(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
17 mai 2018 (17.05.2018)

WIPO | PCT

(10) Numéro de publication internationale
WO 2018/087255 A1

(51) Classification internationale des brevets :
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2017/078809

(22) Date de dépôt international :
09 novembre 2017 (09.11.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1660864 09 novembre 2016 (09.11.2016) FR

(71) Déposant : **SIGFOX** [FR/FR] ; 425, Rue Jean Rostand, 31670 LABEGE (FR).

(72) Inventeur : **LARIGNON, Guillaume** ; c/o SIGFOX - 425 Rue Jean Rostand, 31670 LABÈGE (FR).

(74) Mandataire : **RIBEIRO DIAS, Alexandre** ; IPSIDE, 6, Impasse Michel Labrousse, 31100 TOULOUSE (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

WO 2018/087255 A1

(54) Title: METHOD AND DEVICE FOR TRANSMITTING ENCRYPTED DATA, METHOD AND DEVICE FOR EXTRACTING DATA

(54) Titre : PROCÉDÉ ET DISPOSITIF D'ÉMISSION DE DONNÉES CHIFFRÉES, PROCÉDÉ ET DISPOSITIF D'EXTRACTION DE DONNÉES

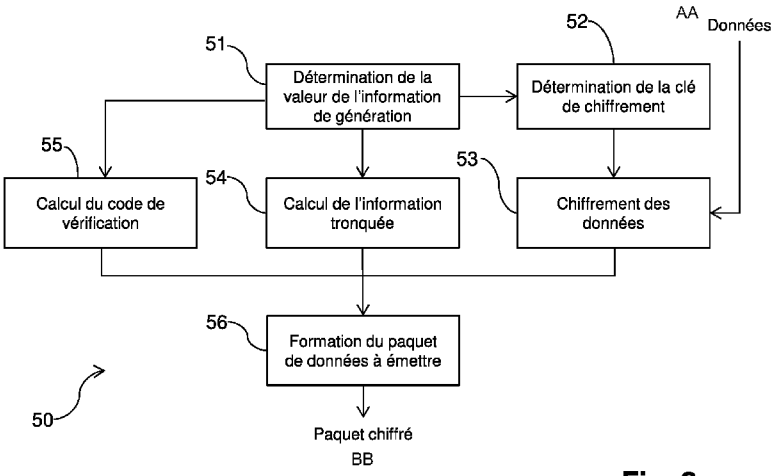

Fig. 2

AA Data
51 Determining the value of the generation information
52 Determining the encryption key
53 Encrypting the data
54 Calculating the truncated information
55 Calculating the verification code
56 Formatting the data packet to be transmitted
BB Encrypted packet

(57) Abstract: The present invention relates to a method (50) for transmitting, by means of a transmitter device (20), a packet to a receiver device (30) of a communication system, said packet including data encrypted according to a symmetric key encryption protocol, including: - determining (51) the value of an item of generation information; - determining (52) an encryption key according to the value of the generation information; - encrypting (53) the data to be included in the encrypted packet to be transmitted according to the encryption key; - calculating (54) a truncated item of information on the basis of the generation information; - calculating (55) a verification code for the encrypted packet according to the encrypted data and the first portion of the generation information; - forming (56) the encrypted packet to be transmitted on the basis of the truncated information, the verification code and the encrypted data.

[Suite sur la page suivante]

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

(57) Abrégé : La présente invention concerne un procédé (50) d'émission, par un dispositif émetteur (20), d'un paquet à destination d'un dispositif récepteur (30) d'un système de communication, ledit paquet comportant des données chiffrées selon un protocole de chiffrement à clé symétrique, comportant : - une détermination (51) de la valeur d'une information de génération, - une détermination (52) d'une clé de chiffrement en fonction de la valeur de l'information de génération, - un chiffrement (53) des données à inclure dans le paquet chiffré à émettre en fonction de la clé de chiffrement, - un calcul (54) d'une information tronquée à partir de l'information de génération, - un calcul (55) d'un code de vérification du paquet chiffré en fonction des données chiffrées et de la première partie de l'information de génération, - une formation (56) du paquet chiffré à émettre à partir de l'information tronquée, du code de vérification et des données chiffrées.

Procédé et dispositif d'émission de données chiffrées, procédé et dispositif d'extraction de données

DOMAINE TECHNIQUE

La présente invention appartient au domaine des télécommunications numériques, et concerne plus particulièrement un procédé d'émission d'un paquet comportant des données chiffrées, ainsi qu'un procédé d'extraction de données incluses dans un tel paquet.

ÉTAT DE LA TECHNIQUE

La présente invention trouve une application particulièrement avantageuse, bien que nullement limitative, dans les systèmes de communication sans fil à bande ultra étroite. Par « bande ultra étroite » (« Ultra Narrow Band » ou UNB dans la littérature anglo-saxonne), on entend que le spectre fréquentiel instantané des signaux radioélectriques émis par des terminaux, à destination d'un réseau d'accès, est de largeur fréquentielle inférieure à deux kilohertz, voire inférieure à un kilohertz.

De tels systèmes de communication sans fil UNB sont particulièrement adaptés pour des applications du type M2M (acronyme anglo-saxon pour « Machine-to-Machine ») ou du type « Internet des objets » (« Internet of Things » ou IoT dans la littérature anglo-saxonne).

Dans un tel système de communication sans fil UNB, les échanges de données se font principalement sur un lien montant depuis des terminaux à destination d'un réseau d'accès dudit système.

Les terminaux émettent des paquets qui sont collectés par des stations de base du réseau d'accès, sans avoir à s'associer préalablement à une ou plusieurs stations de base du réseau d'accès. En d'autres termes, les paquets émis par un terminal ne sont pas destinés à une station de base spécifique du réseau d'accès, et le terminal émet ses paquets en supposant qu'ils pourront être reçus par au moins une station de base.

De telles dispositions sont avantageuses en ce que le terminal n'a pas besoin de réaliser des mesures régulières, gourmandes notamment d'un point de vue consommation électrique, pour déterminer la station de base la plus appropriée pour recevoir ses paquets. La complexité repose sur le réseau

d'accès, qui doit être capable de recevoir des paquets pouvant être émis à des instants arbitraires, et sur des fréquences centrales arbitraires à l'intérieur d'une bande fréquentielle de multiplexage des différents terminaux.

Dans de nombreuses applications, il peut être nécessaire de chiffrer les données incluses dans les paquets, afin d'en assurer la confidentialité sur le lien montant entre les terminaux et le réseau d'accès.

Il existe de nombreux protocoles de chiffrement. Par exemple, dans un protocole de chiffrement à clé symétrique, la même clé est utilisée pour chiffrer et déchiffrer les données. Ladite clé doit par conséquent être connue ou pouvoir être déterminée à la fois par le terminal qui émet les données, et par le réseau d'accès qui reçoit lesdites données.

En outre, pour améliorer la confidentialité des échanges, il est souhaitable de faire varier la clé utilisée au cours du temps, par exemple à chaque nouvelle émission d'un paquet.

Dans un tel cas, il faut prévoir des moyens pour assurer que le terminal et le réseau d'accès utilisent chacun de leur côté la même clé pour respectivement chiffrer et déchiffrer les données.

Par exemple, il est possible de changer la clé à chaque paquet, selon une méthode de génération de clé prédéfinie connue a priori du terminal et du réseau d'accès. Le réseau d'accès, lorsqu'il reçoit un paquet, met à jour la clé en appliquant la même méthode de génération de clé que le terminal.

Un inconvénient d'une telle approche est que, dans un système de communication sans fil UNB, le réseau d'accès ne reçoit pas forcément tous les paquets émis par le terminal, de sorte que le réseau d'accès ne sait pas a priori combien de fois la clé a été modifiée entre le paquet précédent reçu du même terminal et le paquet en cours.

Alternativement, il est possible d'inclure, dans le paquet émis par le terminal, des informations à partir desquelles le réseau d'accès peut déterminer la clé utilisée, selon la méthode de génération de clé prédéfinie. Toutefois, étant donné que le nombre de clés différentes possibles est préférentiellement très élevé pour améliorer la confidentialité des échanges, la quantité d'informations à inclure dans un paquet peut s'avérer importante. Or, dans un système de communication sans fil UNB, la quantité d'informations

pouvant être incluses dans un paquet est très limitée.

EXPOSÉ DE L'INVENTION

La présente invention a pour objectif de remédier à tout ou partie des limitations des solutions de l'art antérieur, notamment celles exposées ci-avant, en proposant une solution qui permette d'assurer une bonne confidentialité des échanges tout en limitant la quantité d'informations à inclure dans les paquets.

A cet effet, et selon un premier aspect, l'invention concerne un procédé d'émission, par un dispositif émetteur, de paquets à destination d'un dispositif récepteur d'un système de communication, comportant, pour l'émission d'un paquet, dit « paquet chiffré », comportant des données chiffrées selon un protocole de chiffrement à clé symétrique :

- une détermination de la valeur d'une information de génération,
- une détermination d'une clé de chiffrement, à utiliser pour chiffrer les données à inclure dans le paquet chiffré à émettre, en fonction de la valeur de l'information de génération,
- un chiffrement des données à inclure dans le paquet chiffré à émettre en fonction de la clé de chiffrement,
- un calcul d'une information tronquée en décomposant l'information de génération en une première partie et une seconde partie, la première partie variant plus lentement, au cours du temps, que la seconde partie, l'information tronquée étant représentative de ladite seconde partie de l'information de génération,
- un calcul d'un code de vérification du paquet chiffré en fonction des données chiffrées et de la première partie de l'information de génération,
- une formation du paquet chiffré à émettre à partir de l'information tronquée, du code de vérification, et des données chiffrées.

Ainsi, selon l'invention, la clé de chiffrement est déterminée en fonction de la valeur d'une information de génération variable au cours du temps. Par conséquent, la clé de chiffrement change à chaque fois que la valeur de l'information de génération change, et peut prendre autant de valeurs différentes que l'information de génération.

Par contre, l'information de génération n'est pas incluse telle quelle

dans le paquet chiffré à émettre, et c'est une information tronquée qui est incluse dans le paquet chiffré émis. Avantageusement, l'information de génération étant décomposée en une première partie et une seconde partie, la première partie variant plus lentement que la seconde partie, l'information tronquée est calculée en fonction de la seconde partie, sans tenir compte de la première partie. Typiquement, la première partie de l'information de génération correspond à une partie qui ne varie pas ou peu sur la durée d'émission de plusieurs paquets consécutifs, tandis que la seconde partie est susceptible de varier d'un paquet à un autre.

Par conséquent, le nombre de valeurs différentes que peut prendre la clé de chiffrement peut être choisi en fonction du niveau de confidentialité souhaité, et ce sans impacter la quantité d'informations à émettre dans le paquet chiffré pour permettre au dispositif récepteur de déterminer la clé de chiffrement. En effet, la quantité d'informations à émettre peut être limitée à la quantité d'informations nécessaires pour encoder l'information tronquée.

Par contre, le dispositif récepteur doit, lors de la réception d'un paquet chiffré émis par le dispositif émetteur, estimer la valeur de la première partie de l'information de génération dudit paquet chiffré (non incluse dans ledit paquet chiffré) afin d'en déduire, à partir de l'information tronquée, la valeur de l'information de génération et ainsi pouvoir déterminer la clé de chiffrement utilisée par le dispositif émetteur. Le code de vérification, qui est calculé par le dispositif émetteur en fonction des données chiffrées et de la première partie de l'information de génération, est alors utilisé par le dispositif récepteur pour déterminer si la valeur estimée de la première partie de l'information de génération est correcte, c'est-à-dire si elle correspond bien à la première partie de l'information de génération utilisée par le dispositif émetteur, en évaluant l'intégrité du paquet chiffré en fonction des données chiffrées et de la valeur estimée de la première partie de l'information de génération. Si le paquet chiffré est considéré comme intègre, alors cela signifie en outre que la valeur estimée de la première partie de l'information de génération correspond bien à la première partie de l'information de génération utilisée par le dispositif émetteur.

Dans des modes particuliers de mise en œuvre, le procédé d'émission

peut comporter en outre l'une ou plusieurs des caractéristiques suivantes, prises isolément ou selon toutes les combinaisons techniquement possibles.

Dans des modes particuliers de mise en œuvre, le code de vérification est calculé en fonction en outre d'une clé d'authentification du dispositif émetteur, de sorte que le code de vérification permette également de vérifier l'authenticité du paquet chiffré.

Dans des modes particuliers de mise en œuvre, le procédé d'émission comporte également une formation et une émission d'un paquet, dit « paquet de recalage », incluant une information de recalage représentative de la première partie de l'information de génération. Ce paquet de recalage peut être émis de manière récurrente, par exemple de manière périodique, ou bien à chaque fois que la première partie de l'information de génération varie, ou encore à chaque fois que le dispositif émetteur émet un nombre prédéterminé de paquets chiffrés. Lors de la réception, par le dispositif récepteur, d'un paquet chiffré émis par le dispositif émetteur, l'estimation d'une valeur candidate de la première partie de l'information de génération dudit paquet chiffré est effectuée en fonction en outre de l'information de recalage extraite d'un paquet de recalage précédemment reçu.

Dans des modes particuliers de mise en œuvre, l'information de génération est un compteur de paquets correspondant au nombre de paquets émis par le dispositif émetteur ou une date de génération du paquet à émettre.

