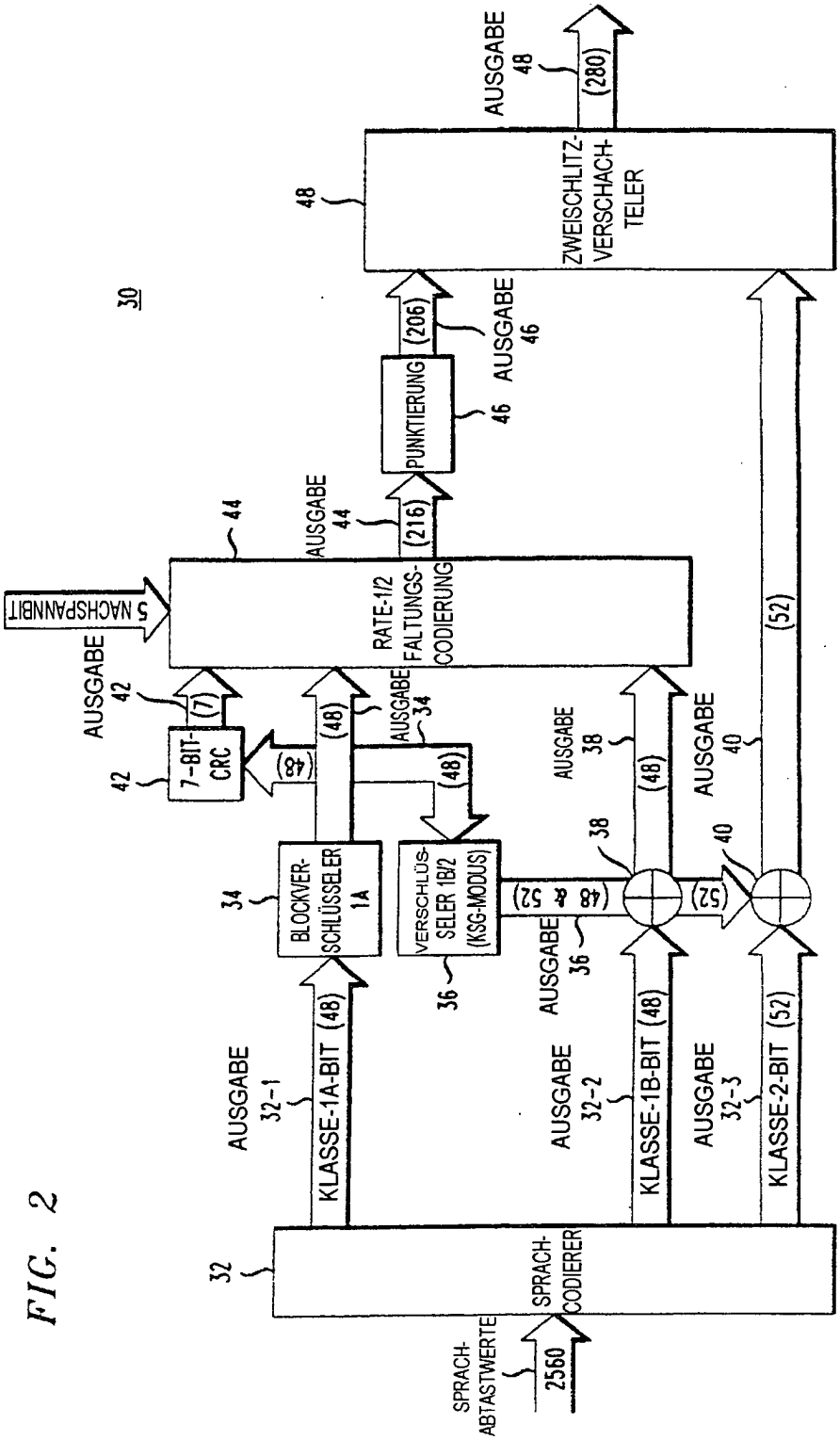

30
SPRACH-ABTASTWERTE
2560
SPRACH-CODIERER
32
AUSGABE 32-1
KLASSE-1A-BIT (48)
AUSGABE 32-2
KLASSE-1B-BIT (48)
AUSGABE 32-3
KLASSE-2-BIT (52)
BLOCKVER-SCHLÜSSELER 1A
34
VERSCHLÜS-SELER 1B/2 (KSG-MODUS)
36
AUSGABE 36
(48 oder 52)
AUSGABE 38
(52)
AUSGABE 40
(52)
7-BIT-CRC
42
(7)
AUSGABE 42
(48)
AUSGABE 34
(48)
5 NACHSPANNBIT
RATE-1/2 FALTUNGS-CODIERUNG
44
AUSGABE 44
(216)
PUNKTIERUNG
46
(206)
AUSGABE 46
ZWEISCHLITZ-VERSCHACH-TELER
48
AUSGABE 48
(280)

