

(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
12 avril 2018 (12.04.2018)



(10) Numéro de publication internationale
WO 2018/065707 A1

(51) Classification internationale des brevets :
H04L 9/00 (2006.01) *H04L 29/06* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2017/052690

(22) Date de dépôt international :
29 septembre 2017 (29.09.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1659537 03 octobre 2016 (03.10.2016) FR

(71) Déposant : ORANGE [FR/FR] ; 78 rue Olivier de Serres,
75015 PARIS (FR).

(72) Inventeurs : CANARD, Sébastien ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR). DIOP, Aida ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR). KHEIR, Nizar ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR). PAINDAVOINE, Marie ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR).

(74) Mandataire : ORANGE IMT/OLR/IPL/PATENTS ; RENARD Béatrice, ORANGE GARDENS - 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR).

(54) Title: METHOD AND DEVICE FOR DETECTING INTRUSIONS IN A NETWORK USING A HOMOMORPHIC ENCRYPTION ALGORITHM

(54) Titre : PROCÉDÉ ET DISPOSITIF DE DÉTECTION D'INTRUSIONS SUR UN RÉSEAU UTILISANT UN ALGORITHME DE CHIFFREMENT HOMOMORPHE

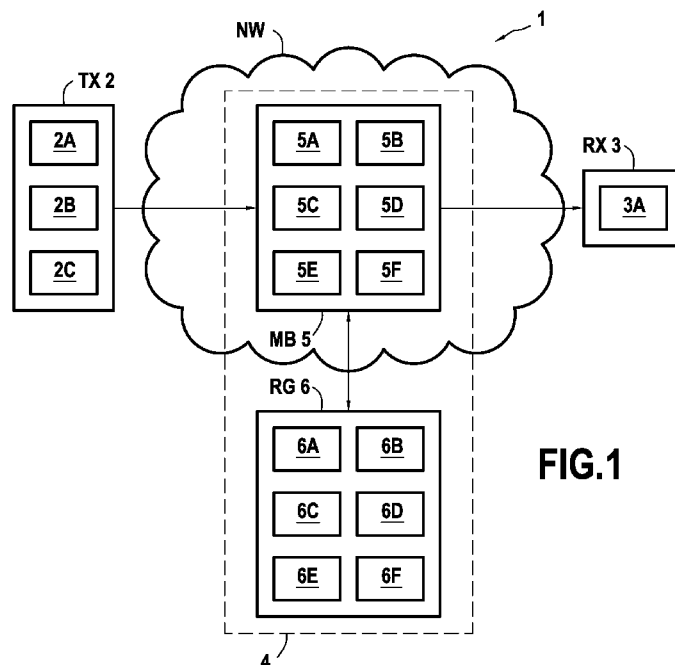


FIG.1

(57) Abstract: Method and device for detecting intrusions in a network using a homomorphic encryption algorithm. The method for detecting intrusions comprises: the reception from a security device (RG 6) having access to at least one rule for detecting intrusions comprising at least one regular expression established from at least one signature, at least one function defining the expression which could be evaluated by means of a homomorphic evaluation function of a homomorphic encryption algorithm, and an encryption of each signature by a homomorphic algorithm encryption procedure and a public key for the security device; the reception from an emitter (TX 2) of an encryption T of content derived from a message obtained by symmetrical encryption by means of a secret key;

(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.

(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))

obtaining an encryption T' from the encryption T and an encryption S from the secret key corresponding to the homomorphic algorithm encryption procedure and the public key for the security device; the evaluation of a symmetrical encryption on the encryption T' by the homomorphic evaluation function with the encryption S, providing an encryption V of the message; the evaluation of said at least one function defining said at least one regular expression in the encryption V with the encryptions of signatures, providing an encryption of a detection result; and the detection of an intrusion if the decrypted result indicates the existence of a regular expression corresponding to the message.

(57) **Abrégé :** Procédé et dispositif de détection d'intrusions sur un réseau utilisant un algorithme de chiffrement homomorphe. Le procédé de détection d'intrusions comprend : la réception depuis un dispositif de sécurité (RG 6) ayant accès à au moins une règle de détection d'intrusions comprenant au moins une expression régulière établie à partir d'au moins une signature, d'au moins une fonction décrivant l'expression pouvant être évaluée au moyen d'une fonction d'évaluation homomorphe d'un algorithme de chiffrement homomorphe, et d'un chiffré de chaque signature par une procédure de chiffrement de l'algorithme homomorphe et une clé publique du dispositif de sécurité; la réception depuis un émetteur (TX 2) d'un chiffré T d'un contenu dérivé d'un message obtenu par chiffrement symétrique au moyen d'une clé secrète; l'obtention d'un chiffré T' du chiffré T et d'un chiffré S de la clé secrète correspondant à la procédure de chiffrement de l'algorithme homomorphe et la clé publique du dispositif de sécurité; l'évaluation d'un déchiffrement symétrique sur le chiffré T' par la fonction d'évaluation homomorphe avec le chiffré S, fournissant un chiffré V du message; l'évaluation de ladite au moins une fonction décrivant ladite au moins une expression régulière sur le chiffré V avec les chiffrés des signatures, fournissant un chiffré d'un résultat de détection; et la détection d'une intrusion si le résultat déchiffré indique l'existence d'une expression régulière correspondant au message.

Procédé et dispositif de détection d'intrusions sur un réseau utilisant un algorithme de chiffrement homomorphe

Arrière-plan de l'invention

5 L'invention se rapporte au domaine général des télécommunications.

Elle concerne plus particulièrement la détection d'intrusions sur un réseau de télécommunications via lequel un dispositif émetteur et un dispositif récepteur s'échangent du trafic chiffré.

De façon connue, les protocoles SSL (Secure Sockets Layer), et plus récemment TLS
10 (Transport Layer Security), sont des protocoles de sécurisation couramment utilisés sur les réseaux comme par exemple sur le réseau public Internet par le protocole HTTPS (HyperText Transfer Protocol Secure) pour assurer la confidentialité des échanges. Ces protocoles permettent de protéger toute donnée sensible partagée par divers dispositifs sur le réseau, en chiffrant les échanges entre ces dispositifs. Malheureusement ce chiffrement rend impuissantes les techniques
15 existantes de détection d'intrusions, qui sont incapables d'inspecter le trafic chiffré échangé sur le réseau.

En effet, les systèmes de détection et de protection contre les intrusions (aussi couramment désignés par IDS (Intrusion Detection Systems) et IPS (Intrusion Protection Systems)) sont classiquement configurés pour surveiller le trafic échangé sur le réseau et identifier
20 des signatures ou des comportements caractéristiques dans ce trafic associés à diverses menaces susceptibles d'affecter le réseau, telles que par exemple l'intrusion de logiciels malveillants ou malwares, la fuite de données sensibles, des attaques perpétrées contre le réseau, etc. A cet effet, ces systèmes mettent en œuvre une inspection des paquets en profondeur plus communément désignée par DPI (pour Deep Packet Inspection en anglais), qui consiste à analyser le contenu d'un
25 paquet réseau (ex. paquet IP) et non pas uniquement son entête, et à comparer ce contenu avec des signatures (ou « patterns » ou encore mots-clés en anglais) caractéristiques de scénarii d'attaques connus. Une telle comparaison peut être réalisée via des tests d'égalité simples ou en utilisant des expressions régulières plus complètes dérivées à partir de ces signatures. On parle alors de systèmes « full IDS ». Ces signatures ou mots-clés, et le cas échéant les expressions
30 régulières, sont déterminé(e)s et fourni(e)s par des éditeurs de sécurité ou autres logiciels à code source ouvert (i.e. « open source »), qui rivalisent entre eux pour proposer un catalogue de signatures à jour couvrant le plus large éventail d'attaques possible sachant que de nouvelles attaques apparaissent chaque jour.

Le point commun de ces systèmes IDS est qu'ils se basent sur l'analyse de
35 communications transmises en clair sur le réseau afin de pouvoir comparer le contenu de ces communications aux signatures préétablies par les éditeurs de sécurité. L'utilisation sur le réseau de procédures de sécurisation telles que SSL ou TLS rend donc impossible l'utilisation en l'état de

ces systèmes, de sorte que les systèmes d'information qui s'appuient sur des échanges chiffrés sur le réseau sont vulnérables à de nombreuses cyber-attaques.

Pour contourner cette limitation, de nombreux éditeurs de sécurité proposent des applications qui se comportent de façon non sécurisée en se positionnant en tant qu'« homme du milieu » (ou man-in-the-middle en anglais) sur une connexion SSL/TLS reliant un dispositif émetteur à un dispositif récepteur, de sorte à intercepter les communications entre ces deux dispositifs. Cette interception est mise en œuvre via l'utilisation de faux certificats de confiance qui permettent de casser le chiffrement de bout en bout utilisé entre les deux dispositifs et d'accéder au contenu en clair de leur échange.

Si une telle solution est satisfaisante du point de vue de la détection des intrusions, elle n'en pose pas moins des problèmes éthiques, juridiques et en termes de confidentialité et de protection de la vie privée des utilisateurs, de sorte que plusieurs navigateurs web aujourd'hui embarquent des plug-ins qui permettent de détecter et de révoquer les faux certificats de confiance utilisés par les systèmes IDS.

Il a ainsi été longtemps considéré qu'il n'était pas possible de satisfaire simultanément aux deux conditions de sécurité du réseau en termes de surveillance et de détection d'intrusions, et de garantie de la vie privée des utilisateurs via le chiffrement de leurs communications.

J. Sherry et al., dans le document intitulé « BlindBox : Deep Packet Inspection over Encrypted Traffic », SIGCOMM'15, 17-21 août 2015, proposent une technique d'inspection de trafic chiffré utilisant des protocoles de chiffrement avancé. Cette technique permet de détecter des attaques perpétrées sur du trafic chiffré via un proxy IDS se trouvant en coupure du trafic (aussi désigné par « middlebox » en anglais). Elle s'appuie sur la fourniture en clair, par l'éditeur de sécurité, des mots-clés à rechercher dans le trafic et le chiffrement par le proxy IDS de ces mots-clés en préliminaire de chaque connexion chiffrée (ex. à chaque connexion SSL) mise en œuvre entre un dispositif émetteur et un dispositif récepteur. Le proxy IDS compare alors via des tests d'égalité les mots-clés ainsi chiffrés avec le trafic échangé entre le dispositif émetteur et le dispositif récepteur. Si une concordance est détectée, le trafic est considéré comme suspect, et différentes actions peuvent dès lors être entreprises, comme par exemple l'envoi d'une notification à l'administrateur du réseau, la suppression du paquet identifié comme suspect, l'arrêt de la connexion entre le dispositif émetteur et le dispositif récepteur, etc. La solution BlindBox prévoit également un mode de réalisation dans lequel, lorsqu'un paquet suspect est identifié, ce paquet est déchiffré par le proxy IDS pour lui appliquer une procédure IDS classique. Il est alors possible au proxy IDS lors de cette procédure de réaliser sur les données en clair de simples tests d'égalité à partir des mots-clés mais également de rechercher dans les données en clair des expressions régulières plus complexes construites à partir des mots-clés.

La solution BlindBox proposée par Sherry et al. présente toutefois divers inconvénients majeurs.