Selon un second aspect, la présente invention concerne un dispositif émetteur pour émettre des paquets à destination d'un dispositif récepteur d'un système de communication, comportant, pour l'émission d'un paquet, dit « paquet chiffré », comportant des données chiffrées selon un protocole de chiffrement à clé symétrique:

- des moyens configurés pour déterminer la valeur d'une information de génération,
- des moyens configurés pour déterminer une clé de chiffrement, à utiliser pour chiffrer les données à inclure dans le paquet chiffré à émettre, en fonction de la valeur de l'information de génération,
- des moyens configurés pour chiffrer des données à inclure dans le paquet chiffré à émettre en fonction de la clé de chiffrement,

- des moyens configurés pour calculer une information tronquée en décomposant l'information de génération en une première partie et une seconde partie, la première partie variant plus lentement, au cours du temps, que la seconde partie, l'information tronquée étant représentative de ladite seconde partie,
- des moyens configurés pour calculer un code de vérification du paquet chiffré en fonction des données chiffrées et de la première partie de l'information de génération,
- des moyens configurés pour former le paquet chiffré à émettre à partir de l'information tronquée, du code de vérification, et des données chiffrées.

Dans des modes particuliers de réalisation, le dispositif émetteur peut comporter en outre l'une ou plusieurs des caractéristiques suivantes, prises isolément ou selon toutes les combinaisons techniquement possibles.

Dans des modes particuliers de réalisation, le code de vérification est calculé en fonction en outre d'une clé d'authentification du dispositif émetteur, de sorte que le code de vérification permette de vérifier en outre l'authenticité du paquet chiffré.

Dans des modes particuliers de réalisation, le dispositif émetteur comporte en outre des moyens configurés pour former et émettre un paquet, dit « paquet de recalage », incluant une information de recalage représentative de la première partie de l'information de génération.

Dans des modes particuliers de réalisation, l'information de génération est un compteur de paquets correspondant au nombre de paquets émis par ledit dispositif émetteur ou une date de génération du paquet à émettre.

Selon un troisième aspect, la présente invention concerne un procédé d'extraction, par un dispositif récepteur, de données incluses dans un paquet chiffré, dit « paquet chiffré en cours », émis par un dispositif émetteur d'un système de communication conformément à un procédé d'émission selon l'un quelconque des modes de mise en œuvre de l'invention. Ledit procédé d'extraction comporte :

- une extraction, à partir du paquet chiffré en cours, de l'information tronquée, du code de vérification, et des données chiffrées,

- une estimation d'une valeur candidate pour la première partie de l'information de génération du dispositif émetteur pour le paquet chiffré en cours en fonction de l'information tronquée extraite dudit paquet chiffré en cours,
- une détermination si la valeur candidate estimée est correcte par une évaluation de l'intégrité du paquet chiffré en cours en fonction de la valeur candidate estimée, des données chiffrées, et du code de vérification extraits dudit paquet chiffré en cours,
- lorsque la valeur candidate estimée est considérée comme correcte :
    - une détermination d'une clé de déchiffrement en fonction de la valeur candidate estimée et en fonction de l'information tronquée extraite,
    - un déchiffrement des données chiffrées extraites en fonction de la clé de déchiffrement.

Dans des modes particuliers de mise en œuvre, le procédé d'extraction peut comporter en outre l'une ou plusieurs des caractéristiques suivantes, prises isolément ou selon toutes les combinaisons techniquement possibles.

Dans des modes particuliers de mise en œuvre, l'intégrité du paquet chiffré en cours est évaluée en fonction en outre d'une clé d'authentification du dispositif émetteur.

Dans des modes particuliers de mise en œuvre, le procédé d'extraction comporte en outre une extraction d'une information de recalage incluse dans un paquet émis par le dispositif émetteur, dit « paquet de recalage ». L'estimation de la valeur candidate de la première partie de l'information de génération pour le paquet chiffré en cours est alors effectuée en outre en fonction de cette information de recalage.

Dans des modes particuliers de mise en œuvre, plusieurs valeurs candidates pour la première partie de l'information de génération sont estimées, et l'intégrité du paquet chiffré en cours est évaluée pour chaque valeur candidate estimée jusqu'à ce qu'un critère d'arrêt soit vérifié.

Dans des modes particuliers de mise en œuvre, l'information de

génération correspond à un compteur de paquets du dispositif émetteur dont la valeur de la première partie pour le paquet chiffré en cours est estimée en fonction en outre de la valeur de la première partie estimée et vérifiée pour un paquet précédent reçu du même dispositif émetteur.

Dans des modes particuliers de mise en œuvre, l'information de génération correspond à une date de génération du paquet émis par le dispositif émetteur dont la valeur de la première partie est estimée en fonction en outre de la première partie de la date de réception dudit paquet chiffré en cours par le dispositif récepteur.

Selon un quatrième aspect, la présente invention concerne un dispositif récepteur pour recevoir des paquets d'un dispositif émetteur d'un système de communication selon l'un quelconque des modes de réalisation de l'invention. Pour extraire les données incluses dans un paquet chiffré en cours, ledit dispositif récepteur comporte :

- des moyens configurés pour extraire, à partir du paquet chiffré en cours, l'information tronquée, le code de vérification, et les données chiffrées,
- des moyens configurés pour estimer une valeur candidate de la première partie d'une information de génération du dispositif émetteur pour le paquet chiffré en cours en fonction de l'information tronquée extraite dudit paquet chiffré en cours,
- des moyens configurés pour déterminer si la valeur candidate estimée est correcte en évaluant l'intégrité du paquet chiffré en cours en fonction de la valeur candidate estimée, des données chiffrées, et du code de vérification extraits dudit paquet chiffré en cours,
- des moyens configurés pour déterminer une clé de déchiffrement en fonction de la valeur de l'information de génération du dispositif émetteur estimée pour le paquet chiffré en cours,
- des moyens configurés pour déchiffrer les données chiffrées extraites du paquet chiffré en cours en fonction de la clé de déchiffrement.

Dans des modes particuliers de réalisation, le dispositif récepteur peut

comporter en outre l'une ou plusieurs des caractéristiques suivantes, prises isolément ou selon toutes les combinaisons techniquement possibles.

Dans des modes particuliers de réalisation, l'intégrité du paquet chiffré en cours est évaluée en fonction en outre d'une clé d'authentification du dispositif émetteur.

Dans des modes particuliers de réalisation, le dispositif récepteur comporte en outre des moyens configurés pour extraire l'information de recalage à partir d'un paquet de recalage émis par le dispositif émetteur. La valeur candidate de la première partie de l'information de génération pour le paquet chiffré en cours est alors estimée en outre en fonction de cette information de recalage.

Dans des modes particuliers de réalisation, plusieurs valeurs candidates pour la première partie de l'information de génération sont estimées, et l'intégrité du paquet chiffré en cours est évaluée pour chaque valeur candidate estimée jusqu'à ce qu'un critère d'arrêt soit vérifié.

Dans des modes particuliers de réalisation, l'information de génération correspond à un compteur de paquets dudit dispositif émetteur dont la valeur de la première partie pour le paquet chiffré en cours est estimée en fonction en outre de la valeur de la première partie estimée et vérifiée pour un paquet précédent reçu du même dispositif émetteur.

Dans des modes particuliers de réalisation, l'information de génération correspond à une date de génération du paquet émis par le dispositif émetteur dont la valeur de la première partie est estimée en fonction en outre de la première partie de la date de réception dudit paquet chiffré en cours par le dispositif récepteur.

Selon un cinquième aspect, la présente invention concerne un système de communication comportant au moins un dispositif émetteur selon l'un quelconque des modes de réalisation de l'invention, et au moins un dispositif récepteur selon l'un quelconque des modes de réalisation de l'invention.

PRÉSENTATION DES FIGURES

L'invention sera mieux comprise à la lecture de la description suivante, donnée à titre d'exemple nullement limitatif, et faite en se référant aux figures

qui représentent :

- Figure 1 : une représentation schématique d'un système de communication sans fil,
- Figure 2 : un diagramme illustrant les principales étapes d'un procédé d'émission d'un paquet comportant des données chiffrées,
- Figure 3 : un diagramme illustrant les principales étapes d'un mode préféré de mise en œuvre du procédé d'émission de la figure 2, avec émission d'un paquet de recalage,
- Figure 4 : un diagramme illustrant les principales étapes d'un procédé d'extraction de données incluses dans un paquet chiffré,
- Figure 5 : un diagramme illustrant les principales étapes d'un mode préféré de mise en œuvre du procédé d'extraction de la figure 4, et mettant en évidence l'utilisation d'un paquet de recalage,
- Figure 6 : un diagramme illustrant les principales étapes d'évaluation d'intégrité d'un paquet chiffré,
- Figure 7 : un diagramme illustrant les principales étapes d'un mode préféré de mise en œuvre du procédé d'extraction de la figure 5, et mettant en évidence l'estimation de plusieurs valeurs candidates.

Dans ces figures, des références identiques d'une figure à une autre désignent des éléments identiques ou analogues. Pour des raisons de clarté, les éléments représentés ne sont pas à l'échelle, sauf mention contraire.

DESCRIPTION DÉTAILLÉE DE MODES DE RÉALISATION

La figure 1 représente schématiquement un système 10 de communication sans fil, par exemple de type UNB, comportant plusieurs terminaux 20 et un réseau d'accès 30. Dans l'exemple illustré par la figure 1, le réseau d'accès 30 comporte plusieurs stations de base 31 et un serveur 32.

Les terminaux 20 et les stations de base 31 du réseau d'accès 30 échangent des données sous la forme de signaux radioélectriques. Par « signal radioélectrique », on entend une onde électromagnétique se propageant via des moyens non filaires, dont les fréquences sont comprises dans le spectre traditionnel des ondes radioélectriques (quelques hertz à plusieurs centaines de gigahertz).

Notamment, les terminaux 20 sont adaptés à émettre des paquets sur

un lien montant à destination du réseau d'accès 30.

Les paquets sont par exemple émis de façon asynchrone. Par « émettre de façon asynchrone », on entend que les terminaux 20 déterminent de manière autonome quand ils émettent et/ou sur quelle fréquence centrale ils émettent, sans coordination desdits terminaux 20 entre eux et avec les stations de base 31 du réseau d'accès 30.

Dans la suite de la description, on se place de manière non limitative dans le cas où les terminaux 20 sont au moins asynchrones en temps, de sorte que les paquets sont émis à des instants non connus a priori du réseau d'accès 30. Rien n'exclut cependant, suivant d'autres exemples, de considérer des terminaux 20 synchronisés temporellement avec les stations de base 31.

Chaque station de base 31 est adaptée à recevoir les paquets des terminaux 20 qui se trouvent à sa portée. Chaque paquet ainsi reçu est par exemple transmis au serveur 32 du réseau d'accès 30, éventuellement accompagné d'autres informations comme un identifiant de la station de base 31 qui l'a reçu, la puissance mesurée dudit paquet reçu, la date de réception mesurée dudit paquet, la fréquence centrale mesurée dudit paquet reçu, etc. Le serveur 32 traite par exemple l'ensemble des paquets reçus des différentes stations de base 31.

A) Procédé d'émission de paquets

La figure 2 représente schématiquement les principales étapes d'un procédé 50 d'émission, par un terminal 20 et à destination du réseau d'accès 30, de paquets comportant des données chiffrées selon un protocole de chiffrement à clé symétrique.

Par exemple, le terminal 20 comporte un circuit de traitement (non représenté sur les figures), comportant un ou plusieurs processeurs et des moyens de mémorisation (disque dur magnétique, mémoire électronique, disque optique, etc.) dans lesquels est mémorisé un produit programme d'ordinateur, sous la forme d'un ensemble d'instructions de code de programme à exécuter pour mettre en œuvre les différentes étapes du procédé 50 d'émission de paquets. Alternativement ou en complément, le circuit de traitement comporte un ou des circuits logiques programmables (FPGA, PLD, etc.), et/ou un ou des circuits intégrés spécialisés (ASIC), et/ou un ensemble

de composants électroniques discrets, etc., adaptés à mettre en œuvre tout ou partie desdites étapes du procédé 50 d'émission de paquets.

En d'autres termes, le circuit de traitement comporte un ensemble de moyens configurés de façon logicielle (produit programme d'ordinateur spécifique) et/ou matérielle (FPGA, PLD, ASIC, composants électroniques discrets, etc.) pour mettre en œuvre les étapes du procédé 50 d'émission de paquets à destination du réseau d'accès 30.

Le terminal 20 comporte également des moyens de communication sans fil, considérés comme connus de l'homme de l'art, permettant au terminal 20 d'émettre des paquets, à destination des stations de base 31 du réseau d'accès 30, sous la forme de signaux radioélectriques.

Tel qu'illustré par la figure 2, le procédé 50 d'émission de paquets chiffrés comporte les étapes suivantes, toutes exécutées par le terminal 20, qui seront décrites en détail ci-après :

- 51 détermination de la valeur d'une information de génération,
- 52 détermination d'une clé de chiffrement en fonction de la valeur de l'information de génération,
- 53 chiffrement des données à inclure dans le paquet chiffré à émettre en fonction de la clé de chiffrement,
- 54 calcul d'une information tronquée à partir de l'information de génération,
- 55 calcul d'un code de vérification du paquet chiffré en fonction des données chiffrées et de la première partie de l'information de génération,
- 56 formation du paquet chiffré à émettre à partir de l'information tronquée, du code de vérification, et des données chiffrées.

