ORGANISATION AFRICAINE DE LA PROPRIETE INTELLECTUELLE (O.A.P.I.)

(19) OAPI

(11) N° 12153

(51) Inter. Cl.[7] H04L 9/00

BREVET D'INVENTION

(21) **Numéro de dépôt :** 1200200070

(22) **Date de dépôt :** 24.08.2000

(30) **Priorité(s) :** CH
30.08.1999 N° 1573/99
US
03.04.2000 N° 60/194,171

(24) **Délivré le :** 26.03.2003

(45) **Publié le :** 08 MAI 2006

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

Société dite : NAGRACARD SA
22, route de Genève
CH-1033 CHESEAUX-SUR-LAUSANNE
(CH)

(72) **Inventeur(s) :**

1-SASSELLI, Marco
20, chemin des Roches
CH-1803 CHARDONNE (CH)
2- NICOLAS, Christophe (CH)
3- HILL, Michael, John (CH)

(74) **Mandataire :** CABINET EKANI
B.P. 5852
YAOUNDE - Cameroun

(54) **Titre :** Méthode d'encryptage multi-modules.

(57) **Abrégé :** Lors de l'utilisation d'un module d'encryptage-décryptage, des méthodes existent pour déterminer la ou les clés utilisées par le module en analysant les données entrantes ou sortantes du module. Pour pallier ce défaut, la méthode multi-modules proposées consiste à ce que le module aval débute ses opérations d'encryptage-décryptage dès qu'une partie des résultats du module amont est disponible.

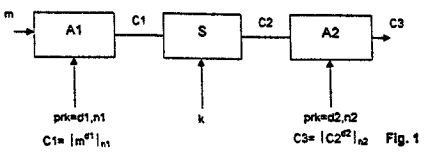

Fig. 1

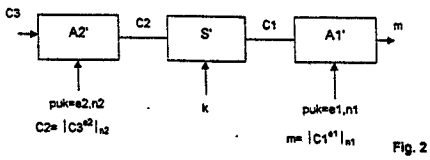

Fig. 2

METHODE D'ENCRYPTAGE MULTI-MODULES

La présente invention concerne le domaine du chiffrement, ou encryptage, et du déchiffrage ou décryptage de données, et particulièrement de données devant rester inaccessibles aux personnes ou appareils non autorisés dans le cadre de systèmes de télévision à péage. Dans de tels systèmes, les données sont chiffrées dans un environnement sécurisé, abritant des puissances de calcul importantes, et appelé sous-système d'encodage, puis envoyées, par des moyens connus en soi, vers au moins un sous-système décentralisé où elles sont déchiffrées, généralement au moyen d'un IRD (Integrated Receiver Decoder) et avec l'aide d'une carte à puce. Cette carte à puce et le sous-système décentralisé qui coopère avec elle sont librement accessibles par une personne éventuellement non autorisée.

Il est connu de chaîner divers moyens d'encryptage-décryptage dans un système de chiffrage-déchiffrage. Dans toute la suite, on appellera encryptage - décryptage un moyen de cryptage particulier utilisé dans un système plus vaste de chiffrage-déchiffrage.

On cherche depuis longtemps à optimiser le fonctionnement de ces systèmes du triple point de vue de la rapidité, de la place occupée en mémoire et de la sécurité. La rapidité s'entend au sens du temps nécessaire pour déchiffrer les données reçues.

Il est connu des systèmes d'encryptage - décryptage à clés symétriques. Leur sécurité inhérente peut être qualifiée en fonction de plusieurs critères.

Le premier critère est celui de la sécurité physique, relative à la facilité ou à la difficulté d'une méthode d'investigation par extraction de certains composants, suivie de leur remplacement éventuel par d'autres composants. Ces composants de remplacement, destinés à renseigner la personne non autorisée sur la nature et le fonctionnement du système de chiffrage-déchiffrage, sont choisis par elle de manière à ne pas être détectés, ou le moins possible, par le reste du système.