En premier lieu, elle est incompatible avec les règles imposées aujourd'hui par l'écosystème auquel participent les éditeurs de sécurité et les systèmes IDS. En effet, comme mentionné précédemment, la solution BlindBox requiert que l'ensemble des mots-clés et des règles de détection (ex. combinaison de plusieurs mots-clés et/ou expressions régulières) proposés par l'éditeur de sécurité soit accessible en clair par le proxy IDS afin qu'il puisse les chiffrer, et donc plus généralement, par chaque proxy IDS présent dans le réseau. Si cette contrainte n'en est pas une du point de vue théorique, elle n'est pas du tout en phase avec les pratiques en la matière des éditeurs de sécurité, pour des raisons économiques évidentes, les bases de mots-clés et autres règles de détection constituant la valeur ajoutée des éditeurs de sécurité. Par conséquent, bien que théoriquement envisageable, la solution proposée par Sherry et al. n'est pas applicable en pratique dans un réseau.

En outre, la solution BlindBox requiert que l'ensemble des mots-clés soit chiffré à chaque connexion entre un dispositif émetteur et un dispositif récepteur traitée par le proxy IDS (typiquement, à chaque connexion SSL/TLS). Le temps nécessaire à ce chiffrement peut être considérable puisqu'il est directement proportionnel au nombre de mots-clés à prendre en compte, qui peut facilement atteindre quelques centaines voire quelques milliers de mots-clés. De plus, les mots-clés chiffrés pour chaque connexion doivent être stockés en mémoire durant toute la durée de la connexion. L'espace mémoire requis à cette fin doit donc être d'une part, proportionnel au nombre de mots-clés à considérer et d'autre part, au nombre de connexions simultanées pouvant être inspectées par le proxy IDS. On comprend bien dès lors que l'utilisation de la solution BlindBox n'est envisageable que dans des conditions réseau limitées.

Par ailleurs, l'approche retenue par BlindBox n'offre une solution « full IDS » qu'au prix d'un déchiffrement des données issues d'un paquet identifié comme suspect. Même si le déchiffrement des données échangées entre le dispositif émetteur et le dispositif récepteur n'est pas systématique, ceci constitue néanmoins une atteinte à la confidentialité de leurs échanges.

Objet et résumé de l'invention

L'invention permet de remédier à ces inconvénients en proposant un procédé de détection d'intrusions sur un réseau via lequel sont aptes à communiquer un dispositif émetteur et un dispositif récepteur en utilisant un algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre le dispositif émetteur et le dispositif récepteur, ce procédé de détection étant destiné à être mis en œuvre par un dispositif de détection d'intrusions et comprenant :

- une étape de réception, en provenance d'un dispositif de sécurité ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter le réseau, ladite au moins une règle de détection comprenant une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion :

- d'au moins une fonction décrivant ladite au moins une expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation homomorphe d'un algorithme de chiffrement homomorphe ; et
 - d'un chiffré de chaque signature caractéristique de ladite au moins une intrusion, obtenu en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ;
- 5
- une étape de réception, en provenance du dispositif émetteur d'un chiffré T d'un contenu dérivé d'un message destiné au dispositif récepteur, ce chiffré T ayant été obtenu en utilisant
- 10
- une procédure de chiffrement de l'algorithme de chiffrement/déchiffrement symétrique paramétré par ladite clé de chiffrement secrète ;
 - une étape d'obtention d'un chiffré T' du chiffré T et d'un chiffré S de la clé de chiffrement secrète, les chiffrés T' et S correspondant à l'application sur le chiffré T et sur la clé de chiffrement secrète de la procédure de chiffrement dudit algorithme de chiffrement
- 15
- homomorphe paramétrée par la clé de chiffrement publique du dispositif de sécurité ;
 - une première étape d'évaluation d'une procédure de déchiffrement de l'algorithme de chiffrement/déchiffrement symétrique sur le chiffré T en utilisant ladite fonction d'évaluation homomorphe dudit algorithme de chiffrement homomorphe et le chiffré S de la clé de chiffrement secrète, cette première étape d'évaluation fournissant un chiffré V du
- 20
- message destiné au dispositif récepteur par la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé publique de chiffrement du dispositif de sécurité ;
 - une seconde étape d'évaluation de ladite au moins une fonction décrivant ladite au moins une expression régulière sur le chiffré V du message en utilisant les chiffrés des signatures, cette
- 25
- seconde étape d'évaluation fournissant un chiffré d'un résultat de détection indiquant l'existence ou non d'une dite expression régulière correspondant au message ; et
 - une étape de détection d'une intrusion sur le réseau si le résultat de détection déchiffré indique qu'il existe au moins une dite expression régulière correspondant au message.
- Corrélativement, l'invention vise aussi un dispositif de détection d'intrusions sur un
- 30
- réseau via lequel sont aptes à communiquer un dispositif émetteur et un dispositif récepteur en utilisant un algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre le dispositif émetteur et le dispositif récepteur, ledit dispositif de détection étant destiné à être localisé entre le dispositif émetteur et le dispositif récepteur et comprenant :
- 35
- un premier module de réception, apte à recevoir en provenance d'un dispositif de sécurité ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter le réseau, ladite au moins une règle de détection comprenant une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion :

- au moins une fonction décrivant ladite au moins une expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation homomorphe d'un algorithme de chiffrement homomorphe ; et
 - un chiffré de chaque signature caractéristique de ladite au moins une intrusion, obtenu en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ;
- un second module de réception, apte à recevoir en provenance du dispositif émetteur un chiffré T d'un contenu dérivé d'un message destiné au dispositif récepteur, ce chiffré T ayant été obtenu en utilisant une procédure de chiffrement de l'algorithme de chiffrement/déchiffrement symétrique paramétré par ladite clé de chiffrement secrète ;
- un module d'obtention d'un chiffré T' du chiffré T et d'un chiffré S de la clé de chiffrement secrète, les chiffrés T' et S correspondant à l'application sur le chiffré T et sur la clé de chiffrement secrète de la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé de chiffrement publique du dispositif de sécurité ;
- un premier module d'évaluation d'une procédure de déchiffrement de l'algorithme de chiffrement/déchiffrement symétrique sur le chiffré T configuré pour utiliser ladite fonction d'évaluation homomorphe dudit algorithme de chiffrement homomorphe et le chiffré S de la clé de chiffrement secrète, ce premier module d'évaluation étant en outre configuré pour fournir un chiffré V du message destiné au dispositif récepteur par la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé publique de chiffrement du dispositif de sécurité ;
- un second module d'évaluation configuré pour évaluer ladite au moins une fonction décrivant ladite au moins une expression régulière sur le chiffré V du message en utilisant les chiffrés des signatures, ce second module d'évaluation étant en outre configuré pour fournir un chiffré d'un résultat de détection indiquant l'existence ou non d'une dite expression régulière correspondant au message ; et
- un module de détection d'une intrusion sur le réseau activé si le résultat de détection déchiffré indique qu'il existe au moins une dite expression régulière correspondant au message.

On note qu'aucune limitation n'est attachée à la façon dont une intrusion détectée par le dispositif de détection d'intrusions est traitée. La détection d'une telle intrusion peut ainsi par exemple faire uniquement l'objet d'une notification envoyée par le dispositif de détection d'intrusions à l'administrateur du réseau, ou déclencher une action corrective, comme par exemple le rejet du message examiné, l'interruption de la connexion entre le dispositif émetteur et le dispositif récepteur, etc.

L'invention propose ainsi une nouvelle approche permettant le chiffrement d'une communication entre un dispositif émetteur et un dispositif récepteur tout en gardant possible une détection d'intrusions sur le réseau de type DPI (i.e. Deep Packet Inspection ou inspection des

paquets en profondeur) par un dispositif intermédiaire ou « middlebox » se trouvant entre le dispositif émetteur et le dispositif récepteur (dispositif de détection d'intrusions au sens de l'invention). Autrement dit, l'invention offre la possibilité d'assurer la sécurité du réseau tout en garantissant aux utilisateurs de ce réseau le respect de la confidentialité de leurs échanges.

5 Cette approche s'appuie sur l'utilisation d'un algorithme de chiffrement homomorphe qui vient en complément de l'algorithme de chiffrement/déchiffrement symétrique utilisé entre le dispositif émetteur et le dispositif récepteur (ex. algorithme de chiffrement symétrique utilisé lors de connexions SSL/TLS). L'algorithme de chiffrement homomorphe permet avantageusement de rechercher des expressions régulières directement dans le trafic chiffré échangé entre le dispositif
10 émetteur et le dispositif récepteur, ces expressions régulières étant dérivées à partir de signatures (ou de mots-clés) caractéristiques d'intrusions et définies par un éditeur de sécurité (dispositif de sécurité au sens de l'invention). Le schéma de détection d'intrusions proposé par l'invention est donc « full IDS » et très efficace. Il ne requiert aucun déchiffrement pour cela, même partiel, des données échangées entre le dispositif émetteur et le dispositif récepteur, contrairement à la
15 solution BlindBox.

En effet, un algorithme de chiffement homomorphe est classiquement défini par un algorithme de génération de clés cryptographiques, une procédure de chiffement notée ici ENC et une procédure de déchiffement notée ici DEC, ainsi que par une fonction d'évaluation homomorphe, notée ici HOM. Cette fonction d'évaluation homomorphe HOM prend en entrée une
20 pluralité de chiffrés $c_1, c_2, \dots, c_N$, N désignant un entier supérieur à 1, obtenus au moyen de la procédure de chiffement ENC ainsi qu'une fonction f qui se présente sous une forme qui peut être évaluée par la fonction d'évaluation homomorphe, par exemple sous la forme d'un circuit arithmétique. La fonction HOM délivre alors en sortie le résultat de l'application de la fonction f sur les chiffrés $c_1, c_2, \dots, c_N$ (on dit alors que la fonction d'évaluation homomorphe HOM « évalue » la
25 fonction f sur les chiffrés $c_1, c_2, \dots, c_N$). Par abus de notation, on note que la fonction d'évaluation homomorphe HOM vérifie la relation suivante :

$$HOM(c_1, \dots, c_N; f) = f(c_1, \dots, c_N) = ENC(f(m_1, \dots, m_N), pk)$$

où $c_i = ENC(m_i)$ pour $i = 1, \dots, N$, m_i désignant un message qui, une fois chiffré par la procédure de chiffement ENC paramétrée par la clé publique pk , donne le chiffré c_i . L'abus de notation vient ici du fait que ce n'est pas exactement la même fonction f qui est appliquée sur les messages en clair
30 $m_1, \dots, m_N$ et sur les messages chiffrés $c_1, \dots, c_N$. En effet, comme mentionné ci-avant et de façon connue en soi, la fonction d'évaluation homomorphe impose certaines contraintes sur la forme de la fonction f pour pouvoir l'évaluer sur les chiffrés $c_1, \dots, c_N$, contraintes qui ne sont pas nécessaires pour appliquer cette fonction aux messages en clair. Au sens strict du terme, on a donc deux fonctions f et f' appliquées respectivement sur les chiffrés et sur les messages en clair. Toutefois,
35 par souci de simplification dans la suite de la description, et pour faciliter la compréhension de l'invention, on considère une unique notation f pour désigner cette fonction et on entend par évaluation d'une fonction f par la fonction d'évaluation homomorphe, l'évaluation de la fonction f

dans sa forme transformée. Ainsi, à titre d'exemple, et par abus de langage, on entend par évaluation de la procédure de déchiffrement, l'évaluation de cette procédure de déchiffrement sous une forme éventuellement transformée et évaluable par la fonction d'évaluation homomorphe.

