(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 561 841**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **85 04296**

(51) Int Cl⁴ : H 04 L 11/26; H 04 B 7/26; H 04 M 15/10.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 22 mars 1985.

(30) **Priorité :** DE, 24 mars 1984, n° P 34 10 937.4.

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 39 du 27 septembre 1985.

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *NV PHILIPS' GLOEILAMPENFABRIEKEN, société anonyme de droit néerlandais.* — NL.

(72) **Inventeur(s) :** Stefan Scheinert et Christoph Grauel.

(73) **Titulaire(s) :**

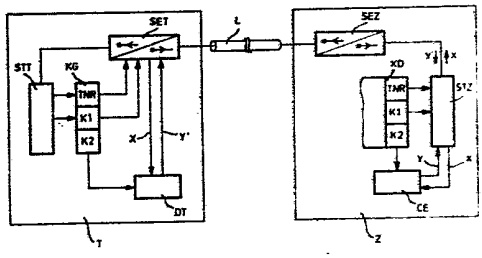
(74) **Mandataire(s) :** Jean Chaffraix, société civile SPID.

(54) Procédé pour reconnaître l'utilisation illicite d'une identification.

(57) Pour distinguer les divers postes d'abonné d'un système de transmission d'informations peuvent être utilisées les soi-disant identifications. L'écoute de l'échange des informations transmises dans un canal L de transmission d'informations entre le poste d'abonné T1 et le central Z permet à un manipulateur d'écouter l'identification et, de ce fait, de demander des services du central par imitation de l'identification étrange.

Pour reconnaître l'imitation de l'identification d'un poste d'abonné dans le central, celui-ci émet au moyen du générateur KG une clef continuellement variable pour l'identification du poste d'abonné; on peut aussi combiner des données fixes et des données variables.

Application : radiotéléphone.



FR 2 561 841 - A1

"Procédé pour reconnaître l'utilisation illicite d'une identification"

L'invention concerne un procédé pour reconnaître l'utilisation illicite d'une identification attribuée à un poste d'abonné d'un système de transmission d'informations, dans lequel des données fixes stockées dans le poste d'abonné (numéro d'abonné, identification caractéristique du poste d'abonné) sont comparées et évaluées pendant l'établissement de communication avec des données fixes stockées dans le central.

Pour distinguer les divers postes d'abonné d'un système de transmission d'information peuvent être utilisés les soi-disant identifications. D'une façon générale, la comptabilité des appels est proposée pour l'identification du poste d'abonné.

Dans le cas d'un système de transmission radio, la comptabilité des appels pour les communications introduites par une poste radio mobile s'effectue dans un central de transmission radio. Du texte de brevet allemand N° 2 419 615 est connu un procédé pour l'identification d'un poste d'abonné (station radio mobile), permettant de reconnaître l'utilisation illicite de l'identification (numéro d'abonné et identification caractéristique) du poste radio mobile dans le système de transmission radio. L'identification est stockée dans le poste radio mobile dans un générateur de signaux d'identité, ce à quoi peut être utilisée par exemple une carte magnétique. Pour faire fonctionner le poste radio mobile, le générateur de signaux d'identité est glissé dans une fente de l'appareil de manoeuvre du poste radio mobile et les données sont lues par un dispositif de lecture de l'appareil de manoeuvre et amenées à un dispositif de commande dans l'appareil de manoeuvre. Pour éviter des imitations des cartes magnétiques selon l'annuaire de téléphone, un deuxième numéro d'abonné "secret" (identification caractéristique) est attribué à chaque abonné

du système de transmission radio et stocké dans la carte magnétique.

Pour l'examen d'identité conformément au texte précité 2 419 615, l'accord de la ré-identification et du numéro d'abonné est examiné. A cet effet, l'identification caractéristique émise par un poste radio mobile pour l'examen de son identité et formée à l'aide d'une clef non connue à l'abonné à partir du numéro d'abonné est transmise au central de transmission radio. Dans le central de transmission radio l'identification caractéristique obtenue du poste d'abonné mobile est déchiffrée à l'aide de la clef inverse. Par suite du déchiffrement, il se forme comme-identification le numéro d'appel (numéro d'abonné du poste radio mobile en question).

