(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 506 536 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
03.07.2019 Bulletin 2019/27

(51) Int Cl.:
H04K 1/00 *(2006.01)*

(21) Numéro de dépôt: **18215523.4**

(22) Date de dépôt: **21.12.2018**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA ME
Etats de validation désignés:
KH MA MD TN

(30) Priorité: **28.12.2017 FR 1701398**

(71) Demandeur: **Thales**
92400 Courbevoie (FR)

(72) Inventeurs:
- **GARRIDO, Eric**
  92622 GENNEVILLIERS Cedex (FR)
- **PAINCHAULT, Philippe**
  92622 GENNEVILLIERS Cedex (FR)
- **BELAID, Sonia**
  92622 GENNEVILLIERS Cedex (FR)
- **MARTINELLI, Jean**
  92622 GENNEVILLIERS Cedex (FR)
- **DELAVEAU, François**
  92622 GENNEVILLIERS Cedex (FR)
- **KAMENI, Christiane**
  92622 GENNEVILLIERS Cedex (FR)
- **MOLIERE, Renaud**
  92622 GENNEVILLIERS Cedex (FR)

(74) Mandataire: **Dudouit, Isabelle et al**
Marks & Clerk France
Conseils en Propriété Industrielle
Immeuble " Visium "
22, avenue Aristide Briand
94117 Arcueil Cedex (FR)

(54) PROCEDE ET SYSTEME POUR SECURISER LES TRANSMISSIONS DE DONNEES

(57) Procédé pour augmenter la sécurité dans un système de transmission de messages utilisant un protocole de chiffrement des données à transmettre entre un émetteur A et un récepteur B caractérisé en ce qu'il comporte au moins les étapes suivantes :
Lorsque l'émetteur A souhaite transmettre un message x_i au récepteur B, l'émetteur ajoute au message x_i des données de sécurité obtenues par l'application d'une fonction *f* qui prend en entrée les α blocs d'une mémoire R_A^S obtenus lors des α transmissions précédentes ou lors d'une phase d'initialisation pour construire un message de niveau de sécurité plus élevé x_i^*,

Le message x_i^* est transmis à l'étape de codage utilisant un code secret (secrecy coding) et, en parallèle, les blocs du message courant x_i^* sont ajoutés à la mémoire de l'émetteur A,

Le message codé est transmis au récepteur B,
A la réception, B ajoute au message issu de l'étape du codage secret la sortie de la fonction inverse f^{-1}, c'est-à-dire les α données contenues dans une mémoire R_B^R du récepteur B pour obtenir le message décodé, puis le récepteur B ajoute à R_B^R, les données issues de l'étape de codage secret.