La fonction d'évaluation homomorphe HOM permet donc de réaliser toute sorte d'opérations sur des chiffrés résultant de la procédure de chiffrement ENC. Typiquement conformément à l'invention, elle permet d'évaluer d'une part, l'algorithme de déchiffrement symétrique correspondant à l'algorithme de chiffrement symétrique utilisé pour chiffrer les données en clair échangées entre le dispositif émetteur et le dispositif récepteur, et d'autre part, des fonctions décrivant les expressions régulières à rechercher dans le trafic chiffré. En exploitant cette propriété de la fonction d'évaluation homomorphe HOM, l'invention permet au dispositif de détection d'intrusions de manipuler les données chiffrées échangées entre le dispositif émetteur et récepteur sans ne jamais accéder aux données en clair, et d'opérer une recherche d'expressions régulières dérivées par l'éditeur de sécurité à partir des signatures caractéristiques d'intrusions sur le réseau.

Plus particulièrement, et de façon schématique, conformément à l'invention les données en clair échangées entre le dispositif émetteur et le dispositif récepteur sont encapsulées dans deux boîtes hermétiques (c'est-à-dire verrouillées l'une par rapport à l'autre), imbriquées l'une dans l'autre : la boîte « interne » résulte du chiffrement des données en clair au moyen de l'algorithme de chiffrement symétrique utilisé par les dispositifs émetteur et récepteur (donnant un chiffré T), et la boîte « externe » résulte du chiffrement par la procédure de chiffrement de l'algorithme homomorphe du chiffré T ainsi obtenu (donnant un chiffré T'). Puis, l'invention manipule en quelque sorte les données contenues dans ces boîtes pour effectuer une détection DPI sur les données chiffrées en exploitant à deux reprises les propriétés de la fonction d'évaluation homomorphe :

- une première fois pour supprimer la couche de chiffrement symétrique interne. Ceci est réalisé en évaluant au moyen de la fonction d'évaluation homomorphe HOM l'algorithme de déchiffrement symétrique sur le chiffré T'. On déchiffre ainsi en quelque sorte ce qu'il y a à l'intérieur de la boîte externe, sans toutefois accéder directement aux données et clair, puisque le résultat de cette première évaluation est un chiffré V des données en clair via la procédure de chiffrement homomorphe ;
- puis une seconde fois, pour rechercher dans le chiffré V les expressions régulières spécifiées par l'éditeur de sécurité et définies à partir des chiffrés des signatures caractéristiques des intrusions. Cette recherche est permise via l'évaluation au moyen de la fonction d'évaluation homomorphe des expressions régulières ou plus particulièrement d'une description appropriée de chacune des expressions régulières fournie au dispositif de détection d'intrusions et apte à être évaluée par la fonction d'évaluation homomorphe. Une telle description est typiquement un circuit arithmétique (ou circuit booléen), fournie par le dispositif de sécurité pour une ou plusieurs expressions régulières destinées à être recherchées dans le trafic chiffré échangé

entre le dispositif émetteur et le dispositif récepteur. Grâce à cette description sous forme de circuit arithmétique, l'invention permet de ne pas se limiter à de simples tests d'égalité mais d'être en mesure de rechercher dans le trafic chiffré échangé entre le dispositif émetteur et le dispositif récepteur des expressions plus complexes définies à partir des signatures caractéristiques des intrusions.

On note que le résultat de la seconde application de la fonction d'évaluation homomorphe est par définition un chiffré d'un résultat de la détection opérée par le dispositif de détection d'intrusions. Son déchiffrement permet de détecter si une expression régulière spécifiée par l'éditeur de sécurité a été détectée dans les données échangées entre le dispositif émetteur et le dispositif récepteur et en corollaire, de détecter la présence ou non d'une intrusion sur le réseau.

Ce déchiffrement peut être opéré soit par le dispositif d'intrusions lui-même. Ainsi, par exemple, dans un mode particulier de réalisation, le procédé de détection comprend en outre :

- une étape d'obtention d'une clé privée de déchiffrement associée à la clé publique de chiffrement du dispositif de sécurité et stockée dans un module matériel de sécurité (ou HSM pour Hardware Security Module) ; et
- une étape de déchiffrement du chiffré du résultat de détection en utilisant la procédure de déchiffrement de l'algorithme de chiffrement homomorphe paramétrée par cette clé privée de déchiffrement.

Ceci permet de rendre autonome le dispositif de détection d'intrusions vis-à-vis du dispositif de sécurité lors de l'étape ultime de détection d'intrusions. Ce mode de réalisation nécessite toutefois que le dispositif de sécurité « livre » sa clé privée de déchiffrement au dispositif de détection d'intrusions. Le recours à un module matériel de sécurité pour stocker la clé privée de déchiffrement du dispositif de sécurité permet de sécuriser cette solution.

Dans un autre mode de réalisation, le procédé de détection d'intrusions est interactif et comprend en outre :

- une étape de transmission du chiffré du résultat de détection au dispositif de sécurité pour déchiffrement en utilisant une procédure de déchiffrement dudit algorithme de chiffement homomorphe paramétrée par une clé privée de déchiffrement associée à la clé publique de chiffement du dispositif de sécurité ; et
- une étape de réception du résultat de détection déchiffré en provenance du dispositif de sécurité.

Dans ce mode de réalisation, il n'est pas nécessaire au dispositif de sécurité de fournir sa clé secrète au dispositif de détection d'intrusions. Toutefois, ce mode de réalisation interactif nécessite que, lors de la détection d'intrusions mise en œuvre par le dispositif de détection d'intrusions, le dispositif de sécurité soit accessible par celui-ci.

Comme mentionné, l'invention permet donc de réaliser une détection de type DPI full IDS sur le réseau sans compromettre à aucun moment la confidentialité des échanges entre le dispositif émetteur et le dispositif récepteur. Par ailleurs, à cet effet, seule la structure des

expressions régulières est fournie par le dispositif de sécurité au dispositif de détection d'intrusions, les signatures caractéristiques des intrusions n'étant livrées à ce dernier que sous forme chiffrée. L'utilisation d'un algorithme de chiffrement homomorphe telle que proposée par l'invention permet donc avantageusement à l'éditeur de sécurité de garder secrets à l'égard du dispositif de détection d'intrusions les signatures qu'il a établies pour la détection d'intrusions. L'approche proposée par l'invention est donc parfaitement compatible avec les modèles économiques existants des éditeurs de sécurité : aucune signature n'est fournie en clair par l'éditeur de sécurité au dispositif de détection d'intrusions.

En outre, les chiffrés des signatures caractéristiques des intrusions étant chiffrés au moyen de la clé publique du dispositif de sécurité, ils n'ont besoin d'être générés et transmis qu'une seule fois au dispositif de détection d'intrusions, par exemple lors d'une étape d'initialisation, du fait de leur indépendance vis-à-vis des dispositifs émetteurs et récepteurs. Ils peuvent ensuite être utilisés par le dispositif de détection d'intrusions pour gérer plusieurs connexions simultanées ou successives entre différents dispositifs émetteurs et récepteurs. Il en est de même de la description des expressions régulières. Il en résulte donc une mise en œuvre simplifiée de la détection DPI full IDS proposée par l'invention, et un gain substantiel en termes de complexité par rapport à la solution BlindBox qui requiert le chiffrement des mots-clés par le proxy IDS à chaque nouvelle connexion entre un dispositif émetteur et un dispositif récepteur.

L'invention offre de plus la possibilité de tenir compte facilement et rapidement d'une mise à jour des signatures et des expressions régulières par l'éditeur de sécurité, par exemple en raison de l'apparition de nouveaux types d'intrusions susceptibles d'affecter le réseau.

Dans un mode particulier de réalisation, le contenu dérivé du message est constitué du message destiné au dispositif récepteur ou d'une concaténation de ce message et d'un aléa connu du dispositif de sécurité et du dispositif de détection d'intrusions.

Par ailleurs, dans un mode de réalisation dans lequel le contenu dérivé du message est constitué d'une concaténation du message et d'un aléa connu du dispositif de sécurité et du dispositif de détection d'intrusions, la première étape d'évaluation peut fournir en outre un chiffré V' de l'aléa par la procédure de chiffrement de l'algorithme de chiffrement homomorphe paramétrée par la clé publique de chiffrement du dispositif de sécurité, le procédé de détection comprenant alors en outre une étape de transmission dudit chiffré V' de l'aléa au dispositif de sécurité pour vérification.

Cette vérification de l'aléa effectuée par le dispositif de sécurité force le dispositif émetteur à chiffrer correctement le message envoyé au dispositif récepteur et l'aléa sous peine d'être « démasqué ». Ce mode de réalisation rend ainsi possible l'application de l'invention non seulement dans un contexte où le dispositif émetteur et le dispositif récepteur sont honnêtes que dans un contexte où l'un au moins de ces dispositifs est « malhonnête », c'est-à-dire qu'il peut être à l'origine de l'intrusion perpétrée sur le réseau (volontairement ou involontairement) ou collaborer avec l'entité à l'origine de cette intrusion. Cela correspond par exemple à un cas où un dispositif

émetteur, dont le contrôle a été pris par un attaquant transmet des données sensibles qui sont reçues et attendues par le dispositif récepteur. Un tel contexte a une importance primordiale dès lors qu'on constate aujourd'hui que la plupart des attaques proviennent des systèmes d'information eux-mêmes, via des logiciels malveillants qui prennent le contrôle des terminaux des systèmes d'information. Par conséquent, le dispositif émetteur comme le dispositif récepteur peuvent être assez facilement corrompus par une entité distante malveillante qui peut en prendre le contrôle de manière totale ou partielle (par exemple, un terminal victime infecté peut faire fuiter des données sensibles vers son logiciel maître via une telle prise de contrôle). On se limitera toutefois ici au cas où, lorsque les deux dispositifs sont « malhonnêtes » indépendamment l'un de l'autre, c'est-à-dire qu'aucune entente préalable n'a été conclue entre eux (par exemple pour transmettre des données sensibles d'une manière spécifique en découpant et en transmettant ces données d'une façon telle que le procédé serait inefficace pour détecter la façon dont la fuite de données a été opérée). Au contraire, l'approche proposée dans le document de J. Sherry et al. ne permet pas de gérer une situation dans laquelle les dispositifs émetteur et récepteur sont tous les deux malhonnêtes indépendamment l'un de l'autre.

Conformément à l'invention, l'évaluation de l'algorithme de déchiffrement symétrique via la fonction d'évaluation homomorphe requiert la fourniture à cette fonction d'évaluation d'un chiffré (i.e. le chiffré T'), mais également d'un chiffré S de la clé de chiffrement secrète utilisée lors du chiffrement symétrique, généré en utilisant la procédure de chiffrement de l'algorithme de chiffrement homomorphe paramétrée par la clé de chiffrement publique du dispositif de sécurité.

Dans un mode particulier de réalisation, le chiffré S de la clé de chiffrement secrète est obtenu du dispositif émetteur.

Ce mode de réalisation est particulièrement simple à mettre en œuvre, le dispositif émetteur disposant de la clé secrète.

Toutefois, dans ce mode de réalisation, la clé secrète étant chiffrée au moyen de la clé de chiffrement publique du dispositif de sécurité, rien n'empêche à un dispositif de sécurité un peu trop curieux d'accéder à la clé secrète et de déchiffrer au moyen de cette clé le message chiffré échangé entre le dispositif émetteur et le dispositif récepteur.

Pour pallier à cette éventualité, dans un mode particulier de réalisation, l'étape d'obtention du chiffré S de la clé de chiffrement secrète comprend :

- une étape de réception, en provenance du dispositif émetteur, d'un chiffré dit intermédiaire S' de la clé de chiffrement secrète obtenu en utilisant la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé de chiffrement publique du dispositif récepteur ;
- une étape d'obtention d'une clé de rechiffrement du dispositif récepteur vers le dispositif de sécurité ; et
- une étape de rechiffrement du chiffré intermédiaire S' en utilisant ladite clé de rechiffrement, cette étape de rechiffrement fournissant ledit chiffré S de la clé de chiffrement secrète.