FIG. 2

FIG. 3

45

<table>
<tr><td colspan="3">148 CODIERTE SPRACHBIT</td></tr>
<tr><td colspan="2">80 BIT DER ERSTEN EBENE</td><td>68 BIT DER ZWEITEN EBENE</td></tr>
<tr><td>AUSGABE 32-1</td><td>AUSGABE 32-2</td><td>AUSGABE 32-3</td></tr>
<tr><td>ERSTER BLOCK</td><td>ZWEITER BLOCK</td><td>DRITTER BLOCK</td></tr>
<tr><td>48 KLASSE-1A-BIT</td><td>48 KLASSE-1B-BIT
32 BIT DER ERSTEN EBENE
16 BIT DER ZWEITEN EBENE</td><td>52 KLASSE-2-BIT</td></tr>
</table>

FIG. 4

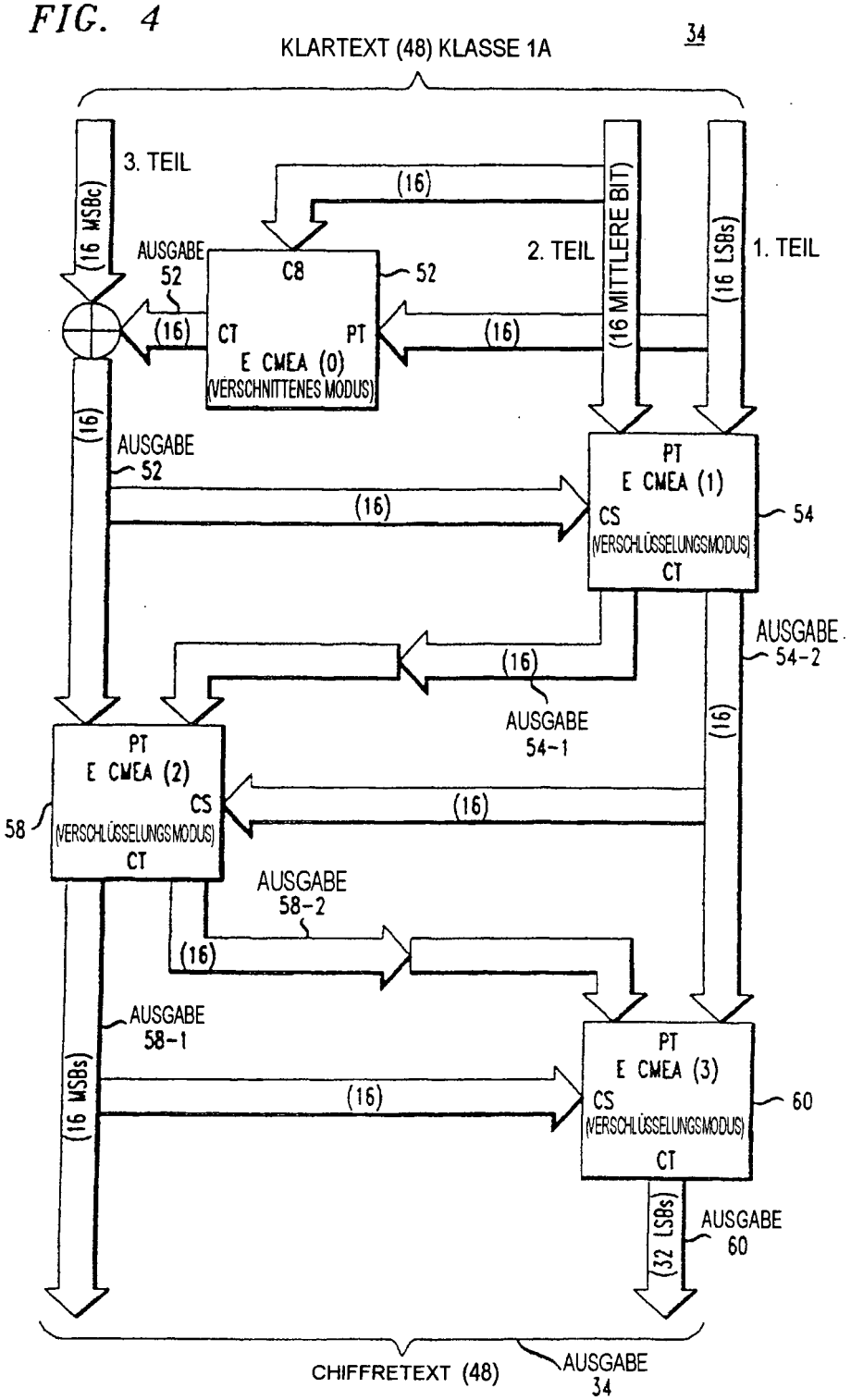

KLARTEXT (48) KLASSE 1A
34
3. TEIL
(16 MSBc)
(16)
AUSGABE
52
C8
52
2. TEIL
(16 MITTLERE BIT)
1. TEIL
(16 LSBs)
(16)
CT
PT
E CMEA (0)
(VERSCHNITTENES MODUS)
(16)
(16)
AUSGABE
52
PT
E CMEA (1)
CS
(VERSCHLÜSSELUNGSMODUS)
CT
54
(16)
AUSGABE
54-2
(16)
AUSGABE
54-1
PT
E CMEA (2)
CS
(VERSCHLÜSSELUNGSMODUS)
CT
58
(16)
AUSGABE
58-2
(16)
AUSGABE
58-1
(16 MSBs)
(16)
PT
E CMEA (3)
CS
(VERSCHLÜSSELUNGSMODUS)
CT
60
(32 LSBs)
AUSGABE
60
CHIFFRETEXT (48)
AUSGABE
34