EP 3 506 536 A1

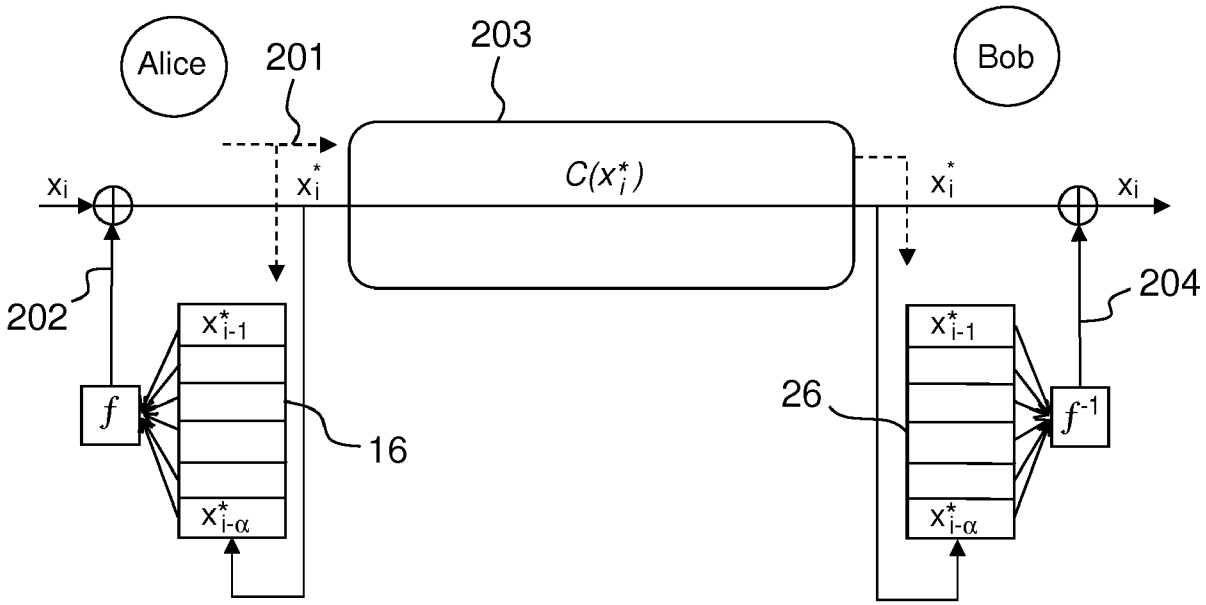

FIG.2

Description

[0001] L'invention concerne un procédé et un système permettant de sécuriser l'échange de données confidentielles au sein d'un système de communication utilisant la technique de codage secret plus connue sous le terme anglo-saxon « secrecy coding ».

[0002] Le « secrecy coding » fait référence à un cadre théorique connu dans l'état de l'art de la théorie de l'information qui analyse la possibilité pour un émetteur Alice de transmettre à un destinataire Bob un message sur un canal de communication de manière confidentielle sans utiliser de clé secrète partagée préalablement. Ce cadre repose uniquement sur les caractéristiques supposées distinctes du canal de propagation et du bruit en réception au niveau de Bob d'une part, et au niveau de l'attaquant potentiel d'autre part (attaquant appelé Eve). L'exemple théorique le plus simple est le modèle du canal à jarretière où Bob reçoit les bits transmis par Alice sans erreur et où Eve ne peut les récupérer qu'avec un taux d'erreur non nul. Ce modèle se généralise à des cas de modèles d'erreurs en réception (au niveau de Bob) et en écoute (au niveau d'Eve) plus complexes. Un autre exemple emprunté à la protection de sécurité physique connue sous l'abréviation anglo-saxonne PHYSEC de système de radio communication par ajout de bruit artificiel est le suivant (très schématiquement) : lorsqu'Alice souhaite envoyer un message m à Bob, elle encode le message et transmet $C(m)$ avec une technique de modulation qui ajoute un bruit artificiel J_m pour tout point de l'espace, excepté la zone où se trouve Bob. Ce bruit est modifié à chaque message m. Bob reçoit après démodulation, l'encodage du message avec un bruit de transmission $C(m) + \eta_B$. Le niveau de bruit η_B permet à Bob de décoder correctement le message m. En revanche, Eve situé en dehors du point de démodulation « facile » occupé par Bob, reçoit l'encodage du message avec un bruit artificiel et un bruit de transmission $C(m) + J_m + \eta_E$. Avec ce niveau de bruit Eve, ne parvient pas à décoder correctement le message.

[0003] De manière générale, dans le cadre de la théorie de l'information, pour un modèle de canal de communication qui fixe les caractéristiques du bruit (au niveau de Bob, et au niveau d'Eve), on montre qu'il est possible de coder effectivement l'information utile avant sa transmission sur le canal de communication de manière à assurer :

- sa confidentialité (l'information d'Eve sur le message reste proche de 0),
- sa transmission sans erreur (Bob décode l'information avec très forte probabilité).

[0004] Pour assurer simultanément ces deux propriétés, la théorie introduit une borne théorique au débit de transmission possible appelée « secrecy capacity ». Cette technique de confidentialité est alors dite inconditionnellement sûre (c'est-à-dire qu'elle ne dépend pas des capacités de calcul de l'attaquant) sous réserve bien entendu que le modèle de canal est correct et que l'on a en conséquence respecté la borne de secrecy capacity associée.

[0005] Ces réserves peuvent limiter en pratique le niveau de sécurité d'un procédé de secrecy coding. Il est toujours difficile de garantir que le modèle théorique du bruit et la borne de secrecy capacity associée sont toujours respectés.

[0006] Une vulnérabilité pratique devant toujours être envisagée est, par exemple que de manière momentanée, le modèle de bruit qui fixe la « secrecy capacity » n'est plus valide. Dans l'exemple précédent on peut par exemple envisager que le même message répété plusieurs fois par Bob peut être plus facilement décodé par Eve. Ou encore, en raison d'une occurrence de bruit artificiel qui s'avère plus faible sur un message, Eve pourra décoder ce message particulier.