Des identifications manipulées, par exemple des identifications formées sans utilisation de la clef non connue à l'abonné sont également déchiffrées dans le central de transmission radio, il est vrai, et transmises comme ré-identification au poste radio mobile. L'identification ainsi formée ne correspond cependant pas à celle identique au numéro d'abonné du poste mobile. Dans le cas d'une comparaison de la ré-identification reçue avec par exemple le numéro d'abonné mentionné sur la carte magnétique dans le récepteur de ré-identification, l'accord faisant défaut est déterminé et la liaison radio formée est éliminée.

Un tel procédé dans lequel est utilisée une clef fixe, n'offre cependant guère de protection dans le cas d'identifications manipulées fournies de façon illicite par l'écoute de tiers de l'échange d'information sur le canal de transmission radio. Lorsque l'échange d'information sur le canal de transmission radio est épié, une manipulation du générateur de signaux d'identité aussi bien que du dispositif de commande (récepteur de ré-identification dans le poste radio mobile) permet

d'atteindre que les taxes téléphoniques accumulées pour ce poste radio mobile seront imputées à un autre abonné du système de transmission radio.

Un autre service accessible au public est un système de transmission télétext. Comme le décrit (TE KA DE Technische Mitteilungen 1980, page 21 chapitre 5 "Verbindungsaufbau"), l'établissement de communication est amorcé par un abonné par manoeuvre de la télécommande d'un téléviseur. Lorsqu'une ligne d'un poste d'abonné vers le central de télétext est libre, le choix automatique du numéro d'appel correspondant au central commence après fermeture de la boucle, afin d'assurer l'alimentation en courant du modem de telétext. Lorsque la communication avec le central peut être établie, le numéro d'abonné (identification) stocké dans le poste d'abonné pour le central de télétext est transmis à l'aide d'un système de commande prévu dans le poste d'abonné. Dans le central de télétext, l'identification, qui est constituée par exemple par au maximum 11 chiffres d'un code ISO-7-bits et un mot de contrôle numérique additionnel, sert à un examen d'autorisation et à une imputation de taxes correcte. De plus, on peut prévoir que le central de télétext demande un soi-disant mot d'ordre (identification) au poste d'abonné avant que le central de télétext ne libère l'accès aux informations y stockées.

Dans ce cas aussi, l'identification (numéro d'abonné et identification) caractéristique peut être écoutée par des méthodes analogues à celles utilisées pendant l'écoute de téléphone et l'identification stockée fixement dans un générateur de signaux d'identité du modem de télétexte peut être modifiée pour des intentions frauduleuses.

L'invention est basée sur l'idée d'empêcher que des taxes ne puissent être imputées à l'autres abonnés du système de transmission de communication par identifications manipulées pouvant être obtenues de façon

illicite par écoute de l'échange d'informations sur un canal de transmission d'information.

Pour résoudre ce problème selon une première caractéristique de l'invention, un procédé du genre mentionné dans le préambule est remarquable en ce que le central Z émet une valeur choisie pseudo aléatoirement X que, dans le poste d'abonné T, la valeur reçue X ensemble avec une deuxième identification caractéristique K2 stockée avec le poste d'abonné T sont amenées à un dispositif de déchiffrage DT et que le dispositif de déchiffrage DT en dérive une nouvelle valeur Y', qui est transmise au central Z et y est comparée avec une nouvelle valeur Y' formée à la sortie d'un dispositif de chiffrage CE, à partir de la combinaison de la deuxième identification caractéristique K2 stockée dans un fichier d'identification KD et attribuée au poste d'abonné T avec la valeur choisie aléatoirement X.

Pour résoudre ce problème selon une seconde caractéristique de l'invention, un procédé du genre mentionné dans le préambule est remarquable en ce que dans le poste d'abonné T et le central Z sont présentes des données variables additionnelles et que lors de l'établissement de communication au central, les données fixes et variables sont transmises, comparées et évaluées ensemble.