FIG. 5

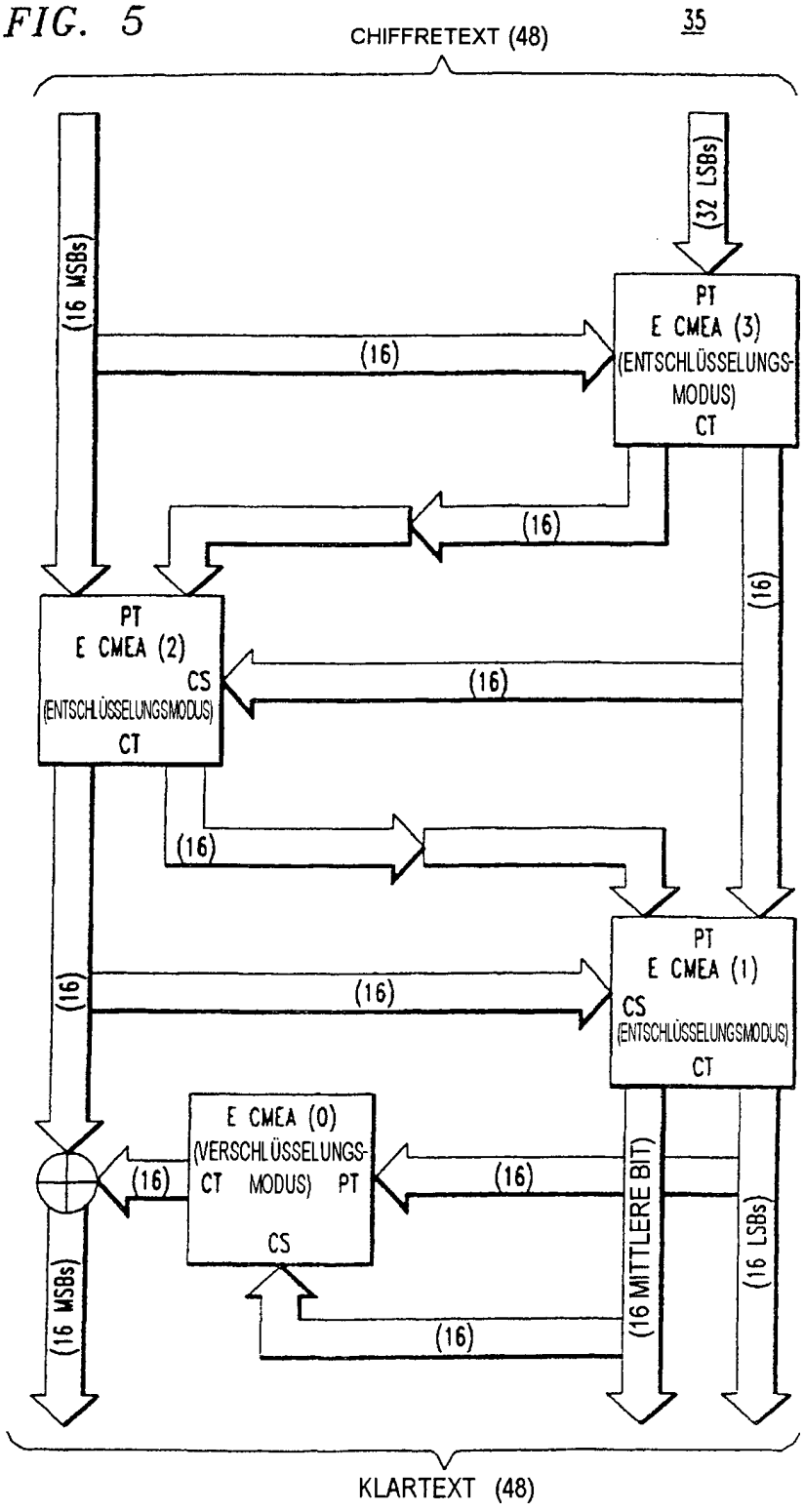
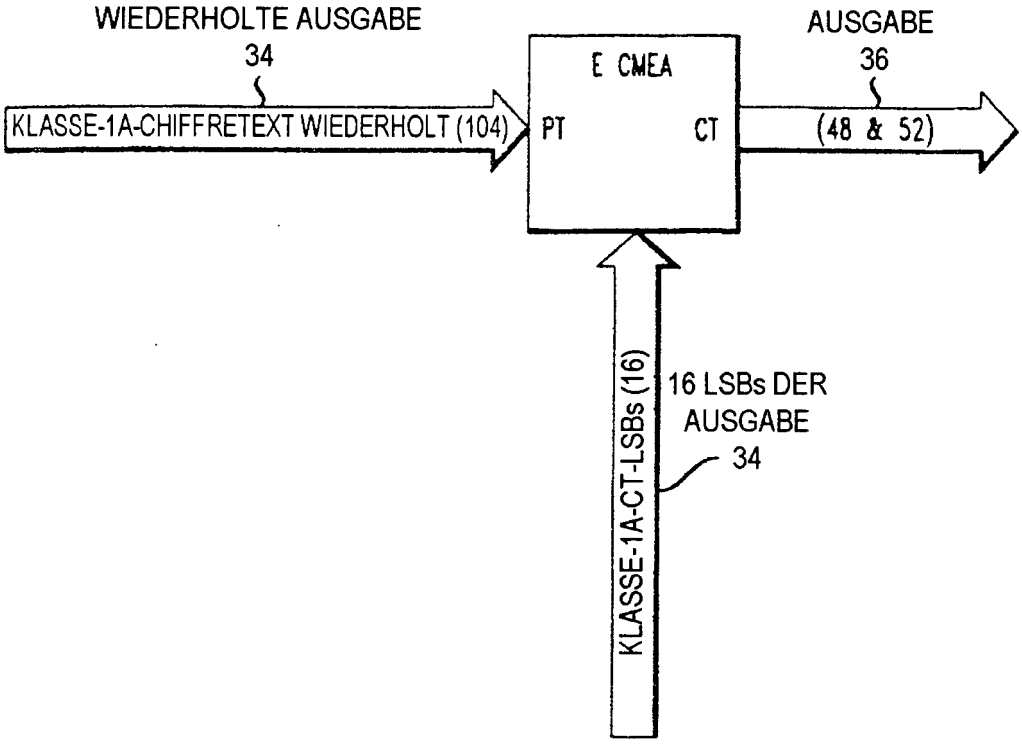

CHIFFRETEXT (48)
35
(16 MSBs)
(32 LSBs)
PT
E CMEA (3)
(ENTSCHLÜSSELUNGS-
MODUS)
CT
(16)
(16)
(16)
PT
E CMEA (2)
CS
(ENTSCHLÜSSELUNGSMODUS)
CT
(16)
(16)
(16)
PT
E CMEA (1)
CS
(ENTSCHLÜSSELUNGSMODUS)
CT
(16)
(16)
E CMEA (0)
(VERSCHLÜSSELUNGS-
CT MODUS) PT
CS
(16)
(16)
(16 MSBs)
(16)
(16 MITTLERE BIT)
(16 LSBs)
KLARTEXT (48)