[0007] On se place dans le cadre général d'une mise en oeuvre d'un schéma de secrecy coding quelconque qui permet de transmettre successivement des blocs d'information utiles en toute confidentialité sous réserve que le bruit exploité a bien les caractéristiques qui garantissent la sécurité pour chaque bloc transmis.

[0008] Dans l'objectif de mieux garantir la confidentialité des données échangées, même en cas de défaillance momentanée du bruit, l'idée de la présente invention consiste notamment à ajouter :

- côté émission, en amont du bloc de codage du « secrecy coding », une fonction de mélange qui combine le bloc d'information courant traité par le schéma de secrecy coding avec les r blocs utiles transmis précédemment,
- coté réception, en aval de la fonction de décodage du « secrecy coding », la fonction de mélange inverse.

[0009] La fonction de mélange (et son inverse) est sans clé, et peut être parfaitement connue de l'attaquant, en fonctionnement normal du dispositif. Globalement, la solution de confidentialité {fonction de mélange + secrecy coding} ainsi complétée ne nécessite aucun secret partagé au départ par Alice et Bob, comme c'est le cas pour le secrecy coding seul.

[0010] La fonction de mélange qui fait dépendre le bloc courant traité par le secrecy coding, des r blocs utiles précédemment transmis est auto-synchronisante : même si au départ l'état - sous la forme de l'historique des r messages transmis précédemment - n'est pas identique pour l'émetteur et le récepteur, il le devient automatiquement dès que r blocs consécutifs ont été correctement traités et sans erreur en réception par Bob. En particulier, l'émetteur peut choisir l'état initial du mélangeur complètement aléatoirement avant le début de la transmission ou transmettre durant une phase préliminaire r blocs de données complètement aléatoires avant de commencer à diffuser les blocs de données utiles.

[0011] Le paramètre r est sélectionné suivant un compromis qui fixe le niveau de sécurité et le temps de synchronisation :

- r est un paramètre qui augmente le niveau de sécurité du schéma global de protection. En effet, pour que l'attaquant puisse éventuellement obtenir une information sur le bloc courant transmis, il faudrait qu'il dispose de l'état complet de la fonction de mélange, ce qui nécessite de connaître les r blocs utiles transmis précédemment. Pour cela, il faudrait que le bruit utilisé par le secrecy coding s'avère défaillant non seulement sur le message courant mais aussi lors de la transmission des r blocs d'information utiles précédents ;
- r est aussi la taille de la mémoire du processus de mélange. Il fixe le nombre de blocs d'information à transmettre sans erreur pour que l'émetteur et le récepteur soit synchronisés automatiquement. En cas d'erreur en réception sur le bloc courant, cette erreur va perturber l'état interne pendant les r blocs suivants. r doit donc être choisi pas trop grand pour limiter le temps de synchronisation et le taux d'erreur en réception.

[0012] Dans la suite de la description, les notations suivantes seront utilisées :

Le flux de données utiles qu'Alice transmet $x_1, x_2, \ldots$,
Le flux en sortie de la fonction de mélange ou scrambling amont qui sera l'entrée du bloc de « secrecy coding » $x_1^*, x_2^*, \ldots$

L'encodage des blocs x_i^* par la technique de « secrecy coding » transmis sur la ligne est désigné par $C(x_1^*), C(x_2^*), \ldots, C(x_k^*),$

En réception, après le décodage du « secrecy coding », on retombe nominalement, sauf erreur, sur le flux x_i^* qui est ensuite décodé par la couche de « descrambling » pour retrouver le flux d'informations utiles selon un procédé connu de l'homme du métier.

[0013] L'invention concerne un procédé pour augmenter la sécurité dans un système de transmission de messages utilisant un codage secret des données à transmettre entre un émetteur A et un récepteur B caractérisé en ce qu'il comporte au moins les étapes suivantes :

Lorsque l'émetteur A souhaite transmettre un message x_i au récepteur B, l'émetteur ajoute au message x_i des données de sécurité obtenues par l'application d'une fonction f qui prend en entrée les α blocs d'une mémoire R_A^S obtenus lors des α transmissions précédentes ou lors d'une phase d'initialisation pour construire un message de niveau de sécurité plus élevé x_i^*,

Le message x_i^* est transmis à l'étape de codage utilisant un code secret (secrecy coding) et, en parallèle, les blocs du message courant x_i^* sont ajoutés à la mémoire de l'émetteur A,
Le message est transmis au récepteur B,
A la réception, B ajoute au message issu de l'étape du codage secret la sortie de la fonction inverse f^{-1}, c'est-à-dire les α données contenues dans une mémoire R_B^R du récepteur B pour obtenir le message décodé, puis le récepteur B ajoute à R_B^R, les données issues de l'étape de codage secret.