Un second critère est celui de la sécurité système, dans le cadre de laquelle les attaques ne sont pas intrusives du point de vue physique mais font appel à de l'analyse de type mathématique. Typiquement, ces attaques seront menées par des

ordinateurs de grande puissance qui tenteront de casser les algorithmes et les codes de chiffrement.

Des moyens d'encryptage - décryptage à clés symétriques sont par exemple les systèmes appelés DES (Data Encryption Standard). Ces moyens, relativement anciens, n'offrent plus qu'une sécurité système et une sécurité physique toute relatives. C'est notamment pour cette raison que de plus en plus, le DES, dont les longueurs de clés sont trop petites pour satisfaire aux conditions de sécurité système, est remplacé par des moyens d'encryptage - décryptage nouveaux ou avec des clés plus longues. De manière générale, ces moyens à clés symétriques font appel à des algorithmes comprenant des rondes de chiffrement.

D'autres stratégies d'attaques sont appelées Simple Power Analysis, et Timing Analysis. Dans le Simple Power Analysis, on utilise le fait qu'un microprocesseur chargé d'encrypter ou de décrypter des données est connecté à une source de tension (en général 5 Volts). Lorsqu'il est au repos, il est parcouru par un courant fixe d'intensité i. Quand il est actif, l'intensité instantanée i est fonction, non seulement des données entrantes, mais aussi de l'algorithme d'encryptage. Le Simple Power Analysis consiste à mesurer le courant i en fonction du temps. On peut de ce fait déduire le type d'algorithme que le microprocesseur effectue.

De la même manière, la méthode du Timing Analysis consiste à mesurer la durée de calcul en fonction d'un échantillon présenté au module de décryptage. Ainsi, la relation entre l'échantillon présenté et le temps de calcul du résultat permet de retrouver les paramètres secrets de module de décryptage tel que la clé. Un tel système est décrit par exemple dans le document "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" publié par Paul Kocher, Cryptography Research, 870 Market St, Suite 1088, San Francisco, CA-USA.

Pour améliorer la sécurité du système de chiffrement, il a été proposé des algorithmes à clé asymétriques, tels que les systèmes dits RSA (Rivest, Shamir et Adleman). Ces systèmes comprennent la génération d'une paire de clés appariées, l'une dite publique servant au chiffrement, et l'autre dite privée servant au déchiffrement. Ces algorithmes présentent un haut niveau de sécurité tant système

que physique. Ils sont par contre plus lents que les systèmes traditionnels, surtout au stade du chiffrement.

Les techniques d'attaque les plus récentes font appel à la notion dite DPA, de l'anglais Differential Power Analysis. Ces méthodes sont basées sur des supputations, vérifiables au bout d'un grand nombre d'essais, sur la présence d'un 0 ou d'un 1 dans une position donnée de la clé de chiffrement. Elles sont quasiment non destructives, ce qui leur confère une bonne indétectabilité, et font appel à la fois à une composante d'intrusion physique et à une composante d'analyse mathématique. Leur fonctionnement rappelle les techniques d'investigation de champs pétrolifères, où une explosion de puissance connue est générée en surface et où des écouteurs et sondes, placés à des distances également connues du lieu de l'explosion, permettent d'émettre des suppositions sur la composition stratigraphique du sous-sol sans trop avoir à le creuser, grâce à la réflexion des ondes de choc par les limites de couches sédimentaires dans ce sous-sol. Les attaques DPA sont décrites notamment dans le § 2.1. du document "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", publié le 1er février 1999 par Suresh Chari, Charanjit Jutla, Josyula R. Rao et Pankaj Rohatgi, de l'IBM T.J. Watson Research Center, Yorktown Heights, NY.