L'utilisation d'une clef variable (valeur X choisie accidentellement) selon la première caractéristique de l'invention permet d'empêcher l'utilisation non permise d'une identification pouvant être obtenue de façon illicite par écoute des échanges d'information sur le canal de transmission d'informations. Lorsqu'éventuellement après un multiple de tentatives infructueuses, un manipulateur s'est procuré de façon illicite une clef, un changement de clef permet d'empêcher que le manipulateur ne puisse demander des services aux frais d'autres abonnés du système de transmission d'informa-

tions. Pour améliorer davantage la mesure de sûreté, il est possible d'exclure le poste d'abonné de la prise de services du central (par exemple de central de télétext) après plusieurs tentatives infructueuses avec des identifications manipulées.

Dans le cas de la deuxième caractéristique de l'invention, l'utilisation non permise d'une identification que le manipulateur s'est procuré de façon illicite par reproduction du générateur de signaux d'identité ou par écoute de l'échange d'informations sur le canal de transmission d'informations peut être reconnue. Selon cette deuxième caractéristique, les données fixes, comme le numéro d'abonné et l'identification caractéristique, peuvent être combinées avec les données variables. Lorsque les données fixes stockées sont reproduites, le manipulateur ne peut pas avoir de communications aux frais d'un autre abonné, du fait qu'il ne connaît pas les données variables stockées. Ce n'est qu'après reproduction des données fixes stockées et écoute des données variables qu'un manipulateur peut avoir des communications aux frais de l'autre abonné du système de transmission d'informations. Toutefois, ces données variables sont modifiées pendant le fonctionnement des deux postes d'abonné, de sorte que, lors de la première communication respectivement pendant la première demande de service, dans certaines conditions, une telle manipulation ne pourra pas être reconnue. Lors d'un fonctionnement poursuivi des deux postes d'abonné,il s'établit des données inégales variables, qui aboutissent à des résultats de comparaison ddifférents dans le central. Vu sur une plus longue période, le manipulateur ne peut pas demander de services sans que l'utilisation illicite de l'identification ne soit reconnue. Un autre avantage du procédé conforme à l'invention réside dans le fait que la quantité de données variables peut être réduite de sorte de le générateur de signaux d'identité (mémoire pour les données fixes), par exemple une carte magnétique, peut

être réalisé d'une façon plus simple.

Lorsque, selon une des caractéristiques de l'invention comme données variables sont utilisés les établissements de communication variables réussis du poste d'abonné, il est possible de simplifier facilement le processus de comparaison et d'évaluation dans le central. En effet, la comparaison de données codées, notamment de deux positions de compteur, peut être effectuée avec des circuits de logique de structure simple.

Dans la plupart des cas, des identifications manipulées sont procurées de façon illicite par écoute de l'échange d'informations sur le canal de transmission d'informations. Dans le cas d'un procédé remarquable en ce que la position de compteur ZS' du compteur ZZ du poste d'abonné T est amenée à un dispositif de codage VE qui en dérive une position de compteur codée VZS', une position de compteur codée est dérivée à l'aide d'un dispositif de codage. Du fait que le manipulateur ne connaît la position de compteur actuelle, ni la clef pour le codage de la position du compteur, il est possible d'atteindre un perfectionnement poursuivi de la mesure de sûreté.

Afin d'empêcher que la clef servant au codage de la position du compteur ne soit décodée par un multiple de tentatives conformément au procédé remarquable en ce que des données fixes additionnelles K2 connues du central Z sont amenées au dispositif de codage VE qui en dérive la position de compteur codée VZS', des données fixes sont amenées de façon additionnelle au dispositif de codage et combinées avec la position de compteur amené au dispositif de codage.Il en résulte des clefs pour plusieurs postes d'abonné du système de transmission d'informations, de sorte que les dépenses pour le décodage de la clef sont très élevées.