Ainsi, la clé de chiffrement est déterminée en fonction de la valeur d'une information de génération qui est variable au cours du temps. Par conséquent, la clé de chiffrement change à chaque fois que la valeur de l'information de génération change. Par contre, l'information de génération n'est pas incluse telle quelle dans le paquet chiffré à émettre, et c'est une information tronquée qui est incluse dans le paquet chiffré émis.

L'information de génération peut être toute information variable au

cours du temps qui peut être décomposée en une première partie et une seconde partie, la première partie variant plus lentement que la seconde partie. Par conséquent, la première partie, qui ne varie pas ou peu sur la durée d'émission de plusieurs paquets consécutifs, n'a pas à être incluse dans le paquet chiffré à émettre. Par contre, la seconde partie, qui varie d'un paquet à un autre, est incluse dans le paquet chiffré à émettre sous toute forme adaptée, et l'information tronquée est calculée à partir de ladite seconde partie uniquement, c'est-à-dire sans tenir compte de la première partie.

Par exemple, l'information de génération est la date de génération du paquet chiffré à émettre. La date de génération est par exemple exprimée sous la forme année-mois-jour-heure-minute-seconde, et est donc décomposable en une première partie qui varie lentement, telle que la partie correspondant à année-mois-jour, tandis que la seconde partie, qui varie plus rapidement, est la partie correspondant à heure-minute-seconde. L'information tronquée est donc, dans cet exemple, représentative de la partie correspondant à heure-minute-seconde, et est par exemple calculée à partir de la partie heure-minute-seconde au moyen d'une fonction de calcul inversible et connue a priori du terminal 20 et du réseau d'accès 30.

Dans la suite de la description, on se place de manière non limitative dans le cas où l'information de génération est un compteur de paquets correspondant au nombre de paquets émis par le terminal 20. L'information tronquée est désignée ci-après par « compteur tronqué ».

A.1) Détermination de la valeur du compteur de paquets

Au cours de l'étape 51 de détermination, le terminal 20 met à jour la valeur d'un compteur de paquets, qui correspond au nombre de paquets émis par ledit terminal 20.

De préférence, la valeur dudit compteur de paquets est incrémentée à chaque nouvelle émission de paquet. Rien n'exclut cependant, suivant d'autres exemples, de n'incrémenter ladite valeur du compteur de paquets que pour certains paquets. Par exemple, il est possible, afin d'augmenter la probabilité de réception, par le réseau d'accès 30, des données incluses dans un paquet, de dupliquer Nr fois lesdites données afin de les inclure dans Nr paquets émis successivement, par exemple sur des fréquences centrales différentes,

comportant tous les mêmes données. Dans un tel cas, par exemple, il est possible de n'incrémenter la valeur dudit compteur de paquets que tous les Nr paquets, c'est-à-dire uniquement lorsque de nouvelles données doivent être émises par le terminal 20.

Dans la suite de la description, on se place de manière non limitative dans le cas où la valeur du compteur de paquets est incrémentée à chaque nouvelle émission d'un paquet.

La valeur du compteur de paquets est par exemple incrémentée modulo Nc, Nc étant un nombre entier positif prédéterminé. Ainsi, le compteur de paquets du terminal 20 peut prendre Nc valeurs différentes. Par exemple, le nombre Nc est égal à 2^{Nb1}, Nb1 étant un nombre entier positif prédéterminé, de sorte que la valeur du compteur de paquets peut être encodée au moyen de Nb1 bits. Par exemple, Nb1 est égal à 128, de sorte que le compteur de paquets du terminal 20 peut prendre plus de 10^{38} valeurs différentes.

A.2) Détermination de la clé de chiffrement

Au cours de l'étape 52 de détermination, la clé de chiffrement, à utiliser pour chiffrer les données à inclure dans le paquet chiffré à émettre, est déterminée en fonction de la valeur du compteur de paquets.

Ainsi, la clé de chiffrement à utiliser est modifiée à chaque fois que la valeur du compteur de paquets est incrémentée. En outre, comme le compteur de paquets peut prendre Nc valeurs différentes, il en résulte que la clé de chiffrement peut également prendre Nc valeurs différentes.

Par conséquent, le nombre Nc est avantageusement prédéterminé de sorte à assurer notamment un bon niveau de confidentialité des échanges. Par exemple, en considérant le nombre Nc égal à 2^{Nb1} et Nb1 égal à 128, alors la clé de chiffrement peut prendre plus de 10^{38} valeurs différentes, ce qui permet d'assurer un bon niveau de confidentialité.

La clé de chiffrement est déterminée, à partir de la valeur du compteur de paquets, selon une méthode de génération de clé prédéfinie, connue a priori du terminal 20 et du réseau d'accès 30. L'invention peut mettre en œuvre tout type de méthode de génération de clé adaptée connue de l'homme de l'art, et le choix d'une méthode de génération de clé particulière ne constitue qu'une variante de mise en œuvre de l'invention. En outre, la clé de chiffrement peut

également être déterminée à partir d'informations additionnelles qui, le cas échéant, sont par exemple concaténées avec le compteur de paquets pour obtenir un mot de génération de taille supérieure à celle du seul compteur de paquets. Par exemple, il peut être envisagé de concaténer avec le compteur de paquets une séquence statique générée de manière pseudo-aléatoire, unique pour un terminal 20 donné, et connue a priori par le réseau d'accès 30.

A.3) Chiffrement des données

Au cours de l'étape 53 de chiffrement, les données à inclure dans le paquet chiffré à émettre sont chiffrées en fonction de la clé de chiffrement, selon le protocole de chiffrement à clé symétrique considéré.

De manière générale, l'invention est applicable à tout type de protocole de chiffrement à clé symétrique connu de l'homme de l'art, et le choix d'un protocole de chiffrement à clé symétrique particulier ne constitue qu'une variante d'implémentation de l'invention.

Dans des modes préférés de mise en œuvre, le protocole de chiffrement à clé symétrique utilisé est un protocole de chiffrement de flux (aussi connu sous le terme de chiffrement par flot, « stream cipher » dans la littérature anglo-saxonne) éventuellement émulé à partir d'un protocole de chiffrement par bloc comme l'AES (« Advanced Encryption Standard »).

En effet, contrairement aux protocoles de chiffrement par bloc, un protocole de chiffrement de flux permet de chiffrer des données quelle que soit leur taille par rapport à la taille de la clé de chiffrement. Par conséquent, il est possible de choisir des clés de chiffrement longues, pouvant ainsi prendre un nombre très élevé de valeurs différentes, sans avoir à augmenter d'autant la quantité des données à inclure dans un paquet.

Dans la suite de la description, on se place de manière non limitative dans le cas d'un protocole de chiffrement de flux. De manière conventionnelle, les données se présentent par exemple sous forme de bits, de même que la clé de chiffrement qui comporte au moins Nb1 bits. Les données chiffrées sont par exemple obtenues en combinant un à un les bits successifs des données et de la clé de chiffrement, par exemple au moyen d'une fonction logique de type « OU EXCLUSIF » (« XOR » dans la littérature anglo-saxonne).

A.4) Calcul du compteur tronqué

Au cours de l'étape 54 de calcul, un compteur tronqué est déterminé à partir de la valeur du compteur de paquets du terminal 20.

A cet effet, tel qu'indiqué précédemment, le compteur de paquets est décomposé en un première partie et une seconde partie.

Par exemple, la seconde partie du compteur de paquets correspond à la valeur dudit compteur de paquets modulo Nt, Nt étant un nombre entier positif prédéterminé inférieur à Nc. En d'autres termes, la seconde partie correspond au reste de la division euclidienne de la valeur du compteur de paquets par Nt, tandis que la première partie correspond au quotient de ladite division euclidienne de la valeur du compteur de paquets par Nt.

Par exemple, le nombre Nt est égal à 2^{Nb2}, Nb2 étant un nombre entier positif prédéterminé inférieur à Nb1, de sorte que la seconde partie correspond alors aux Nb2 bits de poids faible (« Least Significant Bits » ou LSB dans la littérature anglo-saxonne) parmi les Nb1 bits du compteur de paquets. Par exemple, Nb2 est égal à 12, de sorte que la seconde partie correspond à la valeur du compteur de paquets modulo 4096. Le nombre Nt peut par exemple être choisi de telle sorte que la probabilité, pour le réseau d'accès 30, de manquer Nt paquets consécutifs émis par le même terminal 20 est inférieure à une valeur seuil prédéfinie, par exemple inférieure à 10^{-6}.

Le compteur tronqué est représentatif de la seconde partie du compteur de paquets, et est par exemple calculé à partir de ladite seconde partie selon une fonction de calcul inversible connue a priori du terminal 20 et du réseau d'accès 30. Dans la suite de la description, on se place de manière non limitative dans le cas où le compteur tronqué est choisi égal à la seconde partie, de sorte que ledit compteur tronqué correspond à la valeur du compteur de paquets modulo Nt.

A.5) Calcul du code de vérification

Au cours de l'étape 55 de calcul, un code de vérification est déterminé à partir des données chiffrées et de la première partie du compteur de paquets.

En effet, le réseau d'accès 30 doit, lors de la réception d'un paquet chiffré émis par le terminal 20, estimer la valeur de la première partie du compteur de paquets pour ledit paquet chiffré afin d'en déduire, à partir du compteur tronqué, la valeur de l'information de génération, et ainsi pouvoir

déterminer la clé de déchiffrement pour pouvoir déchiffrer les données chiffrées contenues dans ledit paquet chiffré.

Le code de vérification, qui est calculé par le terminal 20 en fonction des données chiffrées et de la première partie du compteur de paquets, est alors utilisé par le réseau d'accès 30 pour évaluer l'intégrité du paquet chiffré. Si le paquet chiffré est considéré comme intègre, alors cela signifie que les données chiffrées extraites du paquet chiffré et la valeur estimée de la première partie du compteur de paquets sont correctes. Dans le cas contraire, cela signifie que les données chiffrées extraites du paquet chiffré et/ou la valeur estimée de la première partie du compteur de paquets ne sont pas correctes.

L'utilisation d'un tel code de vérification, calculé en fonction de la première partie de l'information tronquée qui n'est pas incluse dans le paquet chiffré, permet donc de vérifier la valeur de la première partie du compteur de paquets estimée par le réseau d'accès 30, et permet donc d'éviter le cas où les données chiffrées d'un paquet chiffré seraient déchiffrées à partir d'une clé de déchiffrement erronée du fait d'une erreur dans l'estimation de la première partie du compteur de paquets.

Différentes méthodes plus ou moins robustes sont connues de l'homme de l'art pour vérifier l'intégrité de données, comme par exemple l'utilisation d'un bit de parité, ou un contrôle de redondance cyclique (CRC). Dans la suite de la description, on se place de manière non limitative dans le cas où le code de vérification est un Code d'Authentification de Message ou CAM (« Message Authentication Code » ou MAC dans la littérature anglo-saxonne) calculé en fonction en outre d'une clé d'authentification du terminal 20 qui est également connue a priori par le réseau d'accès 30.

Il est en effet courant, dans un système de communication, d'utiliser un code d'authentification de message pour vérifier simultanément l'authenticité d'un paquet reçu et l'intégrité des données contenues dans ce paquet. Dans notre exemple, comme ce code est calculé en fonction en outre de la première partie du compteur de paquets, il permet également, sans augmenter la quantité d'informations à inclure dans le paquet chiffré, de vérifier au niveau du réseau d'accès 30 l'estimation de la première partie du compteur

de paquets d'un paquet reçu. Ainsi, un tel code de vérification permet au réseau d'accès 30 :

- de vérifier l'intégrité des données chiffrées reçues ;
- de vérifier la valeur estimée de la première partie du compteur de paquets ;
- d'authentifier le terminal 20 qui a émis le paquet chiffré.

A.6) Formation du paquet chiffré à émettre

Au cours de l'étape 56 de formation, le paquet chiffré à émettre est formé à partir des données chiffrées, du code de vérification, et du compteur tronqué. En d'autres termes, la valeur du compteur de paquets n'est pas incluse dans le paquet chiffré à émettre, qui ne comporte que le compteur tronqué.

On comprend donc que la quantité d'informations incluses, dans le paquet chiffré, pour encoder le compteur tronqué est inférieure à celle nécessaire pour encoder la valeur du compteur de paquets, puisque le compteur tronqué correspond par exemple aux Nb2 bits de poids faible parmi les Nb1 bits du compteur de paquets. Par conséquent, les (Nb1 – Nb2) bits de poids fort (« Most Significant Bits » ou MSB dans la littérature anglo-saxonne) du compteur de paquets, qui correspondent à la première partie dudit compteur de paquets, ne sont pas inclus dans le paquet chiffré à émettre, ce qui correspond à 116 bits non inclus dans le cas où Nb1 est égal à 128 et où Nb2 est égal à 12.

Ainsi, il est possible d'assurer un bon niveau de confidentialité, par le choix d'une valeur Nc élevée, tout en limitant la quantité d'informations à inclure dans le paquet chiffré, par le choix d'une valeur Nt significativement inférieure.

Le paquet chiffré ainsi formé est ensuite émis, par le terminal 20, à destination du réseau d'accès 30.

A.7) Variante de mise en œuvre utilisant un paquet de recalage

La figure 3 représente les principales étapes d'une variante de mise en œuvre du procédé 50 d'émission comportant, outre les étapes décrites ci-avant en référence à la figure 2, une étape 56 de formation d'un paquet de recalage à partir d'une information de recalage représentative de la première partie du

compteur de paquets.