Autrement dit, on se prémunit dans ce mode de réalisation contre un dispositif de sécurité trop curieux en combinant à l'algorithme de chiffrement homomorphe utilisé dans l'invention un schéma de rechiffrement (ou « proxy reencryption » en anglais). De façon connue, un tel schéma de rechiffrement permet de donner accès à un tiers B à des données chiffrées par exemple au moyen d'un algorithme de chiffrement à clé publique utilisant la clé publique d'une entité A, et ce sans que l'entité A n'ait à divulguer sa clé privée de chiffrement et même si les données n'étaient pas initialement destinées au tiers. A cet effet, le schéma de rechiffrement s'appuie sur une clé dite de rechiffrement ou de transition à l'attention du tiers B donnant un droit d'accès au tiers B aux données chiffrées avec la clé publique de l'entité A. Cette clé est utilisée pour rechiffrer les données chiffrées de l'entité A de sorte à les rendre accessibles au tiers B en utilisant sa propre clé privée de déchiffrement.

Ainsi, dans ce mode de réalisation « combiné », la clé secrète utilisée par l'algorithme de chiffrement symétrique n'est plus chiffrée en utilisant la clé publique de chiffrement du dispositif de sécurité mais en utilisant une clé publique de chiffrement du dispositif récepteur, qui est le seul à détenir la clé privée de déchiffrement associée. Pour permettre au dispositif de sécurité d'effectuer les tâches qui lui incombent (ex. déchiffrement du chiffré du résultat de détection, vérification de l'aléa, etc.) en dépit du fait qu'il ne connaît pas la clé privée de déchiffrement du dispositif récepteur, le dispositif de détection d'intrusions utilise une clé de rechiffrement du dispositif récepteur vers le dispositif de sécurité pour rechiffrer le chiffré S' de la clé secrète transmis par le dispositif émetteur. Ceci permet au dispositif de détection d'intrusions d'obtenir un chiffré S de la clé de chiffrement secrète correspondant à la clé publique de chiffrement du dispositif de sécurité qu'il peut alors utiliser lors de l'évaluation de l'algorithme de déchiffrement symétrique. Grâce à ce rechiffrement, le dispositif de sécurité est en mesure de déchiffrer les éléments qui lui sont envoyés par le dispositif de détection d'intrusions dans un mode interactif.

Selon un autre aspect, l'invention vise un procédé de communication d'un dispositif de sécurité avec un dispositif de détection d'intrusions sur un réseau, le dispositif de sécurité ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter le réseau, ladite au moins une règle de détection comprenant une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion, le procédé de communication comprenant :

- une étape de transformation de ladite au moins une expression régulière en une fonction décrivant ladite au moins une expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation d'un algorithme de chiffrement homomorphe ;
- une étape de génération d'un chiffré de chaque signature caractéristique de ladite au moins une intrusion en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ; et

- une étape de transmission de ladite au moins une fonction décrivant ladite au moins une expression régulière et de chaque chiffré de chaque signature caractéristique de ladite au moins une intrusion à un dispositif de détection d'intrusions sur le réseau.

Corrélativement, l'invention vise également un dispositif de sécurité ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter un réseau, ladite au moins une règle de détection comprenant une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion, le dispositif de sécurité comprenant :

- un module de transformation, configuré pour transformer ladite au moins une expression régulière en une fonction décrivant ladite au moins une expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation d'un algorithme de chiffrement homomorphe ;
- un module de chiffrement, configuré pour générer un chiffré de chaque signature caractéristique de ladite au moins une intrusion en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ; et
- un module de transmission, configuré pour transmettre ladite au moins une fonction décrivant ladite au moins une expression régulière et chaque chiffré de chaque signature caractéristique de ladite au moins une intrusion à un dispositif de détection d'intrusions sur le réseau.

Dans un mode particulier de réalisation dit interactif, le procédé de communication comprend en outre :

- une étape de réception en provenance du dispositif de détection d'un chiffré d'un résultat de détection ;
- une étape de déchiffrement du chiffré du résultat de détection en utilisant une procédure de déchiffrement de l'algorithme de chiffrement homomorphe paramétrée par une clé privée de déchiffrement associée à la clé publique de chiffrement du dispositif de sécurité ; et
- une étape de transmission du résultat de détection déchiffré au dispositif de détection d'intrusions.

Corrélativement, le dispositif de sécurité comprend en outre :

- un module de réception, apte à recevoir en provenance du dispositif de détection un chiffré d'un résultat de détection ;
- un module de déchiffrement, configuré pour déchiffrer ledit chiffré du résultat de détection en utilisant une procédure de déchiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé privée de déchiffrement associée à la clé publique de chiffrement du dispositif de sécurité ; et
- un module de transmission, configuré pour transmettre le résultat de détection déchiffré au dispositif de détection d'intrusions.

Le procédé de communication et le dispositif de sécurité dans ces différents modes de réalisation bénéficient des mêmes avantages que ceux cités précédemment pour le procédé et le dispositif de détection d'intrusions selon l'invention.

On note que conformément à l'invention, le dispositif de sécurité fournit au dispositif de détection d'intrusions différents éléments lui permettant de réaliser une détection DPI full IDS, sans ne jamais lui livrer les signatures caractéristiques des intrusions qu'il a établies. Celles-ci sont avantageusement gardées secrètes par le dispositif de sécurité à l'égard du dispositif de détection d'intrusions qui n'a accès qu'à la structure en définitive des expressions régulières et aux chiffrés des signatures.

Dans un mode particulier de réalisation, lors de l'étape de transformation du procédé de communication, au moins une fonction décrivant ladite au moins une expression régulière est un circuit arithmétique obtenu au moyen d'un automate à nombre fini d'états non déterministe modélisant l'expression régulière et d'une fonction de sélection des états de cet automate.

Ce mode de réalisation fournit un moyen simple et efficace pour générer une description des expressions régulières proposées par le dispositif de sécurité pouvant être évaluées par la fonction d'évaluation homomorphe de l'algorithme de chiffrement homomorphe.

Dans un mode particulier de réalisation, les différentes étapes du procédé de détection d'intrusions et/ou les différentes étapes du procédé de communication sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un dispositif de sécurité ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de communication tel que décrit ci-dessus.

L'invention vise également un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un dispositif de détection d'intrusions ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de détection d'intrusions tel que décrit ci-dessus.

Chacun de ces programmes peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations ou d'enregistrement lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations ou d'enregistrement peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations ou d'enregistrement peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique

ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations ou d'enregistrement peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être
5 utilisé dans l'exécution du procédé en question.

Selon un autre aspect encore, l'invention vise un système de détection d'intrusions sur un réseau via lequel sont aptes à communiquer un dispositif émetteur et un dispositif récepteur en utilisant un algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre le dispositif émetteur et le dispositif récepteur, ce système de
10 détection d'intrusions comprenant :

- un dispositif de détection d'intrusions conforme à l'invention ; et
- un dispositif de sécurité conforme à l'invention.

L'invention concerne aussi un système de communications comprenant :

- au moins un dispositif émetteur et au moins un dispositif récepteur aptes à communiquer sur
15 un réseau en utilisant un algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre le dispositif émetteur et le dispositif récepteur ; et
- un système de détection d'intrusions selon l'invention, le dispositif de détection d'intrusions dudit système de détection étant destiné à être localisé entre ledit au moins un dispositif
20 émetteur et ledit au moins un dispositif récepteur.

Les systèmes de détection d'intrusions et de communication bénéficient des mêmes avantages que ceux cités précédemment pour le procédé et le dispositif de détection d'intrusions selon l'invention et pour le procédé de communication et le dispositif de sécurité selon l'invention.

On peut également envisager, dans d'autres modes de réalisation, que le procédé de
25 détection d'intrusions, le procédé de communication, le dispositif de détection d'intrusions, le dispositif de sécurité, le système de détection d'intrusions, et le système de communication selon l'invention présentent en combinaison tout ou partie des caractéristiques précitées.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

- la figure 1 représente, de façon schématique, un système de communications selon l'invention, dans un premier mode de réalisation de l'invention ;
- 35 — la figure 2 illustre l'architecture matérielle d'un dispositif de détection d'intrusions selon l'invention, appartenant au système de communications de la figure 1 ;
- la figure 3 illustre l'architecture matérielle d'un dispositif de sécurité selon l'invention, appartenant au système de communications de la figure 1 ;

- les figures 4, 5 et 7 représentent respectivement, sous forme d'ordinogramme, les principales étapes d'un procédé de communication selon l'invention, d'un procédé de détection d'intrusions selon l'invention et d'un procédé d'émission d'un message telles qu'elles sont mises en œuvre dans le premier mode de réalisation de l'invention par le dispositif de sécurité, par le
5 dispositif de détection d'intrusions, et par un dispositif émetteur du système de communications de la figure 1 ;
- la figure 6 représente à titre illustratif un automate à nombre d'états finis pouvant être utilisé par le dispositif de sécurité au cours du procédé illustré à la figure 4 ; et
- les figures 8 et 9 représentent respectivement, sous forme d'ordinogramme, les principales
10 étapes d'un procédé de détection d'intrusions selon l'invention et d'un procédé d'émission d'un message telles qu'elles sont mises en œuvre dans un second mode de réalisation de l'invention par le dispositif de détection d'intrusions et par un dispositif émetteur du système de communications selon l'invention.

15 Description détaillée de l'invention

La **figure 1** représente, dans son environnement, un système 1 de communications conforme à l'invention, dans un premier mode de réalisation.

Le système 1 de communications comprend :

- un dispositif émetteur TX 2 ;
- 20 — un dispositif récepteur RX 3 ; et
- un système 4 de détection d'intrusions conforme à l'invention.

Le dispositif émetteur TX 2 et le dispositif récepteur RX 3 sont aptes à communiquer l'un avec l'autre via un réseau de télécommunications NW. Aucune limitation n'est attachée à la nature de ce réseau, hormis le fait que sur ce réseau, les communications entre le dispositif
25 émetteur TX 2 et le dispositif récepteur RX 3 sont sécurisées via l'utilisation d'un algorithme cryptographique de chiffrement/déchiffrement symétrique noté ALG-SYM s'appuyant sur une clé de chiffrement secrète K partagée entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3. On note ici SYM-ENC, respectivement SYM-DEC, la procédure (ou algorithme) de chiffrement, respectivement de déchiffrement, symétrique correspondante. L'algorithme de
30 chiffrement/déchiffrement symétrique ALG-SYM est par exemple identique à l'algorithme de chiffrement/déchiffrement symétrique utilisé par les protocoles sécurisés TLS ou SSL.

Le réseau NW peut ainsi être indifféremment un réseau public tel que le réseau Internet ou un réseau privé, un réseau fixe ou mobile, un réseau filaire ou sans fil, il peut être constitué d'un unique réseau ou être composé d'une pluralité de sous-réseaux, etc.