Selon les procédés remarquables en ce que comme données variables, dans le cas d'un établissement de communication, n'est émise qu'une partie TSZ' de la position de compteur ZS' du poste d'abonné T du fait que dans un circuit sélectionneur AST sont choisies certaines positions de bit dans la position de compteur codée amenée VZS' et en ce que comme données variables pendant un fonctionnement

de communication n'est émise qu'une partie TZS' de la position de compteur ZS' du poste d'abonné T du fait que dans un circuit sélectionneur AST est formée la somme des chiffres de la position de compteur codée amenée VZS', le poste d'abonné n'émet comme données variables qu'une partie de la position décodée du compteur, qui se forme par exemple par choix de certaines positions de bit ou par formation de sommes des chiffres. Lorsqu'un manipulateur écoute l'échange d'informations sur le canal de transmission d'informations, il ne reonnaît qu'une partie de la position codée du compteur, mais non toute la position de compteur. En effet, dans le cas de formation des sommes de chiffres de la position de compteur codée jsuqu'à un nombre déterminé de positions de compteur, toujours la même "transversale", par exemple jusqu'aux positions de compteur 005, 122, 221, la somme "transversale" décimale 5. Ainsi, le manipulateur ne peut essayer que de deviner la position entière du compteur, de sorte que, d'une façon générale, la première tentative du manipulateur peut déjà être reconnue.

L'invention sera décrite et expliquée ci-après à l'aide des formes de réalisation représentées sur le dessin.

La figure 1 montre un schéma synoptique d'une première forme de réalisation et

La figure 2 montre comme schéma synoptique une deuxième forme de réalisation de l'invention.

Le schéma synoptique selon la figure 1 montre les dispositifs utilisés dans le procédé conforme à l'invention dans un poste d'abonné T et un central Z du système de transmission d'informations. Dans le poste d'abonnée T et dans le central Z sont prévus des systèmes de commande STT et STZ à l'aide desquels est commandé l'établissement des communications. Lorsqu'un poste d'abonné T veut demander des services du central Z, le central Z invite le poste d'abonné T à faire connaître son identification. Pour cette identification, le poste d'abonné T émet l'identification stockée dans un générateur de signaux d'identité KG, par exemple une carte magnétique, à l'aide d'un dispositif d'émission et de réception SET prévu dans le poste d'abonné T, sur un canal de transmission d'informations L vers le central Z. L'identification émise comprend un numéro d'abonné TNR stocké dans le générateur de signaux d'identité

KG et une première identification caractéristique K1. Dans le central Z, l'identification émise est reçue par un dispositif d'émission et de réception SEZ, amenée au système de commande STZ et comparée à l'aide de ce dernier, avec une identification (numéro d'abonné TNR et première identification caractéristique K1) stockée dans un fichier d'identification caractéristique KD et évaluée.

Le central Z émet au poste d'abonné T une valeur choisie d'une manière aléatoire X, c'est-à-dire une seule variable donnée d'une manière aléatoire au préalable. Dans le poste d'abonné T, la valeur reçue X est amenée à un dispositif de déchiffrage DT, ensemble avec une deuxième identification caractéristique K2 stockée dans le poste d'abonné T dans le générateur de signaux d'identité KG. Le dispositif de déchiffrage DT dérive une nouvelle valeur Y' de la valeur X et de la deuxième identification K2. Cette nouvelle valeur Y' est transmise au central Z par l'intermédiaire du canal de transmission d'information L et comparée avec une nouvelle valeur qui y est calculée : Y. Lorsque les deux valeurs Y, Y' correspondent, l'abonné peut demander les services du central Z.

L'échange continué de la clef, c'est-à-dire le choix accidentel de la valeur X dans le central Z permet d'atteindre que l'identification d'un poste d'abonné T ne sera connue d'un manipulateur par écoute de l'échange d'informations sur le canal de transmission d'informations L.