Ce paquet de recalage peut être émis de manière récurrente, par exemple de manière périodique, ou bien à chaque fois que la valeur de la première partie du compteur de paquets varie, ou à chaque fois que le terminal 20 émet un nombre prédéterminé de paquets chiffrés, etc.

Comme cela sera expliqué plus en détail par la suite, l'information de recalage permet, lors de la réception d'un paquet chiffré par le réseau d'accès 30, d'améliorer l'estimation de la valeur de la première partie du compteur de paquets.

Il est à noter que le compteur de paquets du terminal 20 peut ne compter que les paquets chiffrés, tout comme il peut également compter l'ensemble des paquets émis, en incluant les paquets de recalage. Ce choix de comportement du compteur de paquets ne constitue qu'une variante de mise en œuvre de l'invention.

Il est à noter également que le paquet de recalage peut ne comporter que l'information de recalage, tout comme il peut également comporter d'autres informations, comme par exemple des données chiffrées, ou la seconde partie du compteur de paquets (par exemple si le compteur de paquets est incrémenté lors de l'émission d'un paquet de recalage).

Dans la suite de la description, on se place de manière non limitative dans le cas où ;

- l'information de recalage est la première partie du compteur de paquets, c'est-à-dire les (Nb1 – Nb2) bits de poids fort du compteur de paquets dans l'exemple considéré,
- un paquet de recalage est émis à chaque fois que le compteur a été incrémenté Nt fois exactement, c'est-à-dire à chaque fois que la seconde partie du compteur de paquets (les Nb2 bits de poids faible) repasse à zéro, c'est-à-dire aussi à chaque fois que la première partie du compteur de paquets (les (Nb1 – Nb2) bits de poids fort) est incrémentée,
- le compteur de paquets du terminal 20 est incrémenté lors de l'émission d'un paquet de recalage.

Pour permettre au réseau d'accès 30 de discriminer les différents

types de paquets reçus (paquet chiffré, paquet de recalage, ou autre), une information permettant d'identifier le type de paquet peut être incluse dans le paquet. Cet aspect sort du cadre de l'invention.

B) Procédé d'extraction des données incluses dans le paquet

La figure 4 représente schématiquement les principales étapes d'un procédé 60 d'extraction, par le réseau d'accès 30, de données incluses dans un paquet reçu d'un terminal 20, ledit paquet ayant été émis conformément à un procédé 50 d'émission selon l'un des modes de mise en œuvre de l'invention. Dans la suite de la description, on désigne le paquet chiffré à partir duquel on cherche à extraire des données par « paquet chiffré en cours », afin de le distinguer d'autres paquets précédemment reçus du même terminal 20.

Tel qu'illustré par la figure 4, le procédé 60 d'extraction de données comporte les étapes suivantes, qui seront décrites en détail ci-après :

- 61 extraction, à partir du paquet chiffré en cours, de l'information tronquée, du code de vérification, et des données chiffrées incluses dans le paquet chiffré en cours,
- 62 estimation d'une valeur candidate pour la première partie de l'information de génération du terminal 20 pour le paquet chiffré en cours en fonction de l'information tronquée extraite du paquet chiffré en cours,
- 63 évaluation d'intégrité du paquet chiffré en cours en fonction de la valeur candidate estimée, des données chiffrées, et du code de vérification extraits dudit paquet chiffré en cours,
- lorsque le paquet chiffré en cours est considéré comme intègre :
    - 64 détermination d'une clé de déchiffrement en fonction de la valeur de l'information de génération du terminal 20 estimée pour le paquet chiffré en cours,
    - 65 déchiffrement des données chiffrées extraites du paquet chiffré en cours en fonction de la clé de déchiffrement.

Il est à noter que les étapes représentées par la figure 4 sont toutes mises en œuvre par le réseau d'accès 30.

Dans l'exemple décrit en référence à la figure 1, dans lequel le réseau d'accès 30 comporte une pluralité de stations de base 31 et un serveur 32, le

paquet chiffré en cours, à partir duquel on cherche à extraire les données, est initialement reçu par une ou plusieurs stations de base 31.

Chaque station de base 31 comporte à cet effet des moyens de communication sans fil, considérés comme connus de l'homme de l'art, permettant à ladite station de base de recevoir des paquets émis par un ou plusieurs terminaux 20 sous la forme de signaux radioélectriques.

Par contre, les étapes du procédé 60 d'extraction de données, représentées sur la figure 4, peuvent être exécutées par la ou les stations de base 31 ayant reçu le paquet chiffré en cours et/ou par le serveur 32.

Dans la suite de la description, on se place de manière non limitative dans le cas où les étapes listées ci-dessus sont toutes mises en œuvre par le serveur 32, après avoir reçu le paquet chiffré en cours de la ou des stations de base 31 ayant initialement reçu ledit paquet chiffré en cours sur le lien montant.

A cet effet, les stations de base 31 et le serveur 32 comportent des moyens de communication de réseau respectifs, considérés comme connus de l'homme de l'art, permettant aux stations de base 31 de transmettre chaque paquet reçu au serveur 32.

Le serveur 32 comporte par exemple un circuit de traitement (non représenté sur les figures), comportant un ou plusieurs processeurs et des moyens de mémorisation (disque dur magnétique, mémoire électronique, disque optique, etc.) dans lesquels est mémorisé un produit programme d'ordinateur, sous la forme d'un ensemble d'instructions de code de programme à exécuter pour mettre en œuvre les différentes étapes du procédé 60 d'extraction de données. Alternativement ou en complément, le circuit de traitement comporte un ou des circuits logiques programmables (FPGA, PLD, etc.), et/ou un ou des circuits intégrés spécialisés (ASIC), et/ou un ensemble de composants électroniques discrets, etc., adaptés à mettre en œuvre tout ou partie desdites étapes du procédé 60 d'extraction de données.

En d'autres termes, le circuit de traitement comporte un ensemble de moyens configurés de façon logicielle (produit programme d'ordinateur spécifique) et/ou matérielle (FPGA, PLD, ASIC, composants électroniques discrets, etc.) pour mettre en œuvre les étapes du procédé 60 d'extraction de données à partir du paquet chiffré en cours reçu du terminal 20.

Tel qu'indiqué précédemment, différents types d'information de génération peuvent être considérés. Dans la suite de la description, on se place de manière non limitative dans le cas où l'information de génération est le compteur de paquets du terminal 20. On se place en outre dans le cas où l'information tronquée incluse par le terminal 20 dans le paquet émis est un compteur tronqué qui correspond à la valeur dudit compteur de paquets modulo Nt. En d'autres termes, le compteur tronqué est égal à la seconde partie du compteur de paquets du terminal 20. Pour les autres cas, dans lesquels le compteur tronqué n'est pas directement égal à la seconde partie du compteur de paquets, il suffit, pour obtenir ladite seconde partie du compteur de paquets, d'appliquer sur le compteur tronqué du paquet chiffré en cours la fonction inverse de la fonction de calcul utilisée par le terminal 20.

B.1) Extraction du compteur tronqué, du code de vérification, et des données chiffrées

Au cours de l'étape 61 d'extraction, le serveur 32 extrait du paquet chiffré en cours le compteur tronqué, le code de vérification, et les données chiffrées. L'extraction du compteur tronqué, du code de vérification, et des données chiffrées dépend de la manière dont ils ont été incorporés dans le paquet chiffré en cours, et sort du cadre de l'invention.

B.2) Estimation d'une valeur candidate de la première partie du compteur de paquets

Au cours de l'étape 62 d'estimation, le serveur 32 estime une valeur candidate de la première partie du compteur de paquets du terminal 20 qui a émis le paquet chiffré en cours.

En effet, tel qu'indiqué précédemment, le paquet chiffré en cours comporte uniquement le compteur tronqué du terminal 20 qui l'a émis, et ne comporte donc pas entièrement la valeur du compteur de paquets dudit terminal 20, puisque le compteur tronqué correspond uniquement aux Nb2 bits de poids faible parmi les Nb1 bits du compteur de paquets.

Toutefois, étant donné que la clé de chiffrement, utilisée par ledit terminal 20 pour chiffrer les données incluses dans le paquet chiffré en cours, a été déterminée en fonction de la valeur du compteur de paquets dudit terminal 20, le serveur 32 doit estimer la valeur de la première partie dudit compteur de

paquets du terminal 20 pour en déduire la valeur complète du compteur de paquets, et ainsi pouvoir déterminer à son tour la clé de déchiffrement à utiliser, qui est identique à la clé de chiffrement.

En pratique, le serveur 32 peut estimer la valeur de la première partie du compteur de paquets du terminal 20 lors de l'émission du paquet chiffré en cours, en fonction :

- du compteur tronqué extrait dudit paquet chiffré en cours et
- de la valeur de la première partie du compteur de paquets dudit terminal 20 estimée et vérifiée pour un paquet précédent reçu du même terminal 20.

Par « paquet précédent reçu », il est entendu le dernier paquet reçu du terminal 20 avant le paquet chiffré en cours, parmi les paquets pour lesquels le compteur de paquets du terminal 20 est incrémenté, et pour lequel la valeur de la première partie du compteur de paquets a pu être estimée et vérifiée. Il est à noter qu'il peut donc s'agir d'un autre paquet chiffré, ou d'un autre type de paquet comme par exemple un paquet de recalage.

Ainsi, le serveur 32 mémorise la valeur estimée de la première partie du compteur de paquets utilisée par le terminal 20 lors de l'émission du paquet précédent reçu dudit terminal 20, et met à jour la valeur estimée de ladite première partie du compteur de paquets à chaque fois qu'un nouveau paquet est reçu dudit terminal 20. Pour initialiser ce processus, il est par exemple possible de forcer le terminal 20 à utiliser une valeur initiale prédéfinie de la première partie du compteur de paquets lors de sa toute première émission de paquet, de préférence égale à zéro. Le cas échéant, le serveur 32 considère, lorsqu'il reçoit pour la première fois un paquet émis par ce terminal 20 (qui n'est pas nécessairement le premier paquet émis par le terminal 20 si certains paquets ont été manqués par le réseau d'accès 30), que la valeur estimée de la première partie du compteur de paquets pour le paquet précédent reçu du même terminal 20 est égale à ladite valeur initiale prédéfinie.

A partir de la valeur de la première partie du compteur de paquets estimée pour le paquet précédent reçu du terminal 20, et à partir du compteur tronqué extrait du paquet chiffré en cours, il est alors possible pour le serveur 32 d'estimer la valeur dudit compteur de paquets dudit terminal 20 pour le

paquet chiffré en cours.

Par exemple, la valeur de la première partie du compteur de paquets du terminal 20 pour le paquet chiffré en cours est estimée selon l'expression suivante :

$$C_1(n) = (C_1(n-1) + k) \text{ modulo } 2^{(Nb1-Nb2)}$$

et la valeur du compteur de paquets du terminal 20 pour le paquet chiffré en cours est estimée selon l'expression suivante :

$$C(n) = (C_1(n) \cdot Nt + C_2(n))$$

expressions dans lesquelles :

- C(n) correspond à la valeur du compteur de paquets du terminal 20 estimée pour le paquet chiffré en cours,
- $C_1(n)$ correspond à la première partie du compteur de paquets pour le paquet chiffré en cours,
- $C_2(n)$ correspond au compteur tronqué extrait du paquet chiffré en cours,
- $C_1(n-1)$ correspond à la valeur de la première partie du compteur de paquets du terminal 20 estimée et vérifiée pour le paquet précédent,
- k est un nombre entier à déterminer.

Dans notre exemple, la valeur k correspond au nombre de retours à zéro de la seconde partie du compteur de paquets du terminal 20 depuis le paquet précédent reçu. En effet, la valeur de la première partie du compteur de paquets (correspondant aux (Nb1 – Nb2) bits de poids fort du compteur) est incrémentée à chaque fois que la valeur de la seconde partie du compteur de paquets (la partie tronquée, correspondant aux Nb2 bits de poids faible du compteur) repasse à zéro.

Par exemple, il est possible de considérer d'office que le nombre de paquets éventuellement manqués par le réseau d'accès 30, entre le paquet chiffré en cours et le paquet précédent reçu du même terminal 20, est inférieur à Nt.

Dans ce cas, si le compteur tronqué du paquet chiffré en cours est supérieur au compteur tronqué du paquet précédent, alors le nombre k est égal

à zéro (k = 0). Pour obtenir la valeur estimée du compteur de paquets pour le paquet chiffré en cours, il suffit de remplacer, dans la valeur du compteur de paquets estimée pour le paquet précédent, les Nb2 bits de poids faible par les Nb2 bits du compteur tronqué extrait du paquet chiffré en cours.

Par contre, si le compteur tronqué du paquet chiffré en cours est inférieur au compteur tronqué du paquet précédent, alors le nombre k est égal à un (k = 1), car il y a eu un retour à zéro. Pour obtenir la valeur estimée du compteur de paquets pour le paquet chiffré en cours, il faut alors remplacer, dans la valeur du compteur de paquets estimée pour le paquet précédent, les Nb2 bits de poids faible par les Nb2 bits du compteur tronqué extrait du paquet chiffré en cours, mais également ajouter un (1) aux (Nb1 – Nb2) bits de poids fort de la valeur du compteur de paquets estimée pour le paquet précédent.