35 Le système 4 de détection d'intrusions est configuré pour permettre la détection d'intrusions susceptibles d'affecter les communications sur le réseau NW, et plus particulièrement ici dans l'exemple envisagé à la figure 1, les communications entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3. A cet effet, il comprend :

- un dispositif de détection d'intrusions MB 5 (aussi désigné par « middlebox »), conforme à l'invention, qui se trouve dans le réseau NW entre chaque dispositif émetteur TX susceptible d'émettre des données sur ce réseau et chaque dispositif récepteur RX susceptible de recevoir des données via ce réseau. En l'espèce ici, dans l'exemple illustré à la figure 1, le dispositif MB 5 de détection d'intrusions se trouve localisé dans le réseau NW entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 et est susceptible d'intercepter les échanges sur le réseau NW entre ces deux dispositifs ; et
 - un dispositif de sécurité RG 6, géré par (i.e. sous le contrôle de) un éditeur de sécurité apte à déterminer (c'est-à-dire à établir) une pluralité de règles de détection d'intrusions susceptibles d'affecter le réseau NW. Ces règles de détection se présentent sous la forme de signatures (ou patterns ou encore mots-clés) SIG_i, $i=1,...,I$ où I désignant un entier supérieur à 1, caractéristiques des intrusions susceptibles d'affecter le réseau NW, ainsi que d'une ou plusieurs expressions régulières REG_j, $j=1,...,J$, J désignant un entier supérieur ou égal à 1, établies à partir de ces signatures. Une expression régulière, de façon connue en informatique, est une chaîne de caractères ou un motif qui définit un ensemble de chaînes de caractères possibles. Autrement dit, dans le contexte décrit ici, chaque expression régulière REG_j définit un ensemble de chaînes de caractères possibles à partir d'une ou de plusieurs signatures. Elle peut s'appuyer à cet effet sur différents opérateurs connus en soi dont notamment :
 - l'opérateur de groupement « () » qui indique les caractères pouvant être encadrés de part et d'autre par les caractères se trouvant avant et après l'opérateur ; par exemple « Blind(B|b)ox » comprend « BlindBox » et « Blindbox » ;
 - l'astérisque *, indiquant pour la chaîne de caractères dans laquelle il est utilisé, zéro ou au moins une occurrence du caractère ou d'un ensemble de caractères précédant l'astérisque et délimité par l'opérateur de groupement (). Par exemple « ab* » comprend les chaînes de caractères « a », « ab », « abb », etc.
 - l'opérateur « ou » ou « | » qui traduit des caractères alternatifs ou des chaînes de caractères alternatives de part et d'autre de l'opérateur. Par exemple « rootkit|trojan » désigne les chaînes de caractères « rootkit » ou « trojan » ;
 - le point d'interrogation « ? » qui indique zéro ou une occurrence d'un caractère ou d'un ensemble de caractères délimité par l'opérateur de groupement () ; par exemple « https ? » comprend « http » ou « https » ; et
 - l'opérateur « + » qui indice une ou plusieurs occurrences d'un caractère ou d'un ensemble de caractères délimité par l'opérateur de groupement () ; par exemple, « /content/p+ » comprend « /content/p », « /content/pp », « /content/ppp », etc.
- Ainsi, à titre illustratif, l'expression régulière « p(a|b)* » comprend les chaînes de caractères qui contiennent le caractère p suivi d'un nombre arbitraire (i.e. zéro ou plus) de « a » ou de « b ». Elle comprend donc les chaînes de caractères « p », « pa », « pb », « paaaabb », « pbbba », etc.

Dans le premier mode de réalisation décrit ici, les signatures SIG_i , $i=1,\dots,I$ et les expressions régulières REG_j , $j=1,\dots,J$ établies par l'éditeur de sécurité sont stockées dans une mémoire non volatile référencée par 15 (cf. figure 3) du dispositif de sécurité RG 6 (et donc accessible par celui-ci).

5 En variante, les signatures SIG et les expressions régulières REG établies par l'éditeur de sécurité peuvent être stockées dans une mémoire distante, préférentiellement protégée de façon connue en soi, et accessible par le dispositif de sécurité RG 6.

La façon dont sont déterminées par l'éditeur de sécurité les règles de détection, et plus particulièrement les signatures SIG et les expressions régulières REG, est connue en soi et dépend
10 du savoir-faire de chaque éditeur de sécurité. Elle n'est pas décrite en détail ici. On note que les signatures SIG et les expressions régulières REG associées à ces signatures sont susceptibles d'évoluer ou d'être mis à jour, par exemple suite à l'apparition de nouveaux types d'intrusions susceptibles d'affecter le réseau NW.

En outre, il convient également de noter qu'un même éditeur de sécurité peut être
15 amené à interagir avec plusieurs dispositifs de détection d'intrusions distincts, situés dans le même réseau ou dans des réseaux différents. De façon similaire, un dispositif de détection d'intrusions localisé dans un réseau peut être amené à interagir avec plusieurs éditeurs de sécurité (et donc avec plusieurs dispositifs de sécurité gérés respectivement par ces éditeurs de sécurité). Par souci de simplification toutefois ici, on se limite à un éditeur de sécurité et à un dispositif de détection
20 d'intrusions.

Conformément à l'invention, une inspection en profondeur de type DPI et full IDS est permise sur le réseau NW bien que les communications entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 soient chiffrées, et ce, sans que l'éditeur de sécurité ne soit contraint de divulguer au dispositif de détection d'intrusions MB 5 les signatures qu'il a établies pour détecter
25 des intrusions susceptibles d'affecter le réseau NW. En outre, cette inspection DPI full IDS est permise sans que le trafic échangé entre le dispositif émetteur TX et le dispositif récepteur RX ne soit divulgué au dispositif de détection d'intrusions MB 5, même partiellement, de sorte que la confidentialité de l'échange entre les deux dispositifs est préservée et leur vie privée garantie. A cet effet, l'invention s'appuie sur un algorithme de chiffrement homomorphe noté ci-après ALG-FHE
30 (pour Fully Homomorphic Encryption en anglais).

Aucune limitation n'est attachée à l'algorithme de chiffrement homomorphe en soi qui peut être utilisé : il peut s'agir par exemple de l'algorithme de chiffrement homomorphe décrit dans le document de C. Gentry intitulé « Fully homomorphic encryption using ideal lattices », Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda,
35 MD, USA, 31 mai – 2 juin 2009, ou d'un algorithme décrit dans le document de J. Fan et al. intitulé « Somewhat practical fully homomorphic encryption », IACR Cryptology ePrint Archive 2012 : 144, etc.

De façon connue, un tel algorithme de chiffrement homomorphe est défini par plusieurs procédures, à savoir :

- un algorithme de génération de clés noté FHE.KEYGEN, paramétré par un paramètre de sécurité λ connu en soi, pris par exemple ici égal à 128 bits, conformément aux recommandations de sécurité en vigueur. Cet algorithme est apte à générer une paire de clés cryptographiques comprenant une clé de chiffrement publique notée de façon générale pk et une clé de déchiffrement privée notée sk correspondante ;
- un algorithme de chiffrement/déchiffrement comprenant une procédure de chiffrement FHE.ENC apte à générer un chiffré à partir d'un message et de la clé de chiffrement publique pk , et une procédure de déchiffrement FHE.DEC apte à déchiffrer un chiffré à partir de la clé de déchiffrement privée sk correspondante ;
- une fonction d'évaluation homomorphe FHE.HOM, qui prend en entrée plusieurs chiffrés $c_1, \dots, c_L$ et une fonction f qui se présente sous une forme qui peut être évaluée par la fonction d'évaluation homomorphe (par exemple sous la forme d'un circuit arithmétique, comme détaillé davantage ultérieurement), ladite fonction d'évaluation homomorphe délivrant alors en sortie $f(c_1, \dots, c_L)$. Comme mentionné précédemment, si $c_l, l=1, \dots, L$ désigne le chiffré d'un message m_l obtenu au moyen de l'algorithme de chiffrement ENC paramétré par la clé de chiffrement publique pk , par abus de notation, on peut écrire que la fonction d'évaluation homomorphe HOM vérifie la relation suivante :

$$\text{FHE.HOM}(c_1, \dots, c_L; f) = f(c_1, \dots, c_L) = \text{FHE.ENC}(f(m_1, \dots, m_L), pk)$$

L'abus de notation vient du fait que ce n'est pas exactement la même fonction f qui est en réalité appliquée sur les messages en clair $m_1, \dots, m_L$ et sur les messages chiffrés $c_1, \dots, c_L$. En effet, de façon connue en soi, la fonction d'évaluation homomorphe impose certaines contraintes sur la forme de la fonction f pour pouvoir l'évaluer sur les chiffrés $c_1, \dots, c_L$, contraintes qui ne sont pas nécessaires pour appliquer cette fonction aux messages en clair.

Au sens strict du terme, on a donc deux fonctions f et f' appliquées respectivement sur les chiffrés et sur les messages en clair. Toutefois, par souci de simplification dans la suite de la description, et pour faciliter la compréhension de l'invention, on considère une unique notation f pour désigner cette fonction et on entend par évaluation d'une fonction f par la fonction d'évaluation homomorphe, l'évaluation de la fonction f dans sa forme transformée. Ainsi, à titre d'exemple, et par abus de langage, on entend par évaluation de la procédure de déchiffrement, l'évaluation de cette procédure de déchiffrement sous une forme éventuellement transformée et évaluable par la fonction d'évaluation homomorphe.

Les différentes procédures définissant l'algorithme de chiffrement homomorphe ALG-FHE sont mises en œuvre en tout ou partie, dans le premier mode de réalisation décrit ici, par les différentes entités du système de communication 1 (dispositif émetteur TX 2, dispositif de détection d'intrusions MB 5 et dispositif de sécurité RG 6), comme détaillé davantage ultérieurement.

Dans le premier mode de réalisation décrit ici, le dispositif de détection d'intrusions MB 5 a l'architecture d'un ordinateur, telle qu'illustrée à la **figure 2**. Il comprend notamment un processeur 7, une mémoire vive 8, une mémoire morte 9, une mémoire flash non volatile 10 ainsi que des moyens de communication 11 lui permettant d'une part, d'intercepter toute communication entre les dispositifs émetteur TX 2 et récepteur RX 3 sur le réseau NW, et d'autre part de communiquer avec le dispositif de sécurité RG 6. De tels moyens sont connus en soi et ne sont pas décrits plus en détail ici.

La mémoire morte 9 du dispositif de détection d'intrusions MB 5 constitue un support d'enregistrement conforme à l'invention, lisible par le processeur 7 et sur lequel est enregistré ici un programme d'ordinateur PROG1 conforme à l'invention.

Le programme d'ordinateur PROG1 définit des modules fonctionnels et logiciels ici, configurés pour mettre en œuvre les étapes d'un procédé de détection d'intrusions sur le réseau NW. Ces modules fonctionnels s'appuient sur et/ou commandent les éléments matériels 7-11 du dispositif de détection d'intrusions MB 5 cités précédemment. Ils comprennent notamment ici, comme illustré sur la figure 1 :

- un premier module de réception 5A apte à recevoir en provenance du dispositif de sécurité RG 6 différents éléments, et notamment :
 - une fonction CIRC-REG_j décrivant chaque expression régulière REG_j, $j=1,...,J$ et pouvant être évaluée au moyen de la fonction d'évaluation homomorphe FHE.HOM de l'algorithme de chiffrement homomorphe ALG-FHE. Une telle fonction est ici un circuit arithmétique (ou circuit booléen), connu en soi. La façon dont ce circuit arithmétique est obtenu à partir de l'expression régulière REG_j, $j=1,...,J$ par le dispositif de sécurité RG 6 est décrite ultérieurement ; et
 - un chiffré FHE-SIG_i, $i=1,...,I$ de chaque signature SIG_i, $i=1,...,I$, obtenu ici par le dispositif de sécurité RG 6 en appliquant la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE paramétrée par une clé publique pk(RG) de chiffrement du dispositif de sécurité RG 6 générée au moyen de l'algorithme FHE.KEYGEN.