FIG. 6


WIEDERHOLTE AUSGABE
34
KLASSE-1A-CHIFFRETEXT WIEDERHOLT (104)
E CMEA
PT
CT
AUSGABE
36
(48 & 52)
KLASSE-1A-CT-LSBs (16)
16 LSBs DER
AUSGABE
34

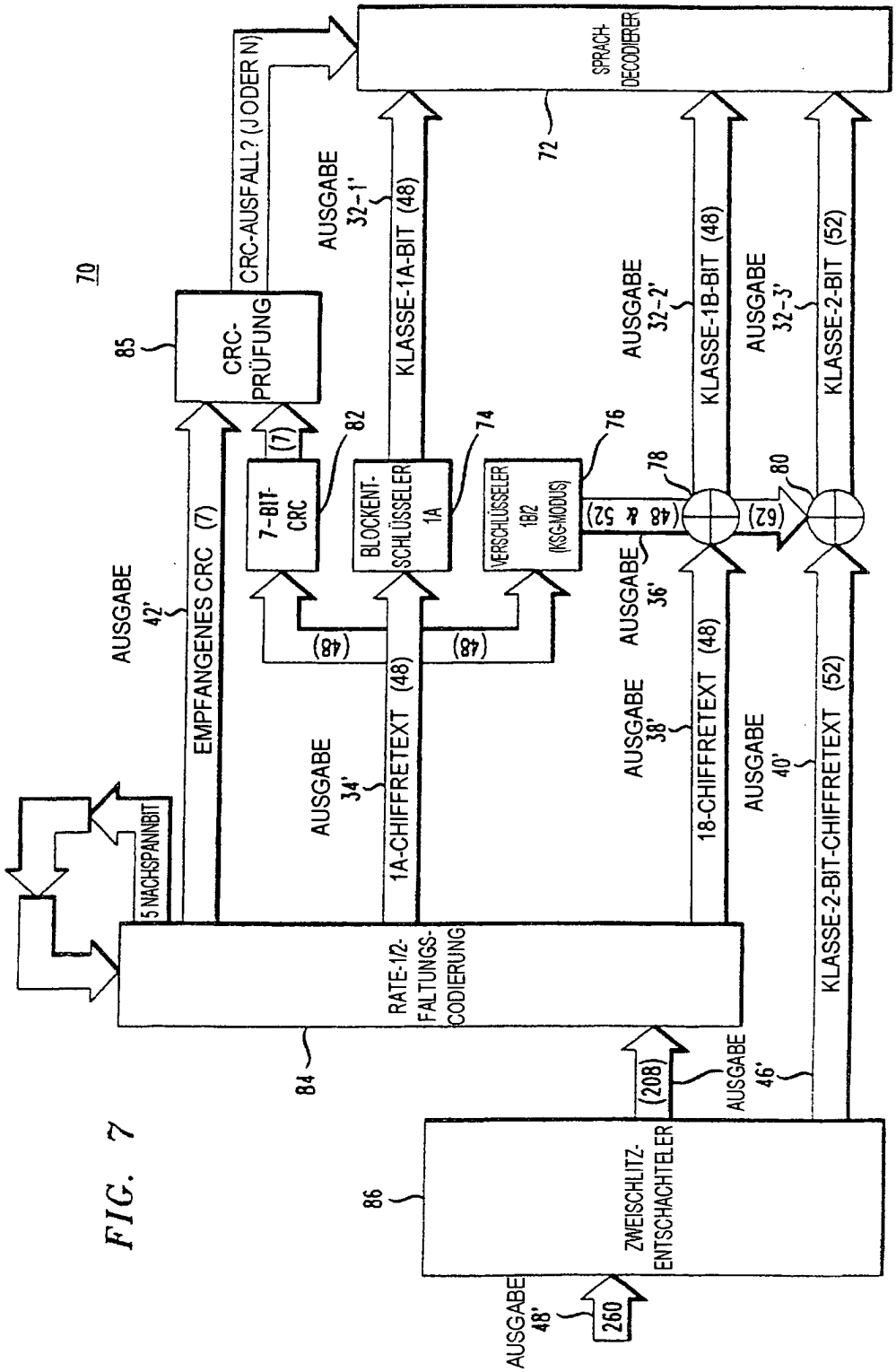

70
SPRACH-DECODIERER
72
CRC-AUSFALL? (J ODER N)
AUSGABE 32-1' (48)
KLASSE-1A-BIT
AUSGABE 32-2' (48)
KLASSE-1B-BIT
AUSGABE 32-3' (52)
KLASSE-2-BIT
85
CRC-PRÜFUNG
82
7-BIT-CRC
(7)
74
BLOCKENT-SCHLÜSSELER 1A
76
VERSCHLÜSSELER 1B/2 (KSG-MODUS)
78
80
(48 & 52)
(62)
AUSGABE 42' (7)
EMPFANGENES CRC
AUSGABE 34' (48)
1A-CHIFFRETEXT
AUSGABE 36' (48)
18-CHIFFRETEXT
AUSGABE 40' (52)
KLASSE-2-BIT-CHIFFRETEXT
(48)
(48)
5 NACHSPANNBIT
AUSGABE 38'
RATE-1/2-FALTUNGS-CODIERUNG
84
(208)
AUSGABE 46'
86
ZWEISCHLITZ-ENTSCHACHTELER
AUSGABE 48'
260