Dans le procédé conforme à l'invention représenté sur la figure 2 sont présentes des données varaibles additionnelles dans le poste d'abonné T et dans le central Z. Dans cette forme de réalisation, on utilise comme données le nombre d'établissement de communication réussis du poste d'abonné T. Le contenu d'un compteur ZZ prévu dans le poste d'abonné T est augmenté par exemple d'une unité à chaque établissement de communication. La position de compteur ZS' à prendre aux sorties Q_o au Q_n est transmise par le dispositif d'émission et de réception SET par l'intermédiaire du canal de transmission d'information L, reçue à partir du dispositif d'émission et de réception SEZ par le central Z et amenée au système de commande STZ. A chaque établissement de communication réussi de ce poste d'abonné T, la position du compteur ZZ1 est augmentée d'une unité à l'aide d'un système de commande STZ. Dans le

cas d'une augmentation de la position de compteur supérieure à l'unité, par exemple d'une différence montant de façon linéaire jusqu'à la valeur maximale, il faut des compteurs et des mémoires pour la différence utilisée en dernier lieu, dans le poste d'abonné T et le central Z, par exemple pour la commande. Dans le cas d'un établissement de communication conforme au procédé décrit à l'aide de la figure 1, le numéro d'abonné TNR, la première identification caractéristique K1 et les positions de compteur ZS' sont transmis au central Z au cours d'une première communication, commandée par le système de commande STT dans le poste d'abonné T et y sont comparés avec le numéro d'abonné TNR et la première identification caractéristique K1, aussi bien qu'avec la position de compteur du compteur ZZ1 stockés dans le fichier d'identification KD.

Lorsque le numéro d'abonné TNR, la première identification caractéristique K1 et les données variables, par exemple la position de compteur, sont égaux entre eux, l'abonné peut demander les services au central Z.

Lorsque les compteurs ZZ et ZZ1 indiquent des positions différentes, le central Z invite le poste d'abonné T à donner la deuxième identification caractéristique K2 à l'aide d'un ordre d'identification. Le central Z compare la deuxième identification caractéristique reçue K2 avec l'identification caractéristique K2 stockée dans le fichier d'identification caractéristique KD et déclenche l'alarme dans le cas de non accord des deuxièmes identifications caractéristiques KD.

Lorsque les deuxièmes identifications caractéristiques KD s'accordent entre elles, le compteur ZZ1 du système de commande central STZ est mis sur la position du compteur ZZ du poste d'abonné T. Avec chaque établissement de communication suivant et réussi, les deux positions de compteur sont augmentées de l'unité. Dans le central Z est stockée l'identification du poste d'abonné T. Lorsqu'au cours des établissements de communication suivants, les deux positions des compteurs ZZ et ZZ1 s'accordent, la mémorisation de l'identification du poste d'abonné T est

dissoute.

Dans le cas où toutes les comparaisons suivantes aboutissent à un résultat négatif, le poste d'abonné T est bloquée.

Dans la réalisation représentée sur la figure 2, la position de contrôle ZS' du compteur ZZ du poste d'abonné T est amenée à un dispositif de codage VE, qui en dérive une position de compteur codée VZS'. Dans le central Z est prévu un dispositif de décodage correspondant EE, qui dérive également une position de compteur codée VZS de la position de compteur ZS du compteur ZZ1. Lorsque le processus d'identification comprend la comparaison des positions de compteur codées VZS' et VZS, la manipulation d'identification peut être reconnue d'une façon simple. Un manipulateur, qui ne connaît pas la clef et la position de compteur ZS' du compteur ZZ ne peut émettre que par hasard des données variables exactes, de sorte que, d'une façon générale, après un multiple de tentatives fructueuses, le manipulateur est abandonné.

Pour perfectionner davantage les mesures de sûreté, des données fixes additionnelles, notamment une deuxième identification caractéristique K2, qui est connue du central Z, est amenée au dispositif de codage VE. Le dispositif de codage VE du poste d'abonné T dérive de la combinaison de la deuxième identification caractéristique amenée K2 et de la position de compteur ZS' la position de compteur codée VZS'. Le dispositif de décodage EE prévu dans le central Z permet d'effectuer le même processus de codage de la position de compteur ZS du compteur ZZ1. Le processus de comparaison s'effectue de la façon déjà décrite ci-dessus.