Le premier module de réception 5A est configuré pour utiliser notamment les moyens de communication 11 du dispositif de détection d'intrusions MB 5 ;

- un second module de réception 5B, apte à recevoir en provenance du dispositif émetteur TX 2 un chiffré noté T d'un contenu dérivé d'un message m destiné au dispositif récepteur RX 3. Le chiffré T est généré par le dispositif émetteur TX 2 au moyen de la procédure de chiffrement SYM-ENC de l'algorithme de chiffrement/déchiffrement symétrique ALG-SYM, paramétrée par la clé de chiffrement secrète K partagée entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3. Le second module de réception 5B est également configuré pour utiliser les moyens de communication 11 du dispositif de détection d'intrusions MB 5.

En outre, dans le premier mode de réalisation décrit ici, le second module de réception 5B est configuré pour recevoir un chiffré S de la clé de chiffrement secrète K générée par le dispositif émetteur TX 2 en appliquant sur la clé secrète K la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE, paramétrée par la clé de chiffrement publique pk(RG) du dispositif de sécurité RG 6 (autrement dit, le module de réception 5B est dans le premier mode de réalisation un module d'obtention d'un chiffré S de la clé de chiffrement secrète K au sens de l'invention) ;

- un module d'obtention 5C d'un chiffré T' du chiffré T. Le chiffré T' résulte de l'application par le module d'obtention 5C sur le chiffré T de la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE paramétrée par la clé de chiffrement publique pk(RG) du dispositif de sécurité RG 6.

Dans un second mode de réalisation, décrit plus en détail ultérieurement, le module d'obtention 5C est en outre configuré pour obtenir un chiffré S de la clé de chiffrement secrète K, ce chiffré correspondant à l'application de l'algorithme de chiffement homomorphe ALG-FHE paramétrée par la clé de chiffement publique pk(RG) du dispositif de sécurité RG 6. On note que dans ce second mode de réalisation, le chiffré S est obtenu par le module d'obtention 5C par rechiffement d'un chiffré intermédiaire S' de la clé de chiffement secrète K fourni au dispositif de détection d'intrusions MB 5 par le dispositif émetteur TX 2. Le chiffré S' résulte de l'application sur la clé secrète K de l'algorithme de chiffement homomorphe ALG-FHE paramétrée par une clé de chiffement publique pk(RX) du dispositif récepteur RX 3, de sorte que le dispositif de détection d'intrusions MB 5 n'est jamais en possession de la clé secrète partagée K. Le module d'obtention 5C est alors configuré, dans le second mode de réalisation, pour utiliser une clé de rechiffement du dispositif récepteur RX 3 vers le dispositif de sécurité RG 6 pour générer le chiffré S ;

- un premier module d'évaluation 5D de la procédure de déchiffement symétrique SYM-DEC de l'algorithme de chiffement symétrique ALG-SYM. Le premier module d'évaluation est configuré pour réaliser cette évaluation sur le chiffré T et pour utiliser à cet effet la fonction d'évaluation homomorphe FHE.HOM de l'algorithme de chiffement homomorphe ALG-FHE et le chiffré S de la clé secrète K. Le premier module d'évaluation 5D est en outre configuré pour fournir un chiffré V du message m par la procédure de chiffement FHE.ENC paramétrée par la clé publique de chiffement pk(RG) du dispositif de sécurité RG 6 ;
- un second module d'évaluation 5E configuré pour évaluer en utilisant la fonction d'évaluation FHE.HOM ainsi que les chiffrés FHE-SIG_i, $i=1, \dots, I$ des signatures SIG_i, chaque fonction CIRC-REG_j décrivant une expression régulière REG_j, $j=1, \dots, J$, sur le chiffré V du message m. Ce second module d'évaluation 5E est en outre configuré pour fournir un chiffré d'un résultat de détection indiquant l'existence ou non d'une expression régulière parmi les expressions REG_j, $j=1, \dots, J$ correspondant au message m ; et

- un module de détection 5F d'une intrusion sur le réseau activé si le résultat de détection une fois déchiffré indique qu'il existe au moins une expression régulière REG_j , $j = 1, \dots, J$ correspondant au message m .

Les fonctions de ces différents modules 5A-5F sont décrites plus en détail ultérieurement.

Le dispositif de sécurité RG 6 a également ici l'architecture matérielle d'un ordinateur, telle qu'illustrée à la **figure 3**. Il comprend notamment un processeur 12, une mémoire vive 13, une mémoire morte 14, la mémoire flash non volatile 15 dans laquelle sont stockées les signatures SIG_i , $i = 1, \dots, I$, les chiffrés $FHE-SIG_i$, $i = 1, \dots, I$ ainsi que les expressions régulières REG_j , $j = 1, \dots, J$ et les circuits arithmétiques $CIRC-REG_j$, $j = 1, \dots, J$ décrivant ces expressions régulières. Le dispositif de sécurité RG 6 comprend également des moyens de communication 16 lui permettant de communiquer avec le dispositif de détection d'intrusions MB 5.

La mémoire morte du dispositif de sécurité RG 6 constitue un support d'enregistrement, lisible par le processeur du dispositif de sécurité et sur lequel est enregistré ici un programme d'ordinateur PROG2 définissant des modules fonctionnels, configurés pour mettre en œuvre les étapes d'un procédé de communication selon l'invention. Ces modules fonctionnels s'appuient sur et/ou commandent les éléments matériels 12-16 du dispositif de sécurité RG 6 cités précédemment. Ils comprennent notamment dans le premier mode de réalisation décrit ici, comme illustré sur la figure 1 :

- un module de génération de clés 6A, configuré pour utiliser l'algorithme de génération de clés FHE.KEYGEN de l'algorithme de chiffrement homomorphe ALG-FHE afin de générer la paire de clés du dispositif de sécurité RG 6 comprenant la clé publique de chiffrement $pk(RG)$ et la clé privée de déchiffrement $sk(RG)$ correspondante ;
- un module de transformation 6B, configuré pour transformer chaque expression régulière REG_j , $j = 1, \dots, J$ en une fonction décrivant cette expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation d'un algorithme de chiffrement homomorphe. Dans le premier mode de réalisation décrit ici, comme évoqué précédemment, le module de transformation 6B est configuré pour transformer chaque expression régulière REG_j en un circuit arithmétique $CIRC-REG_j$;
- un module de chiffrement 6C, configuré pour générer les chiffrés $FHE-SIG_i$, $i = 1, \dots, I$ à partir des signatures SIG_i , $i = 1, \dots, I$ en utilisant la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE paramétrée par la clé publique $pk(RG)$ de chiffrement du dispositif de sécurité RG 6 ; et
- un module de transmission 6D, configuré pour transmettre chacune des fonctions (circuits arithmétiques ici) $CIRC-REG_j$, $j = 1, \dots, J$ décrivant chaque expression régulière REG_j , $j = 1, \dots, J$ et chaque chiffré $FHE-SIG_i$, $i = 1, \dots, I$ de chaque signature SIG_i , $i = 1, \dots, I$ au dispositif de détection d'intrusions MB 5. Ce module de transmission 6D s'appuie sur les moyens de communication 16 du dispositif de sécurité RG 6.

Dans le premier mode de réalisation décrit ici, le programme d'ordinateur PROG2 définit également les modules fonctionnels et logiciels suivants :

- un module de réception 6E, s'appuyant aussi sur les moyens de communication 16, et apte à recevoir en provenance du dispositif de détection d'intrusions MB 5 un chiffré du résultat de détection généré par le module de détection d'intrusions MB 5 ; et
- un module de déchiffrement 6F, configuré pour déchiffrer ce chiffré du résultat de détection en utilisant la procédure de déchiffrement FHE.DEC de l'algorithme de chiffrement homomorphe ALG-FHE, paramétrée par la clé privée $sk(RG)$ du dispositif de sécurité RG 6.

En outre, le module de transmission 6D est configuré pour transmettre le résultat de détection déchiffré par le module 6F au dispositif de détection d'intrusions MB 5.

Les fonctions de ces différents modules 6A-6F sont décrites plus en détail ultérieurement.

En variante, la paire de clés $pk(RG)/sk(RG)$ associée au dispositif de sécurité RG 6 peut être générée par une autorité de confiance, qui se charge ensuite de publier la clé publique $pk(RG)$ et de transmettre la clé privée $sk(RG)$ de manière sécurisée au dispositif de sécurité RG 6.

On note qu'aucune limitation n'est attachée à la nature des dispositifs émetteur TX 2 et récepteur RX 3. Il peut s'agir d'ordinateurs, de serveurs, de terminaux quelconques, dès lors que ceux-ci sont aptes à communiquer sur le réseau NW de façon sécurisée en utilisant ici la procédure de chiffrement/déchiffrement de l'algorithme de chiffrement symétrique ALG-SYM et pour le dispositif émetteur TX 2, la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE. On suppose ici que les dispositifs TX 2 et RX 3 sont en mesure d'échanger ou de partager la clé secrète de chiffrement K.

Dans le premier mode de réalisation décrit ici, les dispositifs émetteur TX 2 et récepteur RX ont l'architecture matérielle d'un ordinateur, cette architecture étant identique à celle du dispositif de détection d'intrusions MB 5 ou à celle du dispositif de sécurité RB 6, à savoir qu'ils comprennent un processeur, une mémoire vive, une mémoire morte, la mémoire flash non volatile, ainsi que des moyens de communication leur permettant de communiquer sur le réseau NW.

La mémoire morte du dispositif émetteur TX 2 constitue un support d'enregistrement, lisible par le processeur du dispositif émetteur TX 2 et sur lequel est enregistré ici un programme d'ordinateur définissant des modules fonctionnels s'appuyant sur et/ou commandent les éléments matériels du dispositif émetteur TX 2 cités précédemment. Ces modules fonctionnels comprennent notamment ici, comme illustré sur la figure 1 :

- un module 2A de génération d'un chiffré à partir d'un contenu dérivé d'un message m destiné au dispositif récepteur RX 3 en utilisant la procédure de chiffrement SYM-ENC de l'algorithme de chiffrement symétrique ALG-SYM, paramétrée par la clé de chiffrement secrète K ;
- un module 2B de génération d'un chiffré de la clé de chiffrement secrète K, configuré pour utiliser à cet effet la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE ; et

— un module 2C d'émission, configuré pour émettre les deux chiffrés générés par le module 2A et par le module 2B sur le réseau NW.

Par ailleurs, la mémoire morte du dispositif récepteur RX 3 constitue un support d'enregistrement, lisible par le processeur du dispositif récepteur RX 3 et sur lequel est enregistré
 5 ici un programme d'ordinateur définissant des modules fonctionnels s'appuyant sur et/ou commandent les éléments matériels du dispositif récepteur RX 3 cités précédemment, et notamment un module de déchiffrement 3A configuré pour appliquer la procédure de déchiffrement SYM-DEC de l'algorithme de chiffrement/déchiffrement symétrique ALG-SYM paramétrée par la clé secrète K partagée avec le dispositif émetteur TX 2.

10 Les fonctions des différents modules 2A-2C et 3A des dispositifs émetteur TX 2 et récepteur RX 3 sont décrites plus en détail ultérieurement.