FIG. 7

FIG. 8

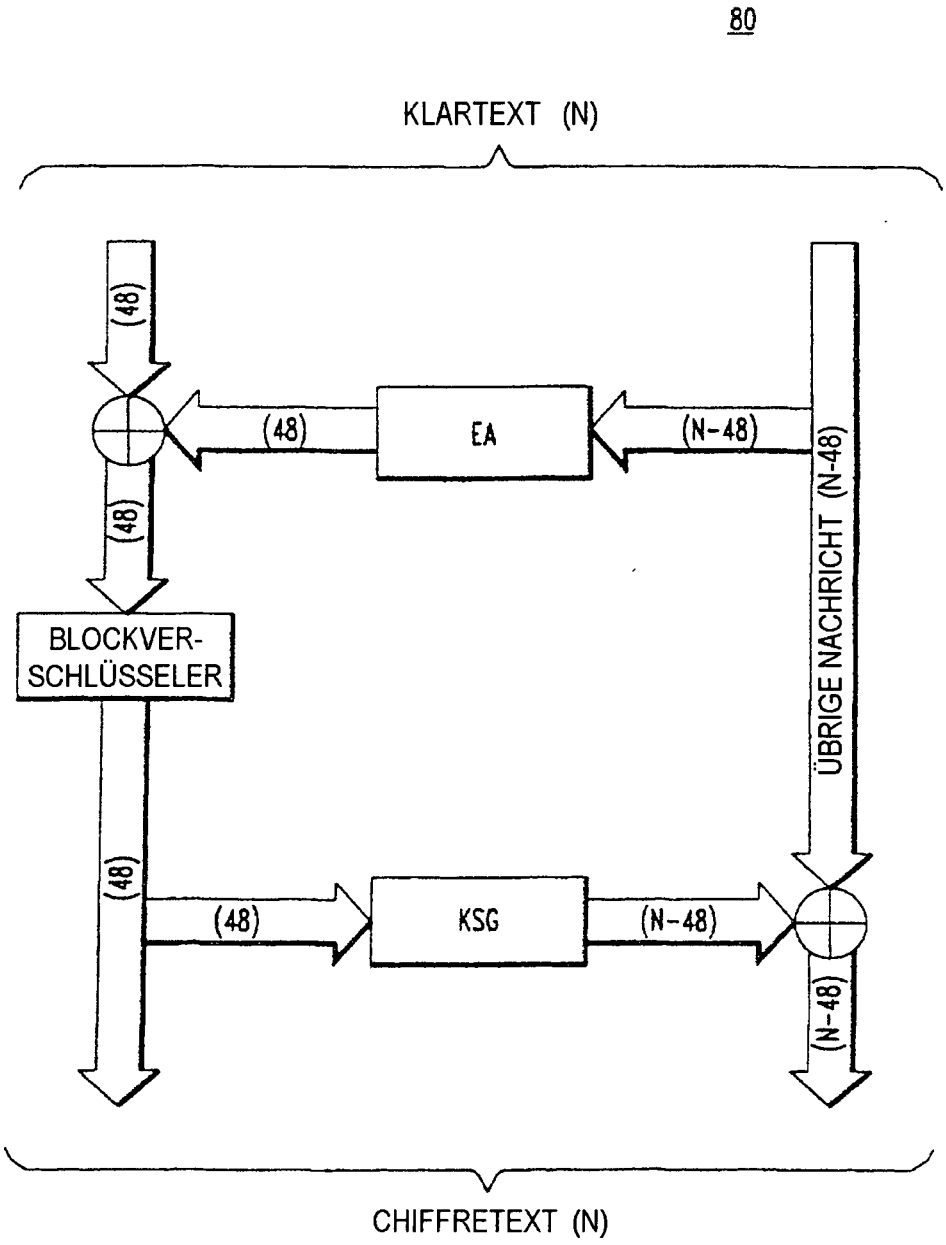

80
KLARTEXT (N)
(48)
(48)
EA
(N-48)
ÜBRIGE NACHRICHT (N-48)
(48)
BLOCKVER-
SCHLÜSSELER
(48)
(48)
KSG
(N-48)
(N-48)
CHIFFRETEXT (N)