L'exigence de devoir résister aux attaques DPA oblige à utiliser des systèmes de brouillage dit "whitening", soit dans les informations à l'entrée, soit en sortie d'un algorithme de chiffrement-déchiffrement. La technique du whitening est décrite dans le § 3.5 du même document précité.

De plus le fait que les puissances de calcul soient limitées dans le sous-système décentralisé d'un système de télévision à péage crée un problème, qui n'a jamais encore été résolu de façon satisfaisante, pour effectuer dans une mesure suffisante le chaînage décrit précédemment.

Le but de la présente invention est de disposer d'une méthode d'encryptage-décrytage qui résiste aux méthodes modernes d'investigation telles que décrites ci-dessus.

Le but visé par la présente invention est atteint par la méthode décrite dans la partie caractérisante de la revendication 1..

La particularité de la méthode réside dans le fait qu'un module intermédiaire ne démarre pas lorsque le résultat du module précédent (ou amont) a terminé mais débute dès qu'une partie déjà des informations sont disponibles. De ce fait, pour un observateur extérieur, il n'est pas possible d'établir les conditions d'entrée ou de sortie de ce module.

Comme le déchiffrage intervient dans le sous-système décentralisé coopérant avec la carte à puce, cette carte à puce n'abritant que des puissances de calcul relativement limitées par rapport au sous-système d'encodage, il est par exemple intéressant d'utiliser une clé asymétrique publique, au fonctionnement relativement rapide, lors des dernières étapes du déchiffrage. Ceci permet d'une part de préserver les caractéristiques d'invulnérabilité du système en sortie de processus, et d'autre part de concentrer la puissance de calcul, liée essentiellement au chiffrage à l'aide de la clé privée, dans le sous-système d'encodage.

Il a été découvert qu'une sécurité supplémentaire est procurée par la possibilité de concaténer, ou d'imbriquer partiellement, deux moyens d'encryptage-décryptage qui se suivent séquentiellement. On entend par cette concaténation ou imbrication partielle, qui est une traduction de l'anglais "interleaving", le procédé consistant à démarrer l'action du deuxième moyen d'encryptage-décryptage sur les données à un moment où le premier moyen d'encryptage-décryptage n'a pas encore terminé son travail sur ces mêmes données. Ceci permet de masquer les données telles qu'elles résulteraient du travail du premier module et avant qu'elles ne soient soumises à l'action du deuxième module.

La chaînage peut démarrer dès que des données calculées en sortie du premier module sont partiellement disponibles pour être traitées par le second module.

L'invention permet de se prémunir contre les attaques précitées en combinant divers moyens d'encryptage-décryptage dans un système de chiffrage-déchiffrage, et en associant éventuellement une concaténation ou imbrication partielle à la séquence dans laquelle se suivent ces moyens.

Dans une forme particulière de réalisation de l'invention, le système de chiffrage-déchiffrage comprend un sous-système d'encodage où trois algorithmes sont utilisés séquentiellement:

a) un algorithme A1 asymétrique à clé privée d1. Cet algorithme A1 effectue une signature sur des données en clair, représentées par un message m, cette opération délivrant un premier cryptogramme c1, au moyen d'opérations mathématiques généralement notées dans la profession par la formule : c1 = m exposant d1, modulo n1. Dans cette formule, n1 fait partie de la clé publique de l'algorithme asymétrique A1, modulo représente l'opérateur mathématique bien connu des congruences dans l'ensemble des entiers relatifs, et d1 est la clé privée de l'algorithme A.

b) un algorithme S symétrique utilisant une clé secrète K. Cet algorithme convertit le cryptogramme c1 en un cryptogramme c2.

c) un algorithme A2 asymétrique à clé privée d2. Cet algorithme A2 convertit le cryptogramme c2 en un cryptogramme c3, au moyen de l'opération mathématique notée, comme précédemment, par : c3 = c2 exposant d2 mod n2, formule dans laquelle n2 fait partie de la clé publique de l'algorithme asymétrique A2, et d2 est la clé privée de l'algorithme A2

Le cryptogramme c3 part du sous-système d'encodage et parvient au sous-système décentralisé par des moyens connus en soi. Dans le cas de systèmes de télévision à péage, il peut s'agir aussi bien de données vidéo que de messages.