La figure 5 représente les principales étapes d'une variante de mise en œuvre du procédé 60 d'extraction de données comportant, outre les étapes décrites ci-avant en référence à la figure 4, une étape 66 d'extraction, à partir d'un paquet de recalage, d'une information de recalage représentative de la première partie du compteur de paquets.

En effet, l'estimation de la valeur de la première partie du compteur de paquets d'un paquet chiffré en cours peut être erronée, notamment dans le cas où un grand nombre, par exemple supérieur à Nt, de paquets consécutifs seraient manqués par le réseau d'accès. Une telle erreur est d'autant plus grave qu'elle entraîne une erreur d'estimation pour tous les paquets suivants.

Il convient donc de corriger cette situation où la valeur mémorisée par le serveur 32 d'une valeur estimée de la première partie du compteur de paquets du terminal 20 est « désynchronisée » avec la valeur réelle de la première partie du compteur de paquets du terminal 20 pour un paquet donné. C'est l'objectif du paquet de recalage.

En effet l'information de recalage incluse dans le paquet de recalage est représentative de la première partie du compteur de paquets. Elle doit permettre en conséquence de déterminer avec une bonne précision la valeur de la première partie du compteur de paquets. Au mieux, et comme c'est le cas dans le mode de mise en œuvre décrit, elle permet de déterminer sans erreur la valeur de la première partie du compteur de paquets. De manière générale,

la valeur de l'information de génération pour un paquet chiffré en cours peut être estimée en concaténant la première partie de l'information de génération déterminée à l'aide de l'information de recalage, avec l'information tronquée extraite du paquet chiffré en cours.

Dans le mode de mise en œuvre considéré, décrit à titre d'exemple non limitatif, l'information de recalage est la première partie du compteur de paquets, un paquet de recalage est émis à chaque fois que le compteur de paquets du terminal 20 a été incrémenté Nt fois exactement, c'est-à-dire à chaque fois que la première partie du compteur change, et le compteur de paquets du terminal 20 est incrémenté à chaque émission d'un paquet de recalage. Il est donc aisé, à la réception d'un paquet de recalage, de déterminer la valeur du compteur de paquets du terminal 20 puisqu'elle correspond, pour ses (Nb1 – Nb2) bits de poids fort, à la valeur de l'information de recalage, et pour ses Nb2 bits de poids faible, à une valeur nulle. En conséquence, un paquet de recalage peut jouer le rôle d'un « paquet précédent reçu » pour lequel la valeur du compteur de paquets a été déterminée sans erreur.

Lors de la réception d'un paquet de recalage, une « désynchronisation » peut être détectée si la valeur de la première partie du compteur de paquets estimée pour le paquet de recalage à partir d'un paquet précédent est différente de la valeur de la première partie du compteur de paquets déterminée à partir de l'information de recalage. Le système 10 est alors resynchronisé pour le terminal 20 en réinitialisant la valeur de la première partie du compteur de paquets du terminal 20 mémorisée par le serveur 32 avec la valeur de l'information de recalage.

B.3) Evaluation de l'intégrité du paquet chiffré en cours

La figure 6 détaille un mode préféré de mise en œuvre de l'étape 63 d'évaluation d'intégrité du paquet chiffré en cours.

Tel qu'illustré par la figure 6, l'étape 63 comporte une étape 631 de calcul d'un code de vérification à partir des données chiffrées et de la valeur candidate estimée de la première partie du compteur de paquets. Ce calcul est effectué selon la même méthode que celle utilisée par le terminal 20 pour calculer le code de vérification à l'émission du paquet chiffré.

L'étape 63 comporte ensuite une étape 632 de comparaison du code de vérification calculé par le serveur 32 avec le code de vérification extrait du paquet chiffré en cours, il est possible d'évaluer l'intégrité du paquet chiffré en cours. Le paquet chiffré n'est considéré comme intègre que si le code de vérification extrait du paquet chiffré en cours et le code de vérification calculé sont identiques.

Si le paquet chiffré en cours est considéré comme intègre, alors la valeur candidate estimée de la première partie du compteur de paquets est jugée correcte, et le serveur 32 peut exécuter l'étape 64 de détermination de la clé de déchiffrement, et l'étape 65 de déchiffrement des données chiffrées.

Si le paquet chiffré en cours n'est pas considéré comme intègre, alors la valeur candidate estimée de la première partie du compteur de paquets est jugée incorrecte, et il n'est en conséquence pas possible de déterminer la clé de déchiffrement. Dans ce cas, le paquet chiffré en cours peut par exemple être simplement ignoré, ou bien il peut éventuellement être mémorisé pour repasser ultérieurement par une nouvelle étape d'estimation d'une valeur candidate de la première partie du compteur de paquets, par exemple suite à la réception d'un paquet de recalage.

Dans le mode de mise en œuvre considéré, décrit à titre d'exemple non limitatif, le code de vérification est un Code d'Authentification de Message ou CAM (« Message Authentication Code » ou MAC dans la littérature anglo-saxonne) calculé en fonction en outre d'une clé d'authentification qui est connue à la fois par le terminal 20 et par le serveur 32. Le serveur 32 peut par exemple déterminer la clé d'authentification à utiliser grâce à une information incluse dans le paquet chiffré en cours qui permet d'identifier de manière unique le terminal 20 qui a émis le paquet. De manière plus générale, la détermination, par le serveur 32, de la clé d'authentification à utiliser peut mettre en œuvre toute méthode connue de l'homme de l'art et sort du cadre de l'invention.

Dans un tel cas, le code de vérification permet de vérifier simultanément l'authenticité du paquet chiffré en cours, l'intégrité des données chiffrées contenues dans ce paquet chiffré, et aussi la valeur candidate

estimée de la première partie du compteur de paquets du paquet chiffré en cours.

B.4) Détermination de la clé de déchiffrement

Au cours de l'étape 64 de détermination, le serveur 32 détermine la clé de déchiffrement à utiliser pour déchiffrer les données chiffrées extraites du paquet chiffré en cours.

La valeur du compteur de paquets du terminal 20 pour le paquet chiffré en cours est déduite à partir de la valeur candidate estimée et vérifiée de la première partie, et à partir de l'information tronquée. La clé de déchiffrement est ensuite déterminée, à partir de la valeur du compteur de paquets du terminal 20 pour le paquet chiffré en cours, selon la même méthode de génération de clé que celle utilisée par le terminal 20 pour générer la clé de chiffrement. En l'absence d'erreurs, la clé de déchiffrement est donc identique à la clé de chiffrement.

B.5) Déchiffrement des données chiffrées

Au cours de l'étape 65 de déchiffrement, le serveur 32 déchiffre les données chiffrées extraites du paquet chiffré en cours, en fonction de la clé de déchiffrement obtenue à l'issue de l'étape 64 de détermination.

Le déchiffrement des données chiffrées dépend du protocole de chiffrement à clé symétrique considéré, et sort du cadre de l'invention. Par exemple, dans le cas d'un protocole de chiffrement de flux dans lequel les données chiffrées sont obtenues en combinant un à un les bits successifs des données et de la clé de chiffrement au moyen d'une fonction logique de type « OU EXCLUSIF », alors les données non chiffrées sont obtenues également en combinant un à un les bits successifs des données chiffrées et de la clé de déchiffrement au moyen d'une fonction logique de type « OU EXCLUSIF ».

B.6) Estimation de plusieurs valeurs candidates

La figure 7 représente les principales étapes d'une variante de mise en œuvre du procédé 60 d'extraction de données comportant, outre les étapes décrites ci-avant en référence à la figure 5, l'estimation et la vérification de plusieurs valeurs candidates de la première partie du compteur de paquets jusqu'à ce qu'un critère d'arrêt soit vérifié.

Ainsi, un ensemble de plusieurs valeurs candidates de la première partie du compteur de paquets du paquet chiffré en cours est défini, et chaque valeur candidate estimée est vérifiée itérativement à l'aide du code de vérification. Le critère d'arrêt est par exemple vérifié lorsque, pour une valeur candidate donnée, l'intégrité du paquet chiffré en cours est vérifiée, ou bien dès que l'ensemble des valeurs candidates est épuisé sans qu'aucune valeur candidate n'ait pu permettre de considérer le paquet chiffré en cours comme intègre.

Cette variante de mise en œuvre permet de pallier la possibilité qu'un grand nombre, par exemple supérieur à Nt, de paquets consécutifs soient manqués par le réseau d'accès 30. En effet, dans un tel cas l'estimation de la valeur candidate de la première partie du compteur de paquets pour le paquet chiffré en cours telle qu'elle a été présentée dans la section B.3 est fausse, et il est alors avantageux d'estimer plusieurs valeurs candidates différentes de la première partie du compteur de paquets, afin de permettre l'extraction des données.

Dans le mode de mise en œuvre considéré, et décrit à titre d'exemple non limitatif, la variable k introduite dans la section B.3 représente, pour un paquet chiffré en cours, le nombre de retours à zéro de la seconde partie du compteur de paquets du terminal 20 depuis le dernier paquet précédent reçu pour lequel la valeur de la première partie du compteur de paquets a pu être estimée et vérifiée.

Pour obtenir différentes valeurs candidates, il est possible d'incrémenter itérativement la valeur de k, en partant d'une valeur nulle, et de procéder ainsi jusqu'à ce que l'intégrité du paquet chiffré en cours soit vérifiée pour une valeur candidate donnée.

Le paquet chiffré en cours peut cependant être considéré comme n'étant pas intègre suite à une erreur de transmission altérant les données chiffrées (par exemple due à des interférences) ou bien si une mauvaise clé d'authentification a été utilisée. Dans un tel cas, il serait fâcheux d'itérer indéfiniment sur des valeurs candidates pour lesquelles le paquet chiffré ne pourra pas être considéré comme intègre. Aussi, il convient de borner l'ensemble des valeurs candidates possibles.

Pour ce faire, il est par exemple possible de définir la fréquence maximale à laquelle le terminal 20 peut émettre des paquets à destination du réseau d'accès 30. En mémorisant la date de réception du dernier paquet reçu, et en calculant le nombre maximum de paquets qui auraient pu être émis par le terminal 20 depuis cette date à la date de réception du paquet chiffré en cours, il est possible de définir le nombre maximum de retours à zéro qu'aurait pu faire la seconde partie du compteur de paquets du terminal 20 pendant cette période de temps selon l'expression suivante :

$$k_{max} = E\left[\frac{t(n) - t(n-1)}{Nt} \cdot F_{max}\right]$$

expression dans laquelle :

- t(n-1) est la date de réception du paquet précédent,
- t(n) est la date de réception du paquet courant,
- F_{max} est la fréquence maximale d'émission de paquets,
- E[x] correspond à la partie entière de x,
- k_{max} est le nombre maximal de retours à zéro de la seconde partie du compteur de paquets du terminal 20 pendant la période de temps entre t(n-1) et t(n).

L'ensemble des valeurs candidates de la première partie du compteur de paquets à considérer est alors défini par :

$C_1(n) = (C_1(n-1) + k)$ modulo $2^{(Nb1-Nb2)}$, avec k variant entre 0 et $k_{max.}$

On comprend cependant qu'il existe d'autres méthodes pour définir un ensemble de valeurs candidates de la première partie du compteur de paquets. En particulier, il est par exemple possible d'estimer la valeur la plus probable de la première partie du compteur de paquets en fonction d'un temps moyen d'émission de paquets par le terminal 20. D'autres valeurs candidates peuvent ensuite être définies à partir de la valeur la plus probable, et vérifiées itérativement par ordre décroissant de probabilité. Le choix d'une méthode particulière ne constitue qu'une variante d'implémentation de l'invention.

En effet, bien que, dans l'exemple considéré ici à titre non limitatif, les terminaux 20 émettent leurs paquets de manière asynchrone, lesdits terminaux 20 peuvent néanmoins émettre leurs paquets avec une certaine régularité. Par

exemple, un terminal 20 peut émettre un nombre prédéterminé de paquets par jour, sans toutefois émettre lesdits paquets de manière strictement périodique. Dans un tel cas, lesdits paquets seront néanmoins émis, en moyenne, de manière sensiblement périodique. Dans un tel cas, notamment, il est avantageux d'estimer la période d'émission moyenne entre les émissions de paquets consécutifs par ledit terminal 20, car celle-ci peut permettre d'améliorer l'estimation de la valeur de la première partie du compteur de paquets.

Par exemple, la période d'émission moyenne dudit terminal 20 est calculée selon l'expression suivante :

$$\mathrm{Tem} = \frac{1}{M-1} \cdot \sum_{m=2}^{M} \frac{t(m) - t(m-1)}{C(m) - C(m-1)}$$

expression dans laquelle :

- Tem correspond à la période d'émission moyenne estimée pour le terminal 20,
- C(m) correspond à la valeur du compteur de paquets du terminal 20 estimée pour le paquet de rang m reçu dudit terminal 20,
- t(m) correspond à la date de réception mesurée pour le paquet de rang m reçu dudit terminal 20,
- C(m-1) correspond à la valeur du compteur de paquets du terminal 20 estimée pour le paquet de rang (m-1) reçu dudit terminal 20,
- t(m-1) correspond à la date de réception mesurée pour le paquet de rang (m-1) reçu dudit terminal 20,
- M correspond au nombre total de paquets reçus dudit terminal 20.