[0014] La fonction utilisée en amont de l'étape de secrecy coding est par exemple une fonction OU exclusif, XOR, considérant bit à bit le message x_i et les blocs issus de la mémoire qui est un registre à décalage :

A l'émission au niveau d'Alice

$$x_i^* \leftarrow x_i \oplus f(x_{i-1}^*, x_{i-2}^*, \ldots, x_{i-\alpha}^*),$$

A la réception au niveau de Bob

$$x_i \leftarrow x_i^* \oplus f^{-1}(x_{i-1}^*, x_{i-2}^*, \ldots, x_{i-\alpha}^*).$$

[0015] Le procédé peut comporter une étape préalable où un identifiant est ajouté au message x_i à transmettre avant de le mélanger avec la fonction f.

[0016] D'autres caractéristiques et avantages de la présente invention apparaîtront mieux à la lecture de la description d'exemples de réalisation annexée des figures qui représentent :

- Figure 1, un schéma global du procédé mis en oeuvre par l'invention, et
- Figure 2, un détail de la fonction utilisée pour assurer une meilleure sécurité et une auto-synchronisation du système.

[0017] Afin de mieux faire comprendre le procédé selon l'invention, l'exemple est donné dans le cas d'un échange entre un premier utilisateur émetteur/récepteur A (Alice) et un deuxième utilisateur émetteur/récepteur

B (Bob), en présence d'un récepteur tiers E (Eve) non autorisé, susceptible d'intercepter les communications et d'accéder au contenu des données échangées entre A et B.

[0018] La figure 1 illustre le principe mis en oeuvre par le procédé selon l'invention. Les données D_i qu'Alice souhaite transmettre à Bob de manière confidentielle sont transformées par une première fonction *f*. Les données transformées D_{if} sont ensuite transmises à une étape de codage secret qui met en oeuvre une technique connue de l'homme du métier. Les données codées D_{ifc} sont ensuite retransformées pour retrouver les données initiales D_i en appliquant une fonction inverse f^{-1} et transmises à Bob.

[0019] L'émetteur/récepteur A est, par exemple, un noeud ou un terminal d'un réseau de communication comportant une unité de calcul 11, un module de codage/décodage 12, un module de démodulation 13, un module composé d'antennes 14, des moyens d'émission et réception radio 15e, 15r, ainsi qu'un dispositif 16 permettant de mémoriser le contenu des messages à transmettre. Le dispositif 16 peut être une pile ou un registre à décalage. L'unité de calcul 11 est configurée pour exécuter une fonction *f* ayant notamment pour objectif d'augmenter la sécurité dans la transmission des données, ou du message.

[0020] De même, l'émetteur/récepteur B, 20, comporte, par exemple, une unité de calcul 21, un module de codage/décodage 22, un module de démodulation 23, un module composé d'antennes 24, des moyens d'émission et réception radio 25e, 25r et un dispositif 26 pour mémoriser, comme lors de l'émission du message, le contenu d'un message reçu par Bob. L'unité de calcul 21 est configurée pour exécuter une fonction f^{-1} inverse de la fonction *f*.

[0021] La figure 2 illustre de manière détaillée les étapes d'une première variante de l'invention ayant notamment pour objectif d'augmenter la sécurité de la transmission de données et d'offrir un procédé auto-synchronisant qui permet en cas d'erreurs dans le message codé reçu par Bob, d'éliminer l'erreur ou les erreurs au fur et à mesure de la lecture par Bob des données. Le procédé dans son fonctionnement normal ne requiert pas de clé de chiffrement.

[0022] Le message transmis peut être composé de blocs de données, de bits, se présenter sous un format connu dans le domaine de la sécurisation de transmission des données.

[0023] Le système met en oeuvre pour chacun des intervenants, Alice et Bob, deux registres ou structure de données qui vont permettre de mémoriser des blocs de messages émis et reçus. Alice possède un registre R_A^S pour mémoriser les messages qu'elle transmet et un registre R_A^R pour les messages qu'elle reçoit. Bob possède un registre R_B^S pour les messages qu'il transmet et un registre R_B^R pour les messages qu'il reçoit. La taille des registres est par exemple choisie en fonction du niveau de sécurité requis par l'application.