Une autre amélioration des mesures de sûreté peut s'obtenir lorsque comme données variables, dans le cas d'un établissement de communication, seule une partie de la position de compteur ZS' du poste d'abonné T est émise. A cet effet, un circuit sélectionneur AST est prévu dans le poste d'abonné T et assure la sélection de certaines positions de bit par exemple dans la position de

compteur codée amenée VZS'. Une autre forme de réalisation est ainsi caractérisée en ce que le circuit sélectionneur AST soumet la position de compteur codée amenée VZS' à une formation de somme des chiffres.

Lorsqu'une manipulateur écoute l'échange d'informations sur le canal de transmission d'information L, il ne connaît qu'une partie de la position de compteur codée VSZ' mais non toute la position de compteur codée VZS'. Du fait que dans le cas d'une formation de la somme des chiffres, respectivement dans le cas d'une réduction de la position de compteur par le choix de certaines positions de bit, il s'agit d'un nombre déterminé de positions de compteur ZS', il ne reste au maximum au manipulateur que d'essayer de deviner la position entière du compteur ZS'. D'une façon générale, la première tentative du manipulateur pour deviner les données variables est déjà reconnue et des mesures correspondantes peuvent être prises.

Un autre cas d'application du procédé conforme à l'invention réside dans le monde du crédit et de paiement pour lequel des données fixes et variables sont stockées dans une carte magnétique. Les données variables sont alors par exemple le solde de compte de l'abonné ou un mode choisi dans une phrase de mots de code.

REVENDICATIONS:

1. Procédé pour reconnaître l'utilisation illicite d'une identification attribuée à un poste d'abonné d'un système de transmission d'informations, dans lequel des données fixes stockées dans le poste d'abonné (numéro d'abonné, identification caractéristique du poste d'abonné) sont comparées et évaluées pendant l'établissement de communication avec des données fixes stockées dans le central, caractérisé en ce que le central Z émet une valeur choisie pseudo aléatoirement X que, dans le poste d'abonné T, la valeur reçue X ensemble avec une deuxième identification caractéristique K2 stockée dans le poste d'abonné T sont amenées à un dispositif de déchiffrage DT et que le dispositif de déchiffrage DT en dérive une nouvelle valeur Y', qui est transmise au central Z et y est comparée avec une nouvelle valeur Y' formée à la sortie d'un dispositif de chiffrage CE, à partir de la combinaison de la deuxième identification caractéristique K2 stockée dans un fichier d'identification KD et attribuée au poste d'abonné T avec la valeur choisie aléatoirement X.

2. Procédé pour reconnaître l'utilisation illicite d'une identification attribuée à un poste d'abonné d'un système de transmission d'informations, dans lequel les données fixes (numéros d'abonné, identification caractéristique du poste d'abonné) stockées dans le poste d'abonné sont comparées et évaluées pendant l'établissement de communication avec des données fixes stockées dans le central, caractérisé en ce que dans le poste d'abonné T et le central Z sont présentes des données variables additionnelles et que lors de l'établissement de communication au central, les données fixes et variables sont transmises, comparées et évaluées ensemble.

3. Procédé selon la revendication 2, caractérisé en ce que des données fixes et variables sont stockées dans

une carte magnétique.

4. Procédé selon la revendication 2, caractérisé en ce que comme données variables sont utilisés les établissements de communication réussis du poste d'abonné T et que dans le poste d'abonné T et dans le central Z sont prévus chaque fois un compteur ZZ, et un compteur ZZ1, ces compteurs ZZ, ZZ1 étant augmentés dans leur position à chaque établissement de communication réussi.

5. Procédé selon la revendication 2, caractérisé en ce que la position de compteur ZS' du compteur ZZ du poste d'abonné T est amenée à un dispositif de codage VE qui en dérive une position de compteur codée VZS'.

6. Procédé selon la revendication 5, caractérisé en ce que des données fixes additionnelles K2 connues du central Z sont amenées au dispositif de codage VE qui en dérive la position de compteur codée VZS'.