Une fois estimée la période d'émission moyenne du terminal 20, la valeur notée k_{prob} la plus probable pour calculer la première partie du compteur de paquets pour le paquet chiffré en cours est par exemple estimée selon l'expression suivante :

$$k_{prob} = E\left[\frac{t(n) - t(n-1)}{\mathrm{Tem} \cdot \mathrm{Nt}}\right] + p$$

expression dans laquelle (t(n) – t(n-1)) correspond à la durée écoulée entre la date de réception du paquet chiffré en cours et la date de réception du paquet

précédent, et p est un nombre entier qui est déterminé comme suit :

- p = 0 si $C_2(n) > C_2(n-1)$,
- p = 1 si $C_2(n) < C_2(n-1)$.

Les valeurs candidates à itérer peuvent alors être, par exemple, définies par l'ensemble :

$$k = k_{prob} \pm i, i \in \mathrm{N}, k \geq 0, k \leq k_{prob} + k_{\max}$$

B.7) Autres types d'information de génération

Dans les exemples de mise en œuvre du procédé 60 d'extraction décrits ci-dessus, on a considéré de manière non limitative le cas où l'information de génération est le compteur de paquets du terminal 20.

Toutefois, tel qu'indiqué précédemment, d'autres types d'information de génération peuvent être considérés, et le choix d'un type particulier d'information de génération, variable au cours du temps, ne constitue qu'une variante de mise en œuvre de l'invention.

On comprend également que l'estimation de la valeur de la première partie de l'information de génération du terminal 20 pour le paquet chiffré en cours peut dépendre du type d'information de génération considéré.

Par exemple, dans le cas où l'information de génération correspond au compteur de paquets du terminal 20, l'estimation de la première partie de la valeur dudit compteur de paquets du terminal 20 pour le paquet chiffré en cours tient avantageusement compte de la valeur de la première partie dudit compteur de paquets estimée pour le paquet précédent reçu du même terminal 20.

Dans le cas où l'information de génération considérée correspond à la date de génération, par le terminal 20, du paquet à émettre, alors il n'est pas nécessaire de tenir compte de la valeur de la première partie de la date de génération estimée pour le paquet précédent reçu du même terminal 20, et la valeur de la première partie de la date de génération du paquet chiffré en cours par le terminal 20 est par exemple estimée en fonction de la date de réception dudit paquet chiffré en cours. En effet, la date de génération du paquet chiffré en cours par le terminal 20 et la date de réception dudit paquet chiffré en cours par le réseau d'accès 30 ont en principe des premières parties respectives

sensiblement identiques, et diffèrent principalement par leurs secondes parties respectives. Etant donné que l'information tronquée extraite du paquet chiffré en cours est représentative de la seconde partie de la date de génération dudit paquet chiffré en cours par le terminal 20, on comprend qu'il est possible d'estimer la valeur de la date de génération dudit paquet chiffré en cours en fonction de l'information tronquée extraite dudit paquet chiffré en cours et en fonction de la date de réception dudit paquet chiffré en cours par le réseau d'accès 30. Par exemple, la valeur de la date de génération du paquet chiffré en cours est obtenue en combinant la première partie de la date de réception du paquet chiffré en cours avec la seconde partie de la date de génération déterminée à partir de l'information tronquée extraite dudit paquet chiffré en cours.

L'utilisation d'une date de génération de paquet comme information de génération suppose néanmoins que les dates courantes du terminal 20 et du réseau d'accès 30 sont synchronisées avec une précision suffisante.

De manière plus générale, il est à noter que les modes de mise en œuvre et de réalisation considérés ci-dessus ont été décrits à titre d'exemples non limitatifs, et que d'autres variantes sont par conséquent envisageables.

Notamment, l'invention a été décrite en considérant uniquement des paquets émis sur le lien montant, depuis les terminaux 20 vers le réseau d'accès 30. L'invention est cependant applicable, alternativement ou en complément, sur un lien descendant depuis le réseau d'accès 30 vers les terminaux 20. En d'autres termes, l'invention est applicable de manière plus générale à l'émission, par un dispositif émetteur, d'un paquet comportant des données chiffrées et à l'extraction, par un dispositif récepteur, des données incluses dans un tel paquet.

En outre, l'invention a été décrite en considérant un système 10 de communication sans fil UNB. Rien n'exclut cependant, suivant d'autres exemples, de considérer d'autres types de systèmes de communication, y compris des systèmes de communication filaires. L'invention trouve cependant une application particulièrement avantageuse dans les systèmes de communication sans fil bas débit, c'est-à-dire de débit inférieur à 1 kilobit/s.

REVENDICATIONS

1 - Procédé (50) d'émission, par un dispositif émetteur (20), de paquets à destination d'un dispositif récepteur (30) d'un système de communication, **caractérisé en ce qu**'il comporte, pour l'émission d'un paquet, dit « paquet chiffré », comportant des données chiffrées selon un protocole de chiffrement à clé symétrique :

- une détermination (51) de la valeur d'une information de génération,
- une détermination (52) d'une clé de chiffrement, à utiliser pour chiffrer les données à inclure dans le paquet chiffré à émettre, en fonction de la valeur de l'information de génération,
- un chiffrement (53) des données à inclure dans le paquet chiffré à émettre en fonction de la clé de chiffrement,
- un calcul (54) d'une information tronquée en décomposant l'information de génération en une première partie et une seconde partie, la première partie variant plus lentement, au cours du temps, que la seconde partie, l'information tronquée étant représentative de la seconde partie de l'information de génération,
- un calcul (55) d'un code de vérification du paquet chiffré en fonction des données chiffrées et de la première partie de l'information de génération,
- une formation (56) du paquet chiffré à émettre à partir de l'information tronquée, du code de vérification et des données chiffrées.

2 - Procédé (50) selon la revendication 1, dans lequel le code de vérification est calculé en fonction en outre d'une clé d'authentification du dispositif émetteur (20).

3 - Procédé selon l'une des revendications précédentes, comportant en outre une formation (57) et une émission d'un paquet, dit « paquet de recalage », incluant une information de recalage représentative de la première partie de l'information de génération.

4 - Procédé (50) selon l'une des revendications précédentes, dans lequel l'information de génération est un compteur de paquets correspondant au

nombre de paquets émis par ledit dispositif émetteur (20) ou une date de génération du paquet à émettre.

5 - Dispositif émetteur (20) pour émettre des paquets à destination d'un dispositif récepteur (30) d'un système de communication, **caractérisé en ce qu'**il comporte, pour l'émission d'un paquet, dit « paquet chiffré », comportant des données chiffrées selon un protocole de chiffrement à clé symétrique :

- des moyens configurés pour déterminer la valeur d'une information de génération,
- des moyens configurés pour déterminer une clé de chiffrement, à utiliser pour chiffrer les données à inclure dans le paquet chiffré à émettre, en fonction de la valeur de l'information de génération,
- des moyens configurés pour chiffrer des données à inclure dans le paquet chiffré à émettre en fonction de la clé de chiffrement,
- des moyens configurés pour calculer une information tronquée en décomposant l'information de génération en une première partie et une seconde partie, la première partie variant plus lentement, au cours du temps, que la seconde partie, l'information tronquée étant représentative de ladite seconde partie,
- des moyens configurés pour calculer un code de vérification du paquet chiffré en fonction des données chiffrées et de la première partie de l'information de génération,
- des moyens configurés pour former le paquet chiffré à émettre à partir de l'information tronquée, du code de vérification, et des données chiffrées.

6 - Dispositif émetteur (20) selon la revendication 5, dans lequel le code de vérification est calculé en fonction en outre d'une clé d'authentification du dispositif émetteur (20).

7 - Dispositif émetteur (20) selon l'une des revendications 5 ou 6, comportant en outre des moyens configurés pour former et émettre un paquet, dit « paquet de recalage », incluant une information de recalage représentative de la première partie de l'information de génération.

8 - Dispositif émetteur (20) selon l'une des revendications 5 à 7, dans lequel

l'information de génération est un compteur de paquets correspondant au nombre de paquets émis par ledit dispositif émetteur (20) ou une date de génération du paquet à émettre.

9 - Procédé (60) d'extraction, par un dispositif récepteur (30), de données incluses dans un paquet chiffré, dit « paquet chiffré en cours », émis par un dispositif émetteur (20) conformément à un procédé d'émission selon l'une des revendications précédentes, **caractérisé en ce qu**'il comporte :

- une extraction (61), à partir du paquet chiffré en cours, de l'information tronquée, du code de vérification et des données chiffrées,
- une estimation (62), en fonction de l'information tronquée extraite, d'une valeur candidate pour la première partie de l'information de génération du dispositif émetteur (20) pour le paquet chiffré en cours,
- une détermination si la valeur candidate estimée est correcte par une évaluation (63) d'intégrité du paquet chiffré en cours en fonction de la valeur candidate estimée, des données chiffrées, et du code de vérification extraits dudit paquet chiffré en cours,
- lorsque la valeur candidate estimée est considérée comme correcte :
    - une détermination (64) d'une clé de déchiffrement en fonction de la valeur candidate estimée et en fonction de l'information tronquée extraite,
    - un déchiffrement (65) des données chiffrées extraites en fonction de la clé de déchiffrement.

10 - Procédé (60) selon la revendication 9, dans lequel l'intégrité du paquet chiffré en cours est évaluée en fonction en outre d'une clé d'authentification du dispositif émetteur (20).

11 - Procédé selon l'une des revendications 9 et 10, comportant en outre une extraction (66) d'une information de recalage incluse dans un paquet émis par le dispositif émetteur (20), dit « paquet de recalage », la valeur candidate de la première partie de l'information de génération du paquet chiffré en cours étant estimée en fonction en outre de l'information de

recalage extraite dudit paquet de recalage.

12 - Procédé (60) selon l'une des revendications 9 à 11, dans lequel plusieurs valeurs candidates pour la première partie de l'information de génération sont estimées, et dans lequel l'intégrité du paquet chiffré en cours est évaluée pour chaque valeur candidate estimée jusqu'à ce qu'un critère d'arrêt soit vérifié.

13 - Procédé (60) selon l'une des revendications 9 à 12, dans lequel l'information de génération est un compteur de paquets du dispositif émetteur (20) dont la valeur de la première partie pour le paquet chiffré en cours est estimée en fonction en outre de la valeur de la première partie estimée et vérifiée pour un paquet précédent reçu du même dispositif émetteur (20).

14 - Procédé (60) selon l'une des revendications 9 à 12, dans lequel l'information de génération correspond à une date de génération du paquet émis par le dispositif émetteur (20) dont la valeur de la première partie est estimée et vérifiée en fonction en outre de la première partie de la date de réception dudit paquet chiffré en cours par le dispositif récepteur (30).

15 - Dispositif récepteur (30) pour recevoir des paquets émis par un dispositif émetteur (20) conformément à un procédé de réception selon l'une des revendications 9 à 14, **caractérisé en ce qu**'il comporte, pour l'extraction des données incluses dans un paquet chiffré en cours :

- des moyens configurés pour extraire, à partir du paquet chiffré en cours, l'information tronquée, le code de vérification, et les données chiffrées,
- des moyens configurés pour estimer une valeur candidate pour la première partie de l'information de génération du dispositif émetteur (20) pour le paquet chiffré en cours en fonction de l'information tronquée extraite,
- des moyens configurés pour déterminer si la valeur candidate estimée est correcte en évaluant l'intégrité du paquet chiffré en cours en fonction de la valeur candidate estimée, des données chiffrées, et du code de vérification extraits,
- des moyens configurés pour déterminer une clé de déchiffrement

en fonction de la valeur candidate considérée comme correcte et de l'information tronquée extraite,

- des moyens configurés pour déchiffrer les données chiffrées extraites du paquet chiffré en cours en fonction de la clé de déchiffrement.

16 - Dispositif récepteur (30) selon la revendication 15, dans lequel l'intégrité du paquet chiffré en cours est évaluée en fonction en outre d'une clé d'authentification du dispositif émetteur (20).

17 - Dispositif récepteur (30) selon l'une des revendications 15 et 16, comportant en outre des moyens configurés pour extraire l'information de recalage incluse dans un paquet de recalage émis par le dispositif émetteur (20), la valeur candidate de la première partie de l'information de génération du paquet chiffré en cours étant estimée en fonction en outre de l'information de recalage extraite dudit paquet de recalage.

18 - Dispositif récepteur (30) selon l'une des revendications 15 à 17, dans lequel plusieurs valeurs candidates pour la première partie de l'information de génération sont estimées, et dans lequel l'intégrité du paquet chiffré en cours est évaluée pour chaque valeur candidate estimée jusqu'à ce qu'un critère d'arrêt soit vérifié.

19 - Dispositif récepteur (30) selon l'une des revendications 15 à 18, dans lequel l'information de génération est un compteur de paquets du dispositif émetteur (20) dont la valeur de la première partie pour le paquet chiffré en cours est estimée en fonction en outre de la valeur de la première partie estimée et vérifiée pour un paquet précédent reçu du même dispositif émetteur (20).

20 - Dispositif récepteur (30) selon l'une des revendications 15 à 18, dans lequel l'information de génération correspond à une date de génération du paquet émis par le dispositif émetteur (20) dont la valeur de la première partie est estimée et vérifiée en fonction en outre de la date de réception dudit paquet chiffré en cours par le dispositif récepteur (30).

21 - Système (10) de communication **caractérisé en ce qu**'il comporte au moins un dispositif émetteur (20) selon l'une des revendications 5 à 8 et au moins un dispositif récepteur (30) selon l'une des revendications 15 à 20.