[0024] Une première phase concerne l'initialisation : Alice code les données ou les bits à transmettre et envoie α messages non sensibles à Bob (contenant k bits générés de manière aléatoire) pour remplir les registres à décalage R_A^S et R_B^R. Bob code et transmet α messages non sensibles à Alice (composés de même de *k* bits) pour remplir les registres à décalage R_B^S et R_A^R. Tout autre dispositif ayant une fonction identique ou similaire à celle des registres à décalage pourra être utilisé. Cette première phase 201 est représentée en pointillés sur la figure.

[0025] La deuxième phase est la phase de communication. Cette phase peut commencer lorsque les registres R_A^S et R_B^R ont été remplis par des messages émis et reçus lors de la séquence antérieure d'initialisation.

[0026] Lorsqu'Alice souhaite transmettre un message x_i à Bob, elle met en oeuvre les étapes décrites ci-après. Le calculateur d'Alice ajoute, 202, au message x_i qu'elle souhaite transmettre des bits obtenus par l'application d'une fonction *f* qui prend en entrée les α blocs du registre R_A^S, 16, obtenus lors de α transmissions précédentes pour construire un message plus sécurisé x_i^*, la construction du message peut se faire en applicant la fonction OU exclusif, XOR, en considérant le message x_i, bit à bit, et les blocs issus du registre à décalage :

$$x_i^* \leftarrow x_i \oplus f(x_{i-1}^*, x_{i-2}^*, \ldots, x_{i-\alpha}^*),$$

les $x_{i-\alpha}^*$ correspondant aux messages émis lors des transmissions antérieures.

[0027] Le message x_i^* est transmis à l'étape de codage 203 utilisant un code secret (secrecy coding) et, en parallèle, les blocs du message courant x_i^* sont ajoutés au registre à décalage d'Alice.

[0028] Le message est ensuite transmis à Bob.

[0029] Le calculateur de Bob va ajouter, 204, au message issu de l'étape du codage secret (secrecy coding), la sortie de la fonction inverse f^{-1}, c'est-à-dire les α blocs correspondant aux x_{i-1}^*, x_{i-2}^*, ..., $x_{i-\alpha}^*$ messa-

ges decodés lors des α transmissions précédentes de son registre à décalage R_B^R, 26, pour obtenir le message décodé :

$$x_i \leftarrow x_i^* \oplus f^{-1}(x_{i-1}^*, x_{i-2}^*, \ldots, x_{i-\alpha}^*),$$

les $x_{i-\alpha}^*$ correspondant aux messages reçus lors des transmissions antérieures.

Bob ajoute ensuite à son registre à décalage R_B^R, les blocs issus de l'étape de codage secret x_i^*.

[0030] Lorsque Bob souhaite transmettre un message à Alice, le procédé exécute les mêmes étapes, le registre de Bob étant un registre pour l'émission du message, le registre utilisé pour Alice un registre pour la réception.

[0031] Les deux registres à décalage utilisés par Alice, respectivement par Bob, peuvent être les mêmes si les échanges sont divisés également entre l'émission et la réception.

[0032] Cette manière de procéder permet notamment d'augmenter la sécurité dans la transmission de messages entre Alice et Bob, les chances qu'Eve intercepte le message transmis étant quasiment nulles.

[0033] Puisque Alice et Bob échangent régulièrement leurs états internes respectifs, ils savent qu'ils communiquent avec la même personne et non avec un tiers non autorisé. Ainsi, même si le procédé ne fait pas d'authentification propre, puisque Alice et Bob n'utilisent pas de clés secrètes pour reconnaître l'identité de leur interlocuteur, ils ont confiance dans l'émetteur du message.

[0034] D'autre part, le procédé permet en cas d'erreur dans la transmission d'un bit ou d'un bloc de données, d'évacuer l'erreur, au fur et à mesure de la transmission des messages du fait de l'utilisation du registre à décalage qui est remis à jour à chaque transmission de message.

[0035] L'invention présente l'avantage d'augmenter la sécurité dans la transmission des données sans avoir à utiliser de clés secrètes, dans le cadre d'un fonctionnement normal du système. Les coûts d'un tel système sont modestes.