FIG. 9

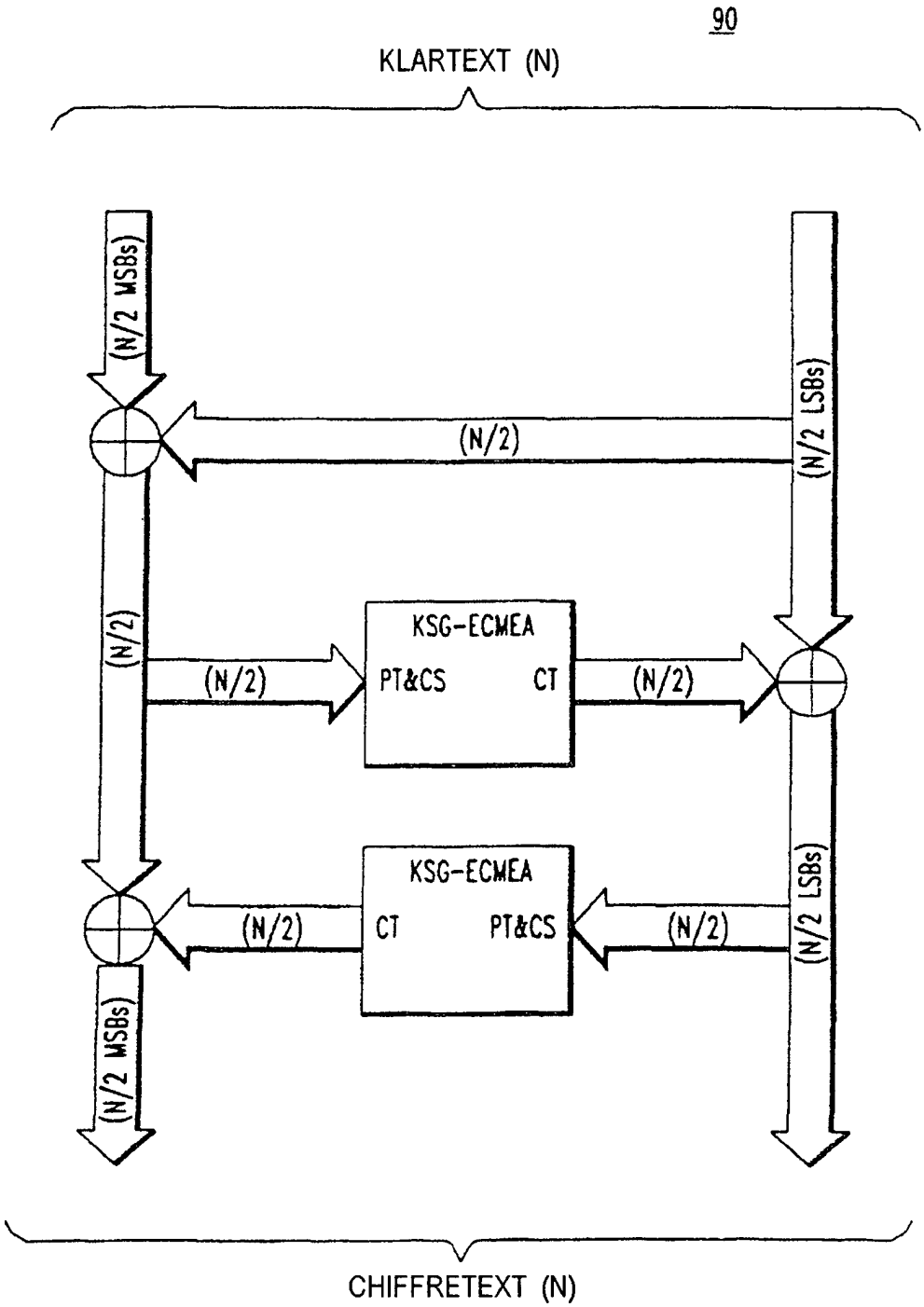
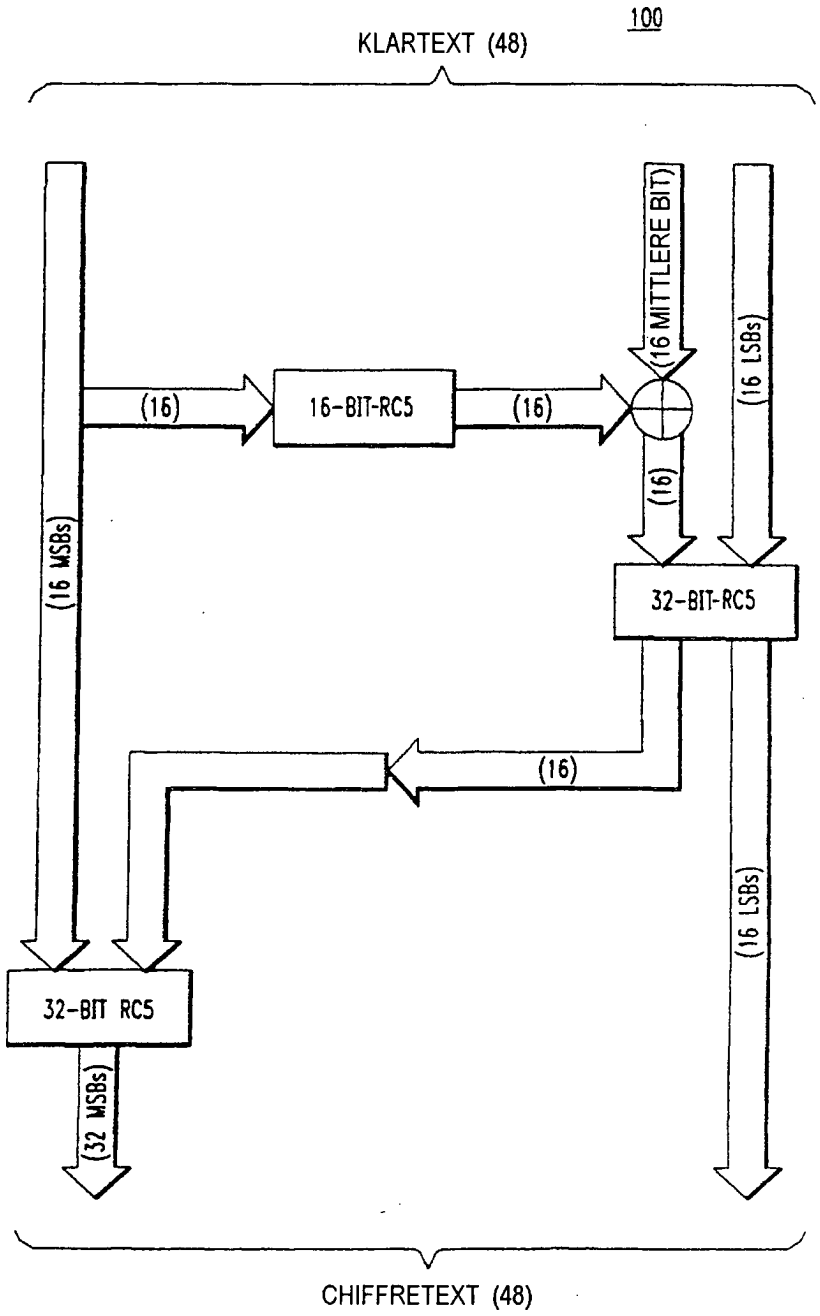

90
KLARTEXT (N)
(N/2 MSBs)
(N/2)
(N/2 LSBs)
(N/2)
KSG-ECMEA
PT&CS
CT
(N/2)
(N/2)
KSG-ECMEA
CT
PT&CS
(N/2)
(N/2)
(N/2 LSBs)
(N/2 MSBs)
CHIFFRETEXT (N)

FIG. 10


100
KLARTEXT (48)
(16 MITTLERE BIT)
(16 LSBs)
(16)
16-BIT-RC5
(16)
(16 MSBs)
(16)
32-BIT-RC5
(16)
(16 LSBs)
32-BIT RC5
(32 MSBs)
CHIFFRETEXT (48)