Le sous-système décentralisé utilise, dans l'ordre inverse du précédent, trois algorithmes A1', S' et A2'. Ces trois algorithmes font partie de trois moyens de cryptage-décryptage A1-A1', S-S' et A2-A2', répartis entre le sous-système d'encodage et le sous-système décentralisé, et représentant le système de chiffrage-déchiffrage.

d) l'algorithme A2' effectue sur c3 une opération mathématique restituant c2 et notée: c2 = c3 exposant e2 mod n2. Dans cette formule, l'ensemble constitué de e2 et n2 est la clé publique de l'algorithme asymétrique A2-A2'.

e) l'algorithme symétrique S' symétrique utilisant la clé secrète K restitue le cryptogramme c1.

f) l'algorithme A1' asymétrique à clé publique e1, n1 retrouve m en effectuant l'opération mathématique notée: m = c1 exposant e1 mod n1.

La concaténation, dans le sous-système décentralisé, consiste à démarrer l'étape de décodage e) alors que c2 n'a pas encore été totalement restitué par l'étape précédente d), et à démarrer l'étape de décodage f) alors que c1 n'a pas été totalement restitué par l'étape e. L'avantage est de déjouer une attaque qui viserait par exemple d'abord à extraire, dans le sous-système décentralisé, le cryptogramme c1 en fin d'étape e, pour le comparer avec les données en clair m, puis au moyen de c1 et de m d'attaquer l'algorithme A1', puis de remonter la chaîne de codage de proche en proche.

La concaténation n'est pas nécessaire dans le sous-système d'encodage, qui est installé dans un environnement physique sécurisé. Elle est par contre utile dans le sous-système décentralisé. Dans le cas de la télévision à péage, l'IRD est en effet installé chez l'abonné et peut être l'objet des attaques du type prédécrit.

On conçoit qu'une attaque d'une combinaison de trois algorithmes de décryptage A1', S' et A2' concaténés a beaucoup moins de chances de réussir que si les cryptogrammes c1 et c2 sont intégralement reconstitués entre chaque étape d), e) et f). Par ailleurs, le fait que les algorithmes A1' et A2' soient utilisés avec des clés publiques e1, n1 et e2, n2 fait que les moyens de calcul nécessaires dans le sous-système décentralisé sont bien plus réduits que dans le sous-système d'encodage.

A titre d'exemple et pour fixer les idées, les étapes a) et c) c'est-à-dire les étapes d'encryptage avec clés privées, sont 20 fois plus longues que les étapes d) et f) de décryptage avec clés publiques.

Dans une forme particulière de réalisation de l'invention, dérivée de la précédente, les algorithmes A1 et A2 sont identiques de même que leurs contreparties A1' et A2'.

Dans une forme particulière de réalisation de l'invention, également dérivée de la précédente, dans l'étape c) on utilise la clé publique e2, n2 de l'algorithme asymétrique A2 alors que dans l'étape d) on décrypte le cryptogramme c3 avec la clé privée d2 de cet algorithme. Cette forme constitue une alternative possible lorsque les ressources du sous-système décentralisé en puissance de calcul sont loin d'être atteintes.

Bien que les cartes à puces sont utilisées majoritairement pour le décryptage des données, il existe également des cartes à puces ayant les capacités nécessaires pour effectuer des opérations de cryptage. Dans ce cas, les attaques décrites plus haut vont se porter également sur ces cartes de cryptage qui fonctionnent hors d'endroits protégés tels qu'un centre de gestion. C'est pourquoi la méthode selon l'invention s'applique également aux opérations de cryptage en série c'est à dire que le module aval débute son opération de cryptage dès qu'une partie des informations délivrées par le module amont sont disponibles. Ce procédé à l'avantage d'imbriquer les différents modules de cryptage avec comme conséquence que le résultat du module amont n'est pas disponible complètement à un temps donné. De plus, le module en aval ne débute pas ses opérations avec un résultat complet mais sur des parties ce qui rend impraticable d'interpréter le fonctionnement d'un module par rapport à un état d'entrée ou de sortie connu.