Revendications

1. Procédé pour augmenter la sécurité dans un système de transmission de messages utilisant un codage secret des données à transmettre entre un émetteur A et un récepteur B **caractérisé en ce qu'**il comporte au moins les étapes suivantes :

   Lorsque l'émetteur A souhaite transmettre un message x_i au récepteur B, l'émetteur ajoute au message x_i des données de sécurité obtenues par l'application d'une fonction *f* qui prend en entrée les α blocs d'une mémoire R_A^S obtenus lors des α transmissions précédentes ou lors d'une phase d'initialisation pour construire un message de niveau de sécurité plus élevé x_i^*, (202),

   Le message x_i^* est transmis à l'étape de codage utilisant un code secret (secrecy coding) et, en parallèle, les blocs du message courant x_i^* sont ajoutés à la mémoire de l'émetteur A, (203),

   Le message est ensuite transmis au récepteur B,

   A la réception, B ajoute, (204), au message issu de l'étape du codage secret la sortie de la fonction inverse f^{-1}, c'est-à-dire les α données contenues dans une mémoire R_B^R du récepteur B pour obtenir le message décodé, puis le récepteur B ajoute à R_B^R, les données issues de l'étape de codage secret.

2. Procédé selon la revendication 1 **caractérisé en ce que** la fonction appliquée aux données avant l'étape de secrecy coding est une fonction OU exclusif, XOR, considérant bit à bit le message x_i et les blocs issus de la mémoire qui est un registre à décalage :

   A l'émission au niveau d'Alice

   $$x_i^* \leftarrow x_i \oplus f(x_{i-1}^*, x_{i-2}^*, \ldots, x_{i-\alpha}^*),$$

   A la réception au niveau de Bob

   $$x_i \leftarrow x_i^* \oplus f^{-1}(x_{i-1}^*, x_{i-2}^*, \ldots, x_{i-\alpha}^*).$$

3. Système pour échanger des données confidentielles entre au moins un émetteur A et un récepteur B, en utilisant la technique de codage secret ou secrecy coding **caractérisé en ce que** l'émetteur A comporte un processeur (11) configuré pour appliquer sur les données à transmettre une fonction de sécurité avant leur codage dans le bloc de codage secret et le récepteur est équipé d'un processeur (21) configuré pour appliquer une fonction inverse de la fonction utilisée à l'émission, sur les données issues du bloc de codage secret (203) et retrouver les données initiales transmises par l'émetteur A, en exécutant les étapes du procédé selon l'une des revendications

précédentes.

4. Système selon la revendication 3 **caractérisé en ce que** l'émetteur et le récepteur comportent chacun au moins un registre à décalage (16, 26) pour mémoriser les blocs de données lors de transmissions de données précédentes.

5. Système selon l'une des revendications 3 ou 4 **caractérisé en ce qu'**un émetteur et/ou un récepteur est un noeud ou un terminal dans un réseau de communication.

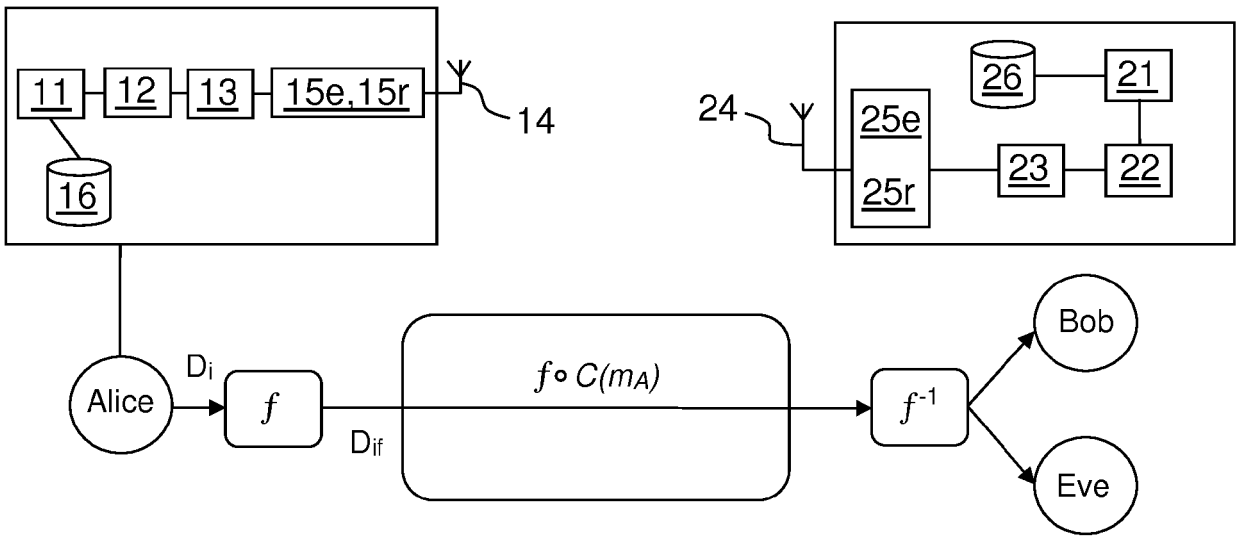
11
12
13
15e,15r
14
16
24
25e
25r
26
21
23
22
Alice
Di
f
Dif
f∘C(mA)
f-1
Bob
Eve