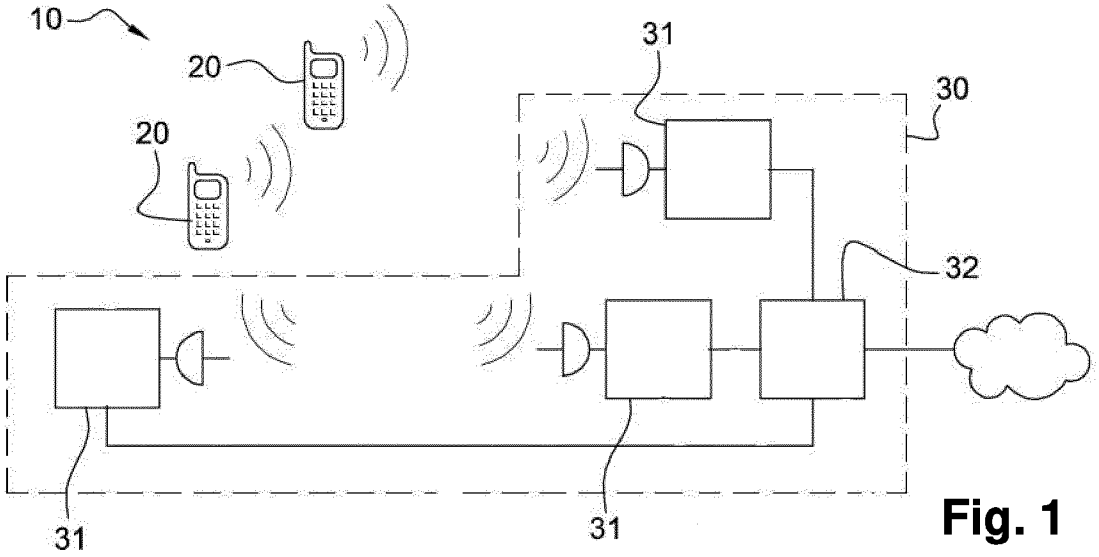
10
20
20
31
30
32
31
31

Fig. 1

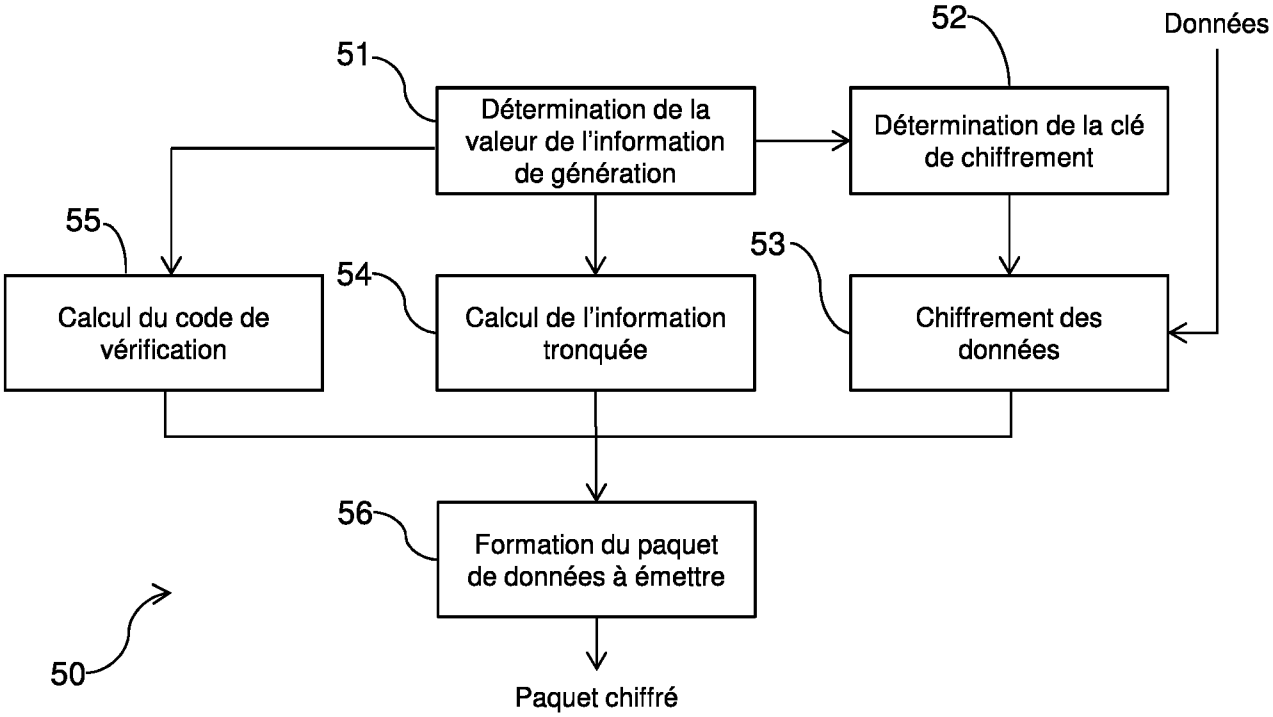
51
Détermination de la valeur de l'information de génération
52
Détermination de la clé de chiffrement
Données
55
Calcul du code de vérification
54
Calcul de l'information tronquée
53
Chiffrement des données
56
Formation du paquet de données à émettre
50
Paquet chiffré

Fig. 2

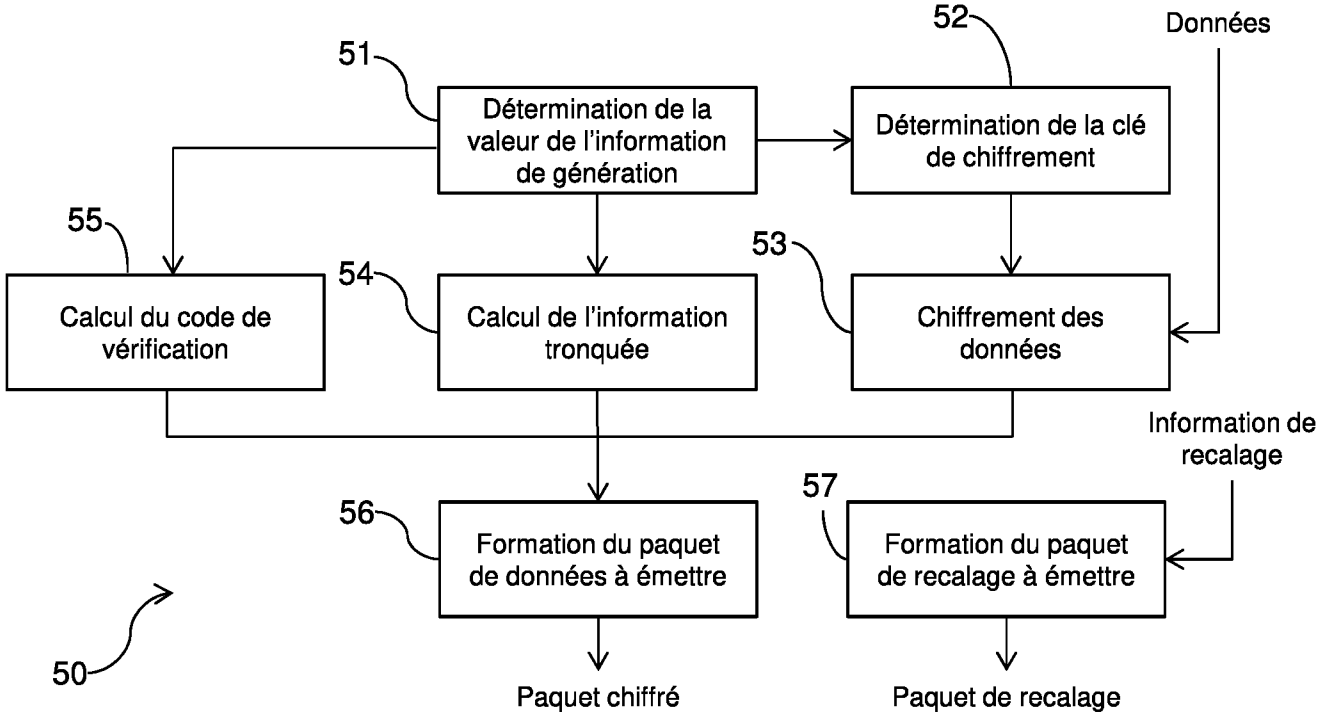
51
Détermination de la valeur de l'information de génération
52
Données
Détermination de la clé de chiffrement
55
Calcul du code de vérification
54
Calcul de l'information tronquée
53
Chiffrement des données
Information de recalage
56
Formation du paquet de données à émettre
57
Formation du paquet de recalage à émettre
50
Paquet chiffré
Paquet de recalage

Fig. 3

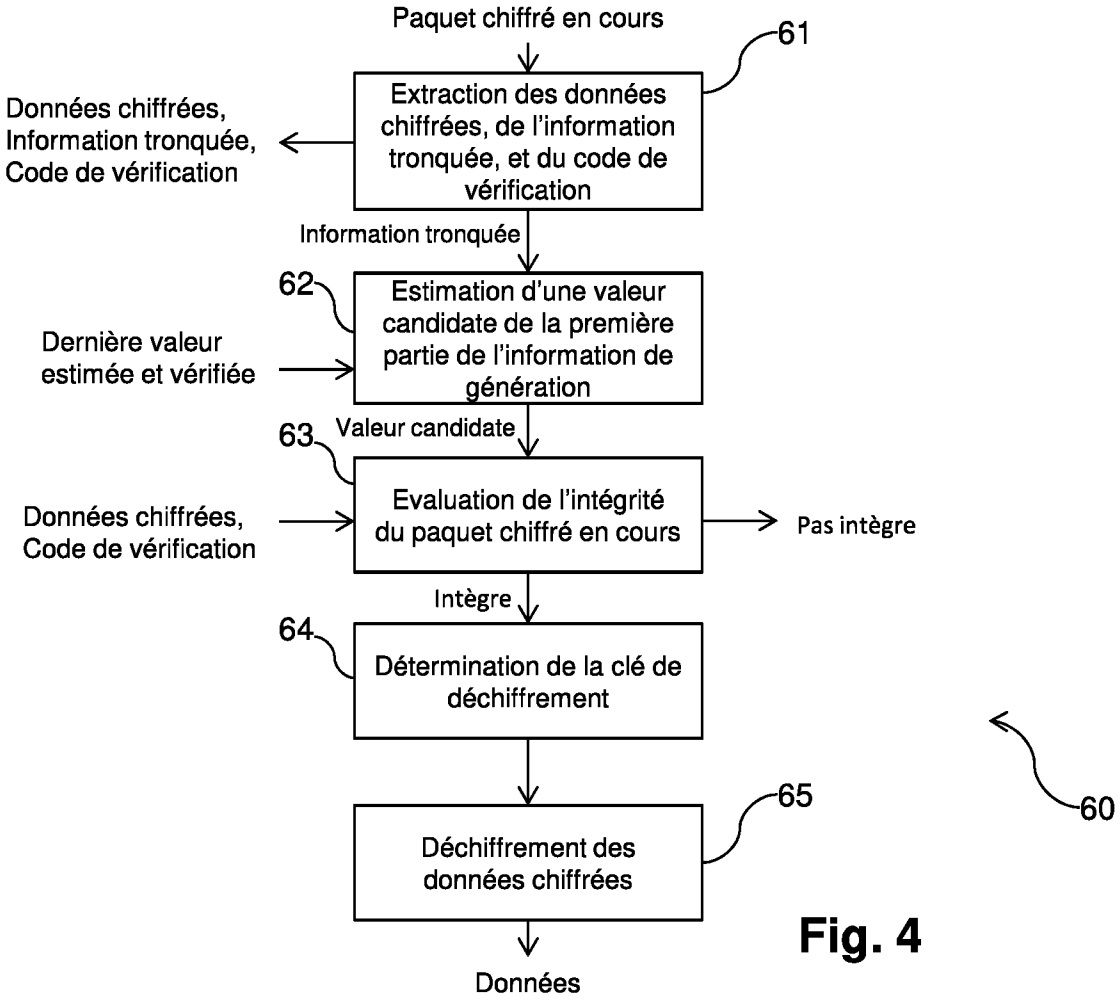
Paquet chiffré en cours
61
Extraction des données chiffrées, de l'information tronquée, et du code de vérification
Données chiffrées, Information tronquée, Code de vérification
Information tronquée
62
Estimation d'une valeur candidate de la première partie de l'information de génération
Dernière valeur estimée et vérifiée
Valeur candidate
63
Evaluation de l'intégrité du paquet chiffré en cours
Données chiffrées, Code de vérification
Pas intègre
Intègre
64
Détermination de la clé de déchiffrement
65
Déchiffrement des données chiffrées
60
Données