La présente invention sera comprise plus en détail grâce aux dessins suivants, pris à titre non limitatifs, dans lesquels:

- la figure 1 représente les opérations de cryptage
- la figure 2 représente les opérations de décryptage
- la figure 3 représente une alternative à la méthode de cryptage

Sur la figure 1, un ensemble de données m est introduit dans la chaîne de cryptage. Un premier élément A1 effectue une opération de cryptage en utilisant la clé dite privée composée de l'exposent d1 et du modulo n1. Le résultat de cette opération est représenté par C1. Selon le mode de fonctionnement de l'invention, dès qu'une partie du résultat C1 est disponible, le module suivant débute son opération. Ce module suivant S effectue son opération de cryptage avec une clé secrète. Le résultat C2 dès que partiellement disponible est transmis au module A2 pour la troisième opération de cryptage utilisant la clé dite privée composée de l'exposant d2 et du modulo n2. Le résultat final, dénommé ici C3 est prêt pour être transmis par des voies connues tels que voie hertzienne ou par câble.

La figure 2 représente le système de décryptage composé des trois modules de décryptage A1', S', A2' similaires à ceux ayant servi à l'encryptage, mais ordonné

inversement. Ainsi, l'on commence d'abord avec le module A2' qui effectue son opération de décryptage sur la base de la clé dite publique composées de l'exposant e2 et du modulo n2. De la même manière que pour l'encryptage, dès qu'une partie du résultat C2 du module A2' est disponible, il est transmis au module S' pour la deuxième opération de décryptage. Pour terminer le décryptage, le module A1' effectue son opération sur la base de la clé dite publique composée de l'exposent e1 et du modulo n1.

Dans une forme particulière de l'invention, les clés des deux modules A1 et A2 sont identiques, c'est-à-dire que côté encryptage, d1=d2 et n1=n2. Par analogie, lors du décryptage, e1=e2 et n1=n2. Dans ce cas, on parle de la clé privée d, n et de la clé publique e, n.

Dans une autre forme de l'invention, telle qu'illustrée aux figures 3 et 4, le module A2 utilise la clé dite publique à la place de la clé dite privée. Au moment de l'encryptage, la clé publique e2, n2 est utilisée par le module A2, (voir figure 3) et lors du décryptage (voir figure 4), le module A2' utilise la clé privée d2, n2 pour opérer. Bien que cette configuration présente une surcharge de travail à l'ensemble de décryptage, l'utilisation d'une clé privée renforce la sécurité offerte par le module A2.

L'exemple illustré aux figures 3 et 4 n'est pas restrictif pour d'autres combinaisons. Par exemple, il est possible de configurer le module A1 pour qu'il effectue l'opération d'encryptage avec la clé publique et le décryptage avec la clé privée.

Il est également possible de remplacer le module d'encryptage-décryptage à clé secrète S par un module de type à clé asymétriques du même type que les module A1 et A2.

REVENDICATIONS

1. Méthode de cryptage et de décryptage utilisant plusieurs modules d'encryptage-décryptage en série, caractérisée en ce que le module d'encryptage-décryptage en aval débute son opération dès qu'une partie du résultat du module d'encryptage-décryptage amont est disponible.

2. Méthode selon la revendication 1, caractérisée en ce que le module de décryptage en aval débute son opération de décryptage dès qu'une partie du résultat du module de décryptage amont est disponible.