Dans le premier mode de réalisation décrit ici, on suppose que le dispositif 2 est l'émetteur d'un message m et le dispositif 3 le destinataire de ce message. Bien entendu, ces rôles sont interchangeable, et le dispositif 2 peut être muni d'un module identique au module 3A du
 15 dispositif 3 pour recevoir et déchiffrer un message chiffré via le réseau NW, de même que le dispositif 3 peut être muni de modules identiques aux modules 2A-2C du dispositif 2 pour émettre des messages chiffrés sur le réseau NW.

Nous allons maintenant décrire, en référence aux **figures 4 et 5** respectivement, les principales étapes d'un procédé de communication et d'un procédé de détection d'intrusions selon
 20 l'invention tel qu'ils sont mis en œuvre respectivement par le dispositif de sécurité RG 6 et par le dispositif de détection d'intrusions MB 5 du système de communication 1 de la figure 1.

En référence à la figure 4, on suppose ici, que durant une phase d'initialisation, le dispositif de sécurité RG 6 génère, via son module de génération de clés 6A, une paire de clés cryptographiques comprenant sa clé publique $pk(RG)$ et sa clé privée $sk(RG)$ (étape E10). A cet
 25 effet, il utilise, comme mentionné précédemment, l'algorithme FHE.KEYGEN de l'algorithme de chiffrement homomorphe ALG-FHE, paramétré par le paramètre de sécurité λ avec $\lambda=128$ bits ici.

La clé publique $pk(RG)$ du dispositif de sécurité RG 6 est publiée (i.e. rendue publique) sur le réseau NW, de sorte à être connue notamment du dispositif de détection d'intrusions RG 6 et du dispositif émetteur TX 2 (étape E20).

30 Le dispositif de sécurité RG 6 transforme ensuite, via son module de transformation 6B, chaque expression régulière REG_j , $j=1,...,J$ portant sur une ou plusieurs signatures SIG_i , $i=1,...,I$, en une fonction décrivant cette expression et pouvant être évaluée par une fonction d'évaluation homomorphe et notamment par la fonction d'évaluation homomorphe FHE.HOM de l'algorithme de chiffrement homomorphe ALG-FHE (étape E30). Dans le premier mode de
 35 réalisation décrit ici, la transformation opérée par le module 6B consiste à transformer chaque expression régulière REG_j , $j=1,...,J$, en un circuit arithmétique CIRC- REG_j , $j=1,...,J$. Par transformation de l'expression régulière REG_j , on entend transformation de sa structure, c'est-à-dire de sa partie algorithmique à proprement parler, cette expression régulière étant destinée à

être appliquée ici sur des éléments chiffrés. Cette transformation vise à permettre la comparaison d'une chaîne de caractères chiffrée avec l'expression régulière en question pour déterminer si une concordance existe, i.e. si la chaîne de caractères chiffrée que l'on examine (i.e. observe) coïncide avec l'une des chaînes de caractères définies par l'expression régulière.

5 Dans le premier mode de réalisation décrit ici, le module de transformation 6B utilise, pour transformer chaque expression régulière REG_j en un circuit arithmétique, un automate à nombre fini d'états non déterministe ou NFA (pour Non Finite Automaton) modélisant cette expression régulière ainsi qu'une fonction de sélection des états de cet automate. A titre illustratif, la **figure 6** représente un tel automate NFA_{ex} pour l'expression régulière « p(a|b) ». Il s'agit d'un
10 graphe orienté, dont les sommets sont des états et les arêtes caractérisent les transitions permettant de passer d'un état à l'autre.

Par exemple sur la figure 6, l'automate NFA_{ex} comprend trois états distincts, à savoir :

- un état initial q₁ ;
- un état accepté (ou vérifié) q₂ ; et
- 15 — un état rejeté (ou non vérifié) q₃.

Les transitions permettant de passer d'un état à l'autre sont représentées sur la figure 6 en association avec les valeurs des caractères commandant ces transitions.

L'automate NFA_{ex} permet ainsi de comparer n'importe quelle chaîne de caractères à l'expression régulière « p(a|b) ». En effet, partant de l'état initial q₁, si le premier caractère de la
20 chaîne de caractères observée est un « p », alors une transition vers l'état q₂ (« accepté ») de l'automate NFA_{ex} est opérée. Si le caractère est différent de « p » (modélisé par $\bar{p}$), alors une transition vers l'état q₃ (« rejeté ») est opérée. Si l'état q₂ est atteint, on observe alors le deuxième caractère de la chaîne. S'il s'agit d'un « a », l'automate reste dans l'état q₂. Sinon, une transition vers q₃ est opérée, et ainsi de suite pour les autres caractères de la chaîne de caractères
25 examinée. Ainsi, partant de l'état initial q₁, si après examen de tous les caractères de la chaîne de caractères, l'état final obtenu est l'état accepté q₂, alors cela signifie que la chaîne de caractères observée est bien définie par l'expression régulière « p(a|b) ». En revanche, si l'état final obtenu est l'état rejeté q₃, cela signifie que l'expression régulière observée ne répond pas à la définition de l'expression régulière « p(a|b) ».

30 Cet automate est traduit sous forme de circuit arithmétique en introduisant la fonction de sélection Select suivante :

$$\text{Select}(x,y,z)=x.y+(1-x).z$$

où y, z désignent ici des entiers relatifs, et x prend les valeurs 0 ou 1. La fonction Select ainsi définie retourne la valeur « y » si x=1 et la valeur « z » si x=0. Cette fonction de sélection Select
35 est utilisée ici pour modéliser chaque transition de l'automate, en appliquant la convention suivante :

$$\begin{aligned} x &= 1 - ([ci] - [ci']) \\ y &= [q2] \end{aligned}$$

$$z=[q3]$$

où i désigne la position du caractère c_i observé dans la chaîne de caractères en cours d'examen ($i=1,\dots,P$ si P désigne le nombre de caractères dans la chaîne), et c_i désigne le caractère associé par l'automate à la transition entre l'état $[q_i]$ et l'état $[q_{i+1}]$. Selon cette convention, si les caractères c_i et c_i' sont identiques, alors c vaut 1, et l'état accepté q_2 est sélectionné, sinon c vaut 0 et l'état rejeté q_3 est sélectionné.

En appliquant pas à pas cette fonction de sélection, le module de transformation 6B peut modéliser chaque test mis en œuvre par l'automate à partir d'une chaîne de caractères observée. Ainsi dans l'exemple de l'automate NFA_{ex}, si l'on considère une chaîne de caractères observée comprenant deux caractères $[c1\ c2]$ que l'on souhaite comparer à l'expression régulière « $p(a|b)$ », le parcours dans l'automate NFA_{ex} peut être traduit ainsi :

— pour le premier caractère $[c1]$, partant de q_1 , on va vers un état e_1 défini par :

$$e_1=[1-([p]-[c1])].[q_2]+([p]-[c1]).[q_3] \quad (eq1)$$

soit e_1 vaut q_2 (état accepté) si $[c1]=[p]$ et q_3 (état rejeté) sinon ;

— pour le deuxième caractère $[c2]$, deux comparaisons sont effectuées au moyen de l'automate par rapport aux deux alternatives possibles « a » et « b » définies par l'expression régulière (i.e. $(a|b)$), qui se traduisent par les états e_2 et e_3 suivants dans lesquels $[e1==q2]$ vaut 1 si e_1 est égal à q_2 et 0 sinon :

$$e_2=[e1==q2].([1-([a]-[c2])].[q_2]+([a]-[c2]).[q_3]) \quad (eq2)$$

soit e_2 vaut q_2 (état accepté) si $[c2]=[a]$ et q_3 (état rejeté) sinon, et

$$e_3=[e1==q2].([1-([b]-[c2])].[q_2]+([b]-[c2]).[q_3]) \quad (eq3)$$

soit e_3 vaut q_2 (état accepté) si $[c2]=[b]$ et q_3 (état rejeté) sinon.

L'état final est l'état accepté q_2 si e_2 ou e_3 vaut q_2 . Le résultat RES de la détection opérée via l'automate peut donc être traduit en langage booléen sous la forme suivante :

$$RES=[e2==q2]+[e3==q2] \quad (eq4).$$

La fonction définissant le résultat RES et donnée par l'équation (eq4), dans laquelle les états e_1 , e_2 et e_3 ont été remplacés par leurs définitions données aux équations (eq1), (eq2) et (eq3), constitue une fonction représentant l'expression régulière « $p(a|b)$ » sous forme de circuit arithmétique CIRC. Une telle fonction peut avantageusement être évaluée par la fonction d'évaluation FHE.HOM de l'algorithme de chiffrement homomorphe.

On note que l'exemple relativement simple de l'expression régulière « $p(a|b)$ » n'a été donné ici qu'à titre illustratif. L'article de S. Fau et al. intitulé « Towards practical program execution overfully homomorphic encryption schemes », 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pages 284-290 introduit d'autres exemples basés sur la fonction de sélection Select et permettant de traduire divers algorithmes sous forme de circuits arithmétiques.

Dans le premier mode de réalisation, le module de transformation 6B procède de façon identique à ce qui a été précédemment décrit dans l'exemple de l'expression régulière « $p(a|b)$ »

pour transformer chaque expression régulière REG_j , $j=1,\dots,J$ en un circuit arithmétique CIRC- REG_j . Autrement dit, il s'appuie d'une part, sur un automate NFA à nombre fini d'états non déterministe modélisant cette expression régulière, et d'autre part, sur la fonction de sélection Select précédemment introduite, et fournit un circuit arithmétique CIRC- REG_j définissant un résultat de
5 détection RES_j , $j=1,\dots,J$. On note que chaque circuit arithmétique CIRC- REG_j est destiné à être appliqué sur des éléments chiffrés et que le résultat de détection RES_j qu'il fournit est lui-même un élément chiffré.

Il convient de noter également que le circuit arithmétique CIRC- REG_j obtenu par le module de transformation 6B pour chaque expression régulière REG_j offre une représentation
10 compacte de l'expression régulière REG_j , évaluable par la fonction d'évaluation homomorphe FHE.HOM. D'autres représentations peuvent toutefois être envisagées en variante. Ainsi par exemple, on peut envisager une autre fonction décrivant l'expression régulière REG_j consistant à énumérer toutes les chaînes de caractères possibles définies par l'expression régulière REG_j . On comprend bien toutefois qu'une telle représentation peut devenir très complexe voire inappropriée
15 pour certaines expressions régulières comprenant par exemple l'opérateur *.

En outre, dans le mode de réalisation décrit ici, le module de transformation 6B détermine un circuit arithmétique distinct pour chaque expression régulière : autrement dit, un circuit arithmétique représente une unique expression régulière. Dans un autre mode de réalisation, on peut envisager que le module de transformation 6B définisse un seul circuit
20 arithmétique représentant toutes les expressions régulières, ou plusieurs circuits arithmétiques représentant chacun une ou plusieurs expressions régulières.

Les circuits arithmétiques CIRC- REG_j sont stockés ici par le module de transformation 6B dans la mémoire non volatile 15 du dispositif de sécurité RG 6. Comme mentionné précédemment, ces circuits arithmétiques CIRC- REG_j , $j=1,\dots,J$, sont destinés à être appliqués sur
25 des éléments chiffrés et nécessitent à cet effet la connaissance des chiffrés des signatures caractéristiques SIG_i , $i=1,\dots,I$.

En référence de nouveau à la figure 4, le dispositif de sécurité RG 6 génère donc pour chaque signature SIG_i , $i=1$, un chiffré FHE- SIG_i de cette signature, via son module de chiffrement 6C (étape E40).