7. Procédé selon l'une des revendications 2 à 6, caractérisé en ce que comme données variables, dans le cas d'un établissement de communication, n'est émise qu'une partie TSZ' de la position de compteur ZS' du poste d'abonné T du fait que dans un circuit sélectionneur AST sont choisies certaines positions de bit dans la position de compteur codée amenée VZS'.

8. Procédé selon l'une des revendications 2 à 6, caractérisé en ce que comme données variables pendant un établissement de communication n'est émise qu'une partie TZS' de la position de compteur ZS' du poste d'abonné T du fait que dans un circuit sélectionneur AST est formée la somme des chiffres de la position de compteur codée amenée VZS'.

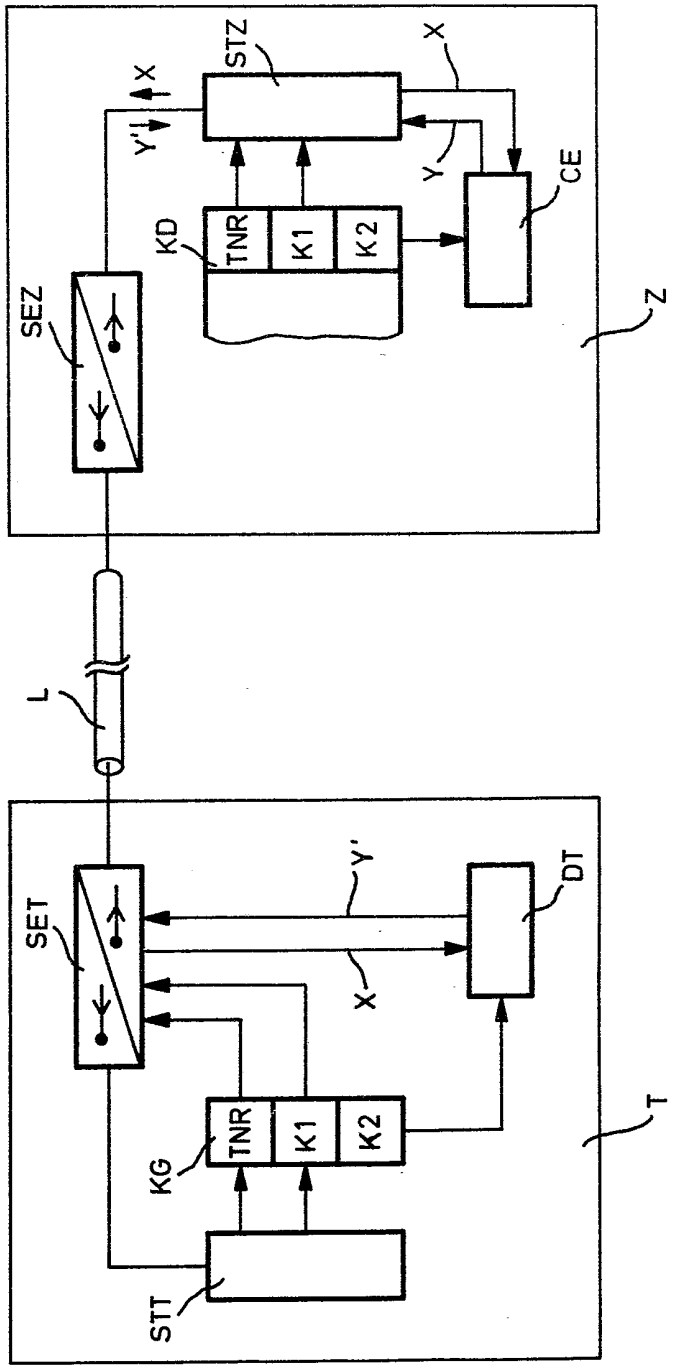


Fig. 1

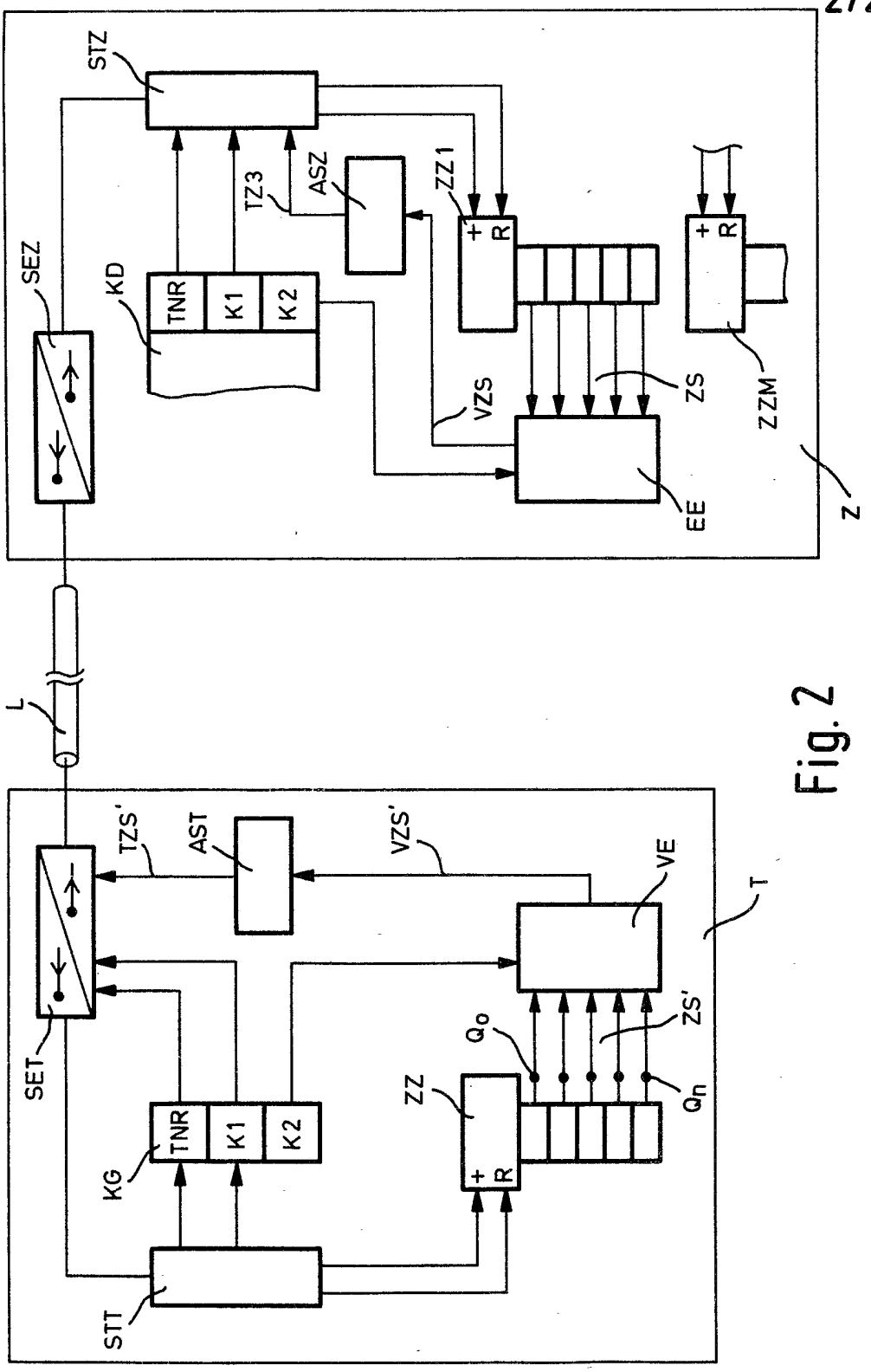

STZ
TZ3
ASZ
ZZ1
SEZ
KD
TNR
K1
K2
VZS
ZS
ZZM
EE
Z
L
TZS'
AST
VZS'
VE
T
SET
ZS'
Q_o
Q_n
ZZ
KG
TNR
K1
K2
STT

Fig. 2