3. Méthode selon la revendication 1, caractérisée en ce que le module d'encryptage en aval débute son opération de cryptage dès qu'une partie du résultat du module amont est disponible.

4. Méthode selon les revendications 1 à 3, caractérisée en ce qu'elle met en œuvre trois modules (A1, S, A2) , le module central (S) étant de type à clé symétrique secrète (k).

5. Méthode selon la revendication précédente, caractérisée en ce que le premier module (A1) et le dernier module (A2) pour l'encryptage et le premier module (A2) et le dernier module (A1) pour le décryptage sont du type RSA à clés asymétriques soit avec une clé privée et une clé publique.

6. Méthode selon la revendication précédente, caractérisée en ce que les deux modules (A1, A2) utilisent la clé dite privée (d,n; d1,n1; d2,n2) pour l'encryptage et la clé dite publique (e, n; e1,n1; e2,n2) pour le décryptage.

7. Méthode selon la revendication précédente, caractérisée en ce que les deux modules (A1, A2) utilisent un même jeu de clé privée (d, n) et publique (e, n).

8. Méthode selon la revendication 6, caractérisée en ce que les deux modules (A1, A2) utilisent un jeu différent de clés privée (d1,n1; d2,n2) et publique (e1, n1; e2,n2).

9. Méthode selon la revendication 5, caractérisée en ce que lors de l'encryptage, le dernier module (A2) utilise la clé dite publique (e2,n2) et lors du décryptage, le premier module (A2) utilise la clé dite privée (d2,n2).

10. Méthode selon les revendications 1 à 3, caractérisée en ce qu'elle met en œuvre trois modules (A1, A, A2) d'encryptage-décryptage à clés asymétriques.

Société Dite : Nagracard, S.A.