Fig. 4

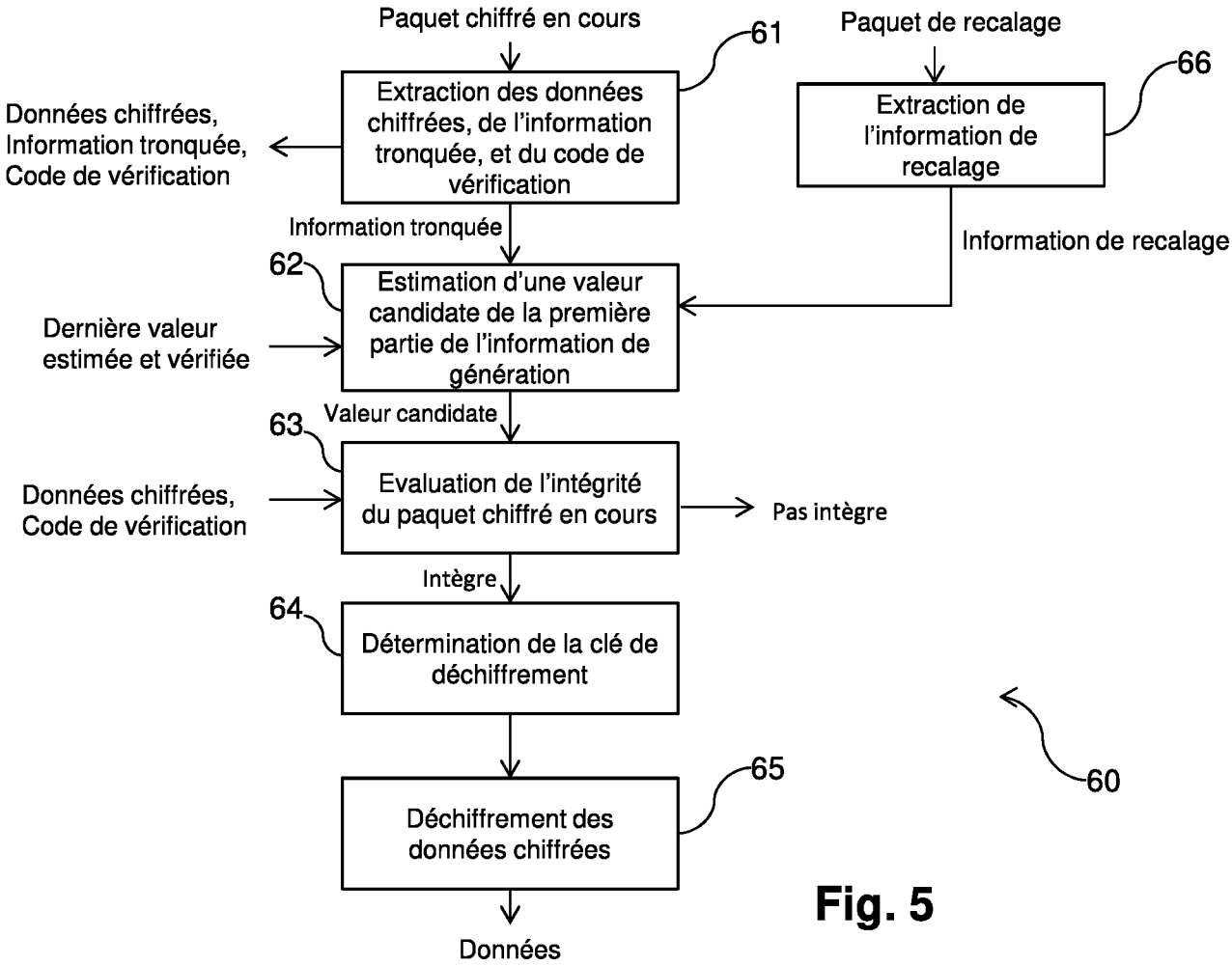
Paquet chiffré en cours
61
Paquet de recalage
66
Extraction des données chiffrées, de l'information tronquée, et du code de vérification
Extraction de l'information de recalage
Données chiffrées, Information tronquée, Code de vérification
Information tronquée
Information de recalage
62
Estimation d'une valeur candidate de la première partie de l'information de génération
Dernière valeur estimée et vérifiée
Valeur candidate
63
Evaluation de l'intégrité du paquet chiffré en cours
Données chiffrées, Code de vérification
Pas intègre
Intègre
64
Détermination de la clé de déchiffrement
60
65
Déchiffrement des données chiffrées
Données

Fig. 5

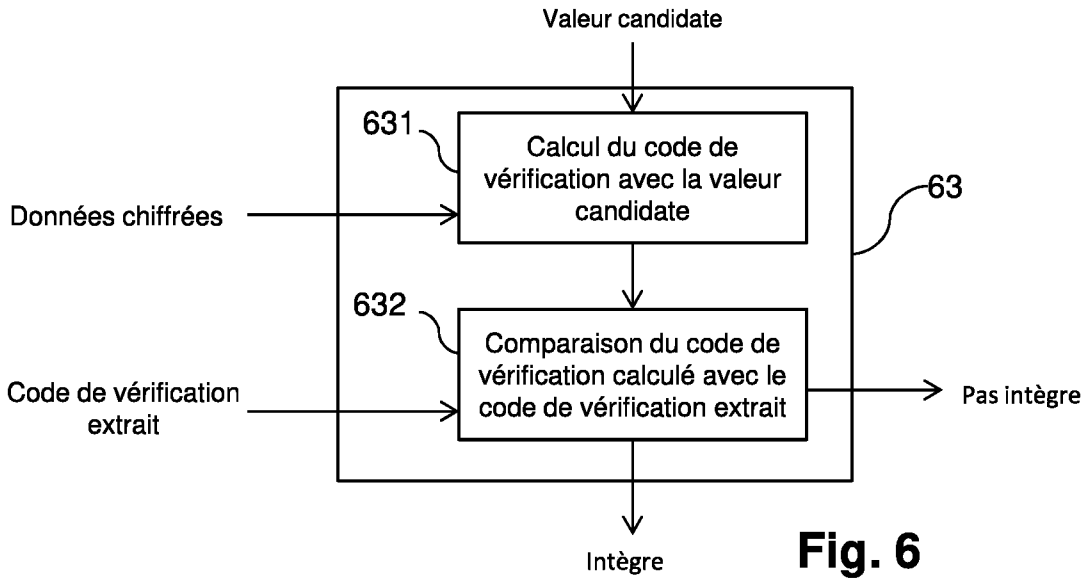
Valeur candidate
631
Calcul du code de vérification avec la valeur candidate
63
Données chiffrées
632
Comparaison du code de vérification calculé avec le code de vérification extrait
Code de vérification extrait
Pas intègre
Intègre

Fig. 6

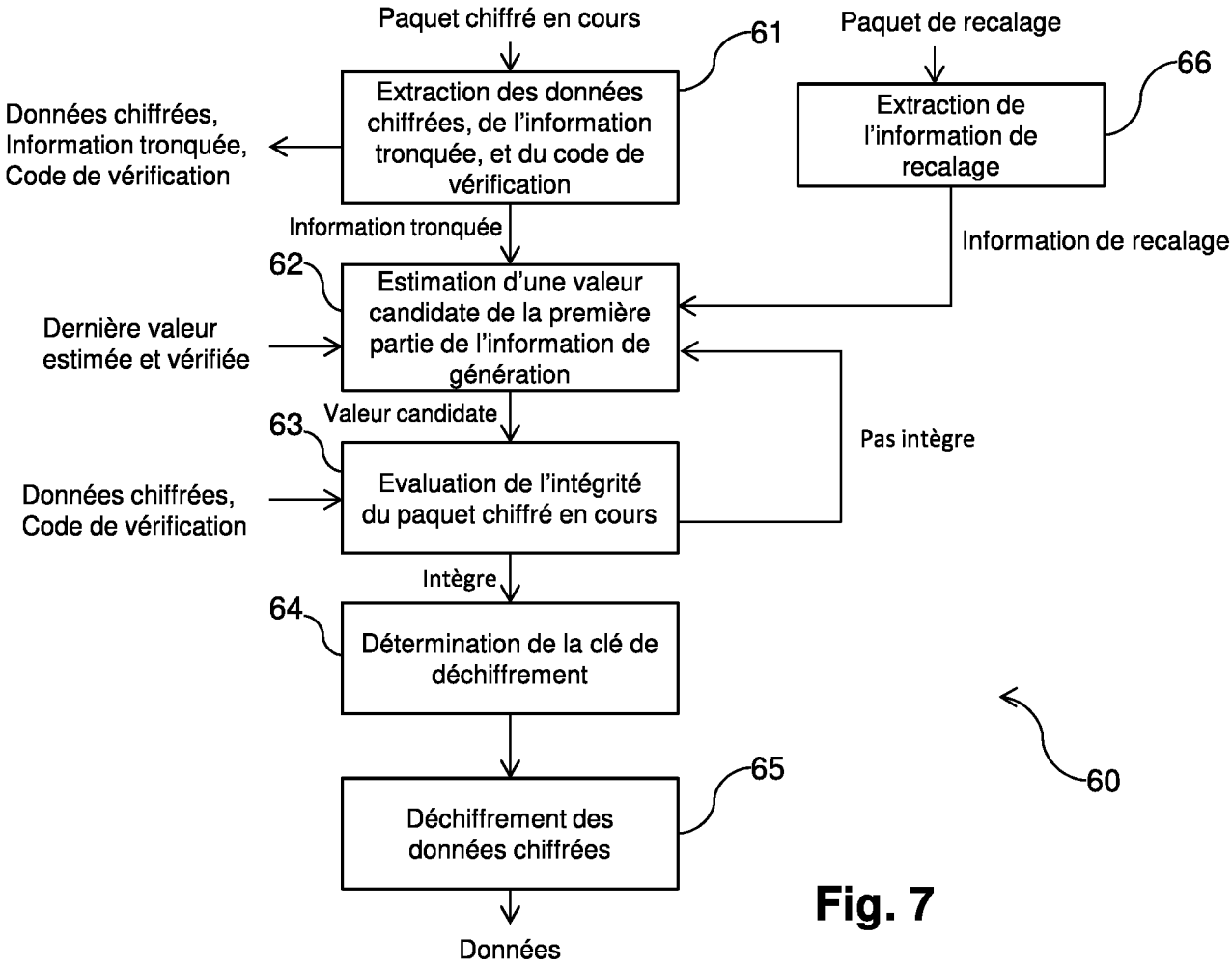
Paquet chiffré en cours
61
Paquet de recalage
66
Extraction des données chiffrées, de l'information tronquée, et du code de vérification
Extraction de l'information de recalage
Données chiffrées, Information tronquée, Code de vérification
Information tronquée
Information de recalage
62
Estimation d'une valeur candidate de la première partie de l'information de génération
Dernière valeur estimée et vérifiée
Valeur candidate
63
Pas intègre
Evaluation de l'intégrité du paquet chiffré en cours
Données chiffrées, Code de vérification
Intègre
64
Détermination de la clé de déchiffrement
60
65
Déchiffrement des données chiffrées
Données

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/078809

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/262937 A1 (HIRTH RYAN E [US] ET AL) 22 October 2009 (2009-10-22)	1-11, 13-17, 19-21
Y	paragraphs [0013], [0054], [0056], [0058], [0063], [0068]; figures 2A, 8B	12,18
X	US 2010/098249 A1 (SHIN JUN-BUM [KR] ET AL) 22 April 2010 (2010-04-22)	1-11, 13-17, 19-21
Y	paragraphs [0031], [0036], [0037], [0043], [0096]; figures 2,5	12,18
Y	EP 3 051 743 A1 (SAMSUNG ELECTRONICS CO LTD [KR]) 3 August 2016 (2016-08-03) paragraphs [0187] - [0188]	12,18

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2018	29/01/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Manet, Pascal

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/078809

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009262937 A1	22-10-2009	CN 102037663 A	27-04-2011
		EP 2291931 A2	09-03-2011
		TW 201004263 A	16-01-2010
		US 2009262937 A1	22-10-2009
		WO 2009131858 A2	29-10-2009
US 2010098249 A1	22-04-2010	KR 20100042457 A	26-04-2010
		US 2010098249 A1	22-04-2010
EP 3051743 A1	03-08-2016	CN 105794147 A	20-07-2016
		EP 3051743 A1	03-08-2016
		JP 2016537850 A	01-12-2016
		KR 20150035355 A	06-04-2015
		KR 20150035364 A	06-04-2015
		KR 20150035456 A	06-04-2015
		US 2016242029 A1	18-08-2016
		US 2017223519 A1	03-08-2017

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2017/078809

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/08 H04L9/32
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2009/262937 A1 (HIRTH RYAN E [US] ET AL) 22 octobre 2009 (2009-10-22)	1-11, 13-17, 19-21
Y	alinéas [0013], [0054], [0056], [0058], [0063], [0068]; figures 2A, 8B	12,18
X	US 2010/098249 A1 (SHIN JUN-BUM [KR] ET AL) 22 avril 2010 (2010-04-22)	1-11, 13-17, 19-21
Y	alinéas [0031], [0036], [0037], [0043], [0096]; figures 2,5	12,18
Y	EP 3 051 743 A1 (SAMSUNG ELECTRONICS CO LTD [KR]) 3 août 2016 (2016-08-03) alinéas [0187] - [0188]	12,18

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
22 janvier 2018	29/01/2018

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Manet, Pascal

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2017/078809

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009262937 A1	22-10-2009	CN 102037663 A	27-04-2011
		EP 2291931 A2	09-03-2011
		TW 201004263 A	16-01-2010
		US 2009262937 A1	22-10-2009
		WO 2009131858 A2	29-10-2009
US 2010098249 A1	22-04-2010	KR 20100042457 A	26-04-2010
		US 2010098249 A1	22-04-2010
EP 3051743 A1	03-08-2016	CN 105794147 A	20-07-2016
		EP 3051743 A1	03-08-2016
		JP 2016537850 A	01-12-2016
		KR 20150035355 A	06-04-2015
		KR 20150035364 A	06-04-2015
		KR 20150035456 A	06-04-2015
		US 2016242029 A1	18-08-2016
		US 2017223519 A1	03-08-2017