FIG.1

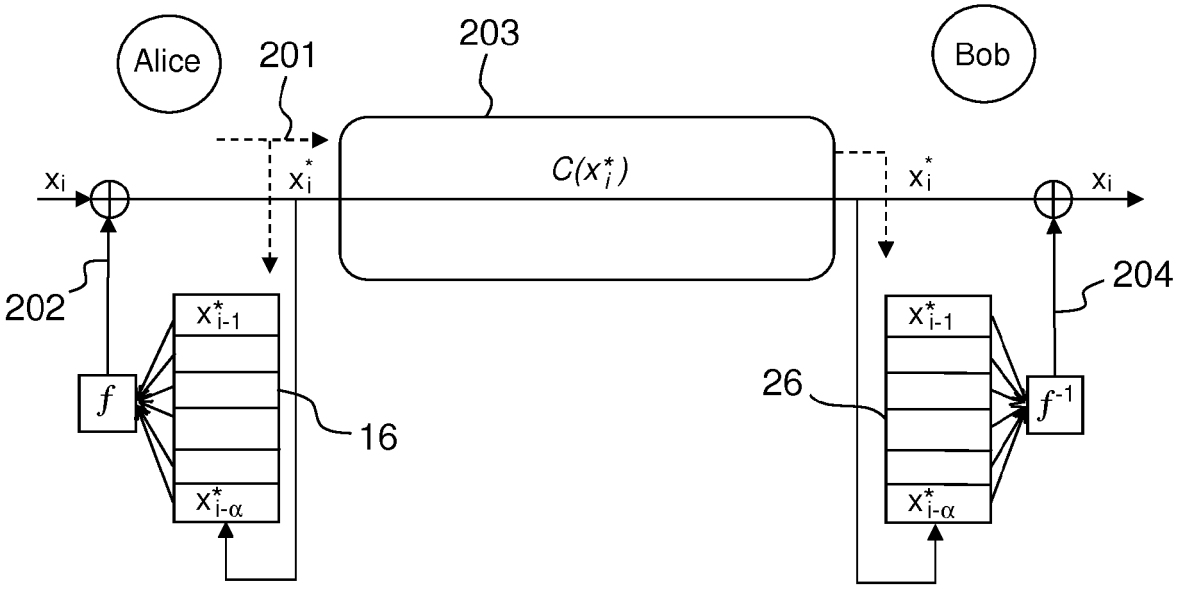
Alice
201
203
Bob
xi
x*i
C(x*i)
x*i
xi
202
204
x*i-1
x*i-α
f
16
26
f-1

FIG.2

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 18 21 5523

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X	BALDI MARCO ET AL: "Practical LDPC coded modulation schemes for the fading broadcast channel with confidential messages", 2014 IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS WORKSHOPS (ICC), IEEE, 10 juin 2014 (2014-06-10), pages 759-764, XP032630885, DOI: 10.1109/ICCW.2014.6881291 * section II; figure 1 *	1-5	INV. H04K1/00
T	MARCO BALDI ET AL: "A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks", IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE, PISCATAWAY, NJ, USA, vol. 2, no. 2, 1 avril 2013 (2013-04-01), pages 183-186, XP011507626, ISSN: 2162-2337, DOI: 10.1109/WCL.2012.122612.120787 * section II; figure 2 *	1-5	DOMAINES TECHNIQUES RECHERCHES (IPC) H04K

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	14 mai 2019	Billet, Olivier

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : doocument de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)