012153

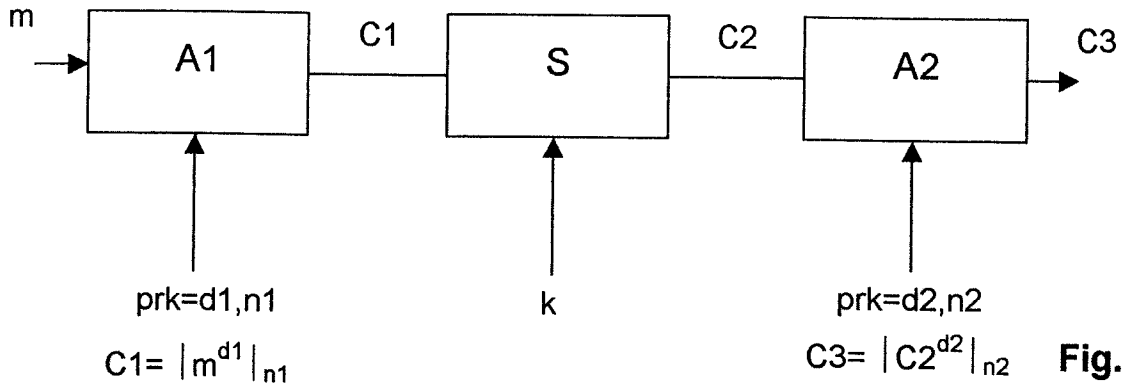

Fig. 1

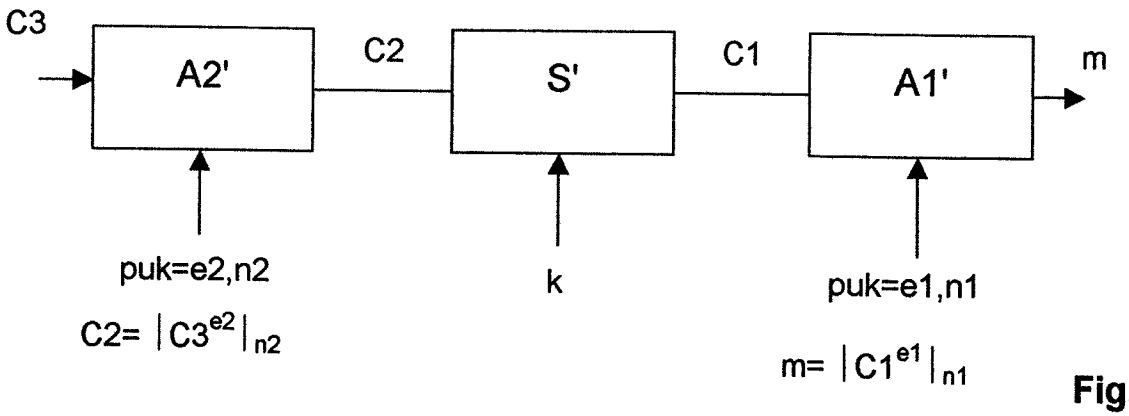

Fig. 2

012153

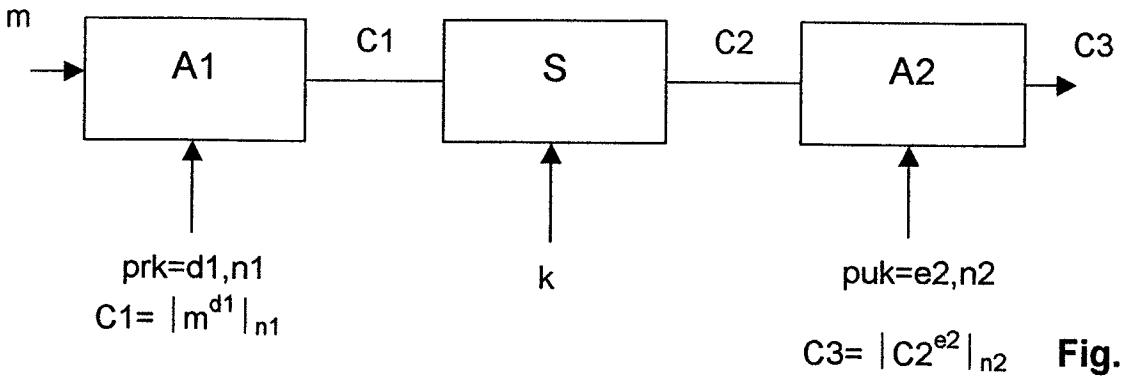

Fig. 3

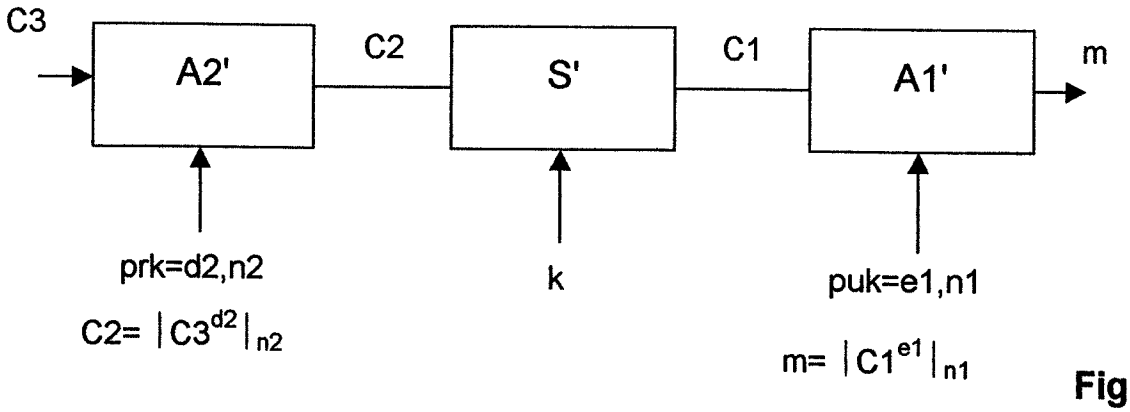

Fig. 4