30 On note que les étapes E30 et E40 peuvent être inversées chronologiquement ou être mises en œuvre en parallèle.

Plus précisément, dans le premier mode de réalisation décrit ici, le module de chiffrement 6C chiffre chaque signature SIG_i , $i=1,\dots,I$ en lui appliquant la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE, paramétrée par la clé publique de
35 chiffrement $pk(RG)$ du dispositif de sécurité RG 6.

Puis le module de transmission 6D du dispositif de sécurité RG 6 transmet au dispositif de détection d'intrusions MB 5, via les moyens de communication 16 du dispositif de sécurité RG 6, les circuits arithmétiques CIRC- REG_j , $j=1,\dots,J$, décrivant les expressions régulières REG_j , $j=1,\dots,J$

ainsi que les signatures chiffrées FHE-SIG_i, $i=1,\dots,I$ (étape E50). On note que les signatures en clair SIG_i, $i=1,\dots,I$ sont gardées secrètes par le dispositif de sécurité RG 6 à l'égard du dispositif de détection d'intrusions MB 5 : seules leurs formes chiffrées et la structure des expressions régulières (sous forme de circuits arithmétiques) sont transmises au dispositif de détection d'intrusions MB 5.

5 En référence à la figure 5, le dispositif de détection MB 5 stocke les circuits arithmétiques CIRC-REG_j, $j=1,\dots,J$ et les signatures chiffrées FHE-SIG_i, $i=1,\dots,I$ reçus du dispositif de sécurité RG 6 par son premier module de réception 5A dans sa mémoire non volatile 10 (étape F10).

10 On suppose maintenant que le dispositif émetteur TX 2 souhaite émettre un message m à destination du dispositif récepteur RX 3. Le message m peut être constitué d'un ou de plusieurs paquets de données. Dans la suite de la description par souci de simplification, on considère un unique paquet de données constitué d'une pluralité de caractères $m_1, m_2, \dots, m_L$, L désignant un entier supérieur à 1.

15 En préparation de cet échange, le dispositif de détection d'intrusions MB 5 génère, dans le premier mode de réalisation décrit ici, un nombre aléatoire (i.e. aléa) x_0 qu'il envoie via le réseau NW au dispositif émetteur TX 2 (étape F20). Dans le premier mode de réalisation décrit ici, ce nombre aléatoire x_0 a vocation à permettre au dispositif de sécurité RG 6 de vérifier si le dispositif émetteur TX2 est honnête, comme détaillé davantage ultérieurement. Il est donc également transmis au dispositif de sécurité RG 6.

20 La **figure 7** illustre les principales étapes mises en œuvre par le dispositif émetteur TX 2 lors de son échange du message m avec le dispositif récepteur RX 3.

25 En préparation de l'envoi du message m , le dispositif émetteur TX 2 génère une clé secrète K de chiffrement, qu'il partage avec le dispositif récepteur RX 3, par exemple, via un échange sécurisé mis en œuvre entre les deux dispositifs (étape G10). Cet échange sécurisé peut s'appuyer par exemple sur la procédure standard prévue par les protocoles SSL/TLS. La clé secrète K est ici éphémère, dans le sens où elle est générée pour la connexion présente avec le dispositif récepteur RX 3.

30 Puis, dans le premier mode de réalisation décrit ici, suite à la réception de l'aléa x_0 (étape G20), le dispositif émetteur TX 2 génère un contenu CONT en concaténant l'aléa x_0 avec le message m qu'il souhaite envoyer au dispositif récepteur RX 3 (étape G30). Le contenu CONT est un contenu dérivé du message m au sens de l'invention. Dans un autre mode de réalisation n'utilisant pas l'aléa x_0 , le contenu CONT dérivé du message m est constitué uniquement du message m .

35 Le dispositif émetteur TX 2 génère alors, au moyen de son module 2A, un chiffré T du contenu CONT en lui appliquant la procédure de chiffrement SYM-ENC de l'algorithme de chiffrement symétrique ALG-SYM paramétrée par la clé de chiffrement secrète K (étape G40).

Le dispositif émetteur TX 2 génère par ailleurs, dans le premier mode de réalisation décrit ici, par l'intermédiaire de son module 2B, un chiffré S de la clé de chiffrement secrète K (étape G50).

Le chiffré S est généré par le module 2B en appliquant à la clé secrète K la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE, paramétrée par la clé de chiffrement publique pk(RG) du dispositif de sécurité RG 6.

Puis, le dispositif émetteur TX 2 par le biais de son module d'émission 2C, émet le chiffré T du contenu CONT et le chiffré S de la clé secrète K à destination du dispositif récepteur RX 3 (étape G60).

En référence à la figure 5 de nouveau, le chiffré T et le chiffré S émis par le dispositif émetteur TX 2 à destination du dispositif récepteur RX 3 sont interceptés par le module de détection d'intrusions MB 5, et plus particulièrement par son second module de réception 5B (étape F30). L'interception du chiffré S par le dispositif de détection d'intrusions MB 5 constitue une étape d'obtention du chiffré S au sens de l'invention.

Le dispositif émetteur TX 2 génère par ailleurs, par le biais de son module d'obtention 5C un chiffré T' du chiffré T en appliquant sur le chiffré T la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE, paramétrée par la clé publique de chiffrement pk(RG) du dispositif de sécurité RG 6 (étape F40). Il en résulte la relation suivante :

$$T' = \text{FHE.ENC}(\text{SYM-ENC}((x_0|m), K), \text{pk(RG)}).$$

Puis, via son premier module d'évaluation 5D, le dispositif de détection d'intrusions MB 5 évalue la procédure de déchiffrement SYM-DEC de l'algorithme de chiffrement/déchiffrement symétrique ALG-SYM sur le chiffré T' (étape F50). Il utilise à cet effet une description de la procédure de déchiffrement SYM-DEC sous forme de circuit arithmétique et le chiffré S de la clé secrète partagée K, sur lesquelles il applique la fonction d'évaluation homomorphe FHE.HOM de l'algorithme de chiffrement homomorphe ALG-FHE. On note que l'obtention d'une description de la procédure de déchiffrement SYM-DEC sous forme d'un circuit arithmétique ou plus généralement sous une forme qui peut être évaluée par la fonction d'évaluation homomorphe FHE.HOM ne pose pas de difficulté en soi, la plupart des algorithmes de déchiffrement se présentant déjà sous une telle forme.

Grâce aux propriétés du chiffement homomorphe, le premier module d'évaluation 5D obtient d'une part, un chiffré V du message m par la procédure de chiffement FHE.ENC paramétrée par la clé publique de chiffement pk(RG) du dispositif de sécurité RG 6, et d'autre part, un chiffré V' de l'aléa x0 par la procédure de chiffement FHE.ENC paramétrée par la clé publique de chiffement pk(RG) du dispositif de sécurité RG 6, soit :

$$V = \text{FHE.ENC}(m, \text{pk(RG)}) \text{ et } V' = \text{FHE.ENC}(x_0, \text{pk(RG)})$$

Le dispositif de détection d'intrusions MB 5, via son second module d'évaluation 5E, évalue alors sur le chiffré V chaque expression régulière REGj, j=1,...,J. Il utilise à cet effet la description de chaque expression régulière REGj sous forme de circuit arithmétique CIRC-REGj et

les chiffrés FHE-SIG_i, $i=1,\dots,I$ des signatures sur lesquels il applique la fonction d'évaluation homomorphe FHE.HOM de l'algorithme de chiffrement homomorphe ALG-FHE (étape F60).

En raison des propriétés du chiffrement homomorphe, le second module d'évaluation 5E obtient à l'issue de cette évaluation un résultat intermédiaire de détection chiffré RES_j pour chaque expression régulière REG_j, $j=1,\dots,J$. Chaque résultat intermédiaire de détection RES_j est égal à 1 si le chiffré V correspond à l'expression régulière REG_j, et à 0 sinon.

Ainsi, une correspondance avec une règle de détection établie par l'éditeur de sécurité est détectée si l'un au moins des résultats intermédiaires RES_j est égal à 1. Le second module d'évaluation évalue ici, à partir des résultats intermédiaires, un résultat de détection chiffré B selon l'expression :

$$B = \text{RES}_1 + \text{RES}_2 + \dots + \text{RES}_J$$

où « + » désigne ici l'opérateur booléen OU, de sorte que le résultat B est égal à 0 ou 1.

On note que dans le mode de réalisation décrit ici, chaque expression régulière est décrite au moyen d'un circuit arithmétique distinct. Comme mentionné précédemment, dans un autre mode de réalisation, on peut envisager d'avoir une seule et même fonction, c'est-à-dire ici un seul et même circuit arithmétique, décrivant l'ensemble des expressions régulières auquel cas le résultat de détection chiffré B est directement obtenu en sortie de la fonction d'évaluation FHE.HOM. Dans un autre mode de réalisation, on considère plusieurs circuits arithmétiques décrivant chacun une ou plusieurs expressions régulières, le résultat de détection chiffré B étant alors obtenu en sommant les résultats intermédiaires obtenus après évaluation de chacun de ces circuits.

Le résultat de détection chiffré B vérifie par ailleurs la relation suivante :

$$B = \text{FHE.ENC}(\text{det}(m), \text{pk}(\text{RG})).$$

où det(m) désigne le résultat de détection qui serait obtenu en appliquant les expressions régulières REG_j directement sur le message m.

Dans le premier mode de réalisation décrit ici, le dispositif de détection d'intrusions MB 5 transmet via ses moyens de communication 11 le résultat de détection chiffré B au dispositif de sécurité RG 6 (étape F70). Il lui transmet également le chiffré V'.

En référence à la figure 4, sur réception des chiffrés B et V' par son module de réception 6E (étape E60), le dispositif de sécurité RG 6 déchiffre le résultat de détection chiffré B (étape E70). Son module de déchiffrement 6F utilise à cet effet la procédure de déchiffrement FHE.DEC de l'algorithme de chiffrement homomorphe ALG-FHE paramétrée par la clé de déchiffrement privée sk(RG) du dispositif de sécurité RG 6. Il obtient ainsi le résultat de détection det(m), qu'il transmet en retour, via son module de transmission 6D, au dispositif de détection d'intrusions MB 5 (étape E80).

Par ailleurs, dans le premier mode de réalisation décrit ici, le dispositif de sécurité RG 6 vérifie également l'intégrité de l'aléa x0 (étape E90). A cet effet, il déchiffre au moyen de son module de déchiffrement 6F le chiffré V' en lui appliquant la procédure de déchiffrement FHE.DEC

paramétrée par la clé de déchiffrement privée $sk(RG)$ du dispositif de sécurité RG 6. Le résultat de ce déchiffrement est comparé à la valeur de l'aléa $x0$ précédemment transmise à l'étape F20 par le dispositif de détection d'intrusions. Si les deux valeurs coïncident (i.e. sont égales), la vérification est validée, autrement dit, le dispositif émetteur TX 2 a agi de façon honnête et transmis le bon aléa au dispositif de détection d'intrusions MB 5. Sinon, cela signifie que le dispositif émetteur TX 2 est malhonnête.

Le dispositif de sécurité RG 6 peut alors lorsque des valeurs discordantes sont détectées lors de l'étape de vérification E90, informer le dispositif de détection d'intrusions MB 5, et/ou un administrateur du réseau NW.

On note que cette étape de vérification, et corrélativement l'utilisation de l'aléa $x0$ par le dispositif émetteur TX 2, par le dispositif de détection d'intrusions MB 5 et par le dispositif de sécurité RG 6, sont optionnelles. L'invention peut être mise en œuvre en considérant un contenu CONT constitué uniquement du message m .

En référence à la figure 5, sur réception du résultat de détection $det(m)$ en provenance du dispositif de sécurité RG 6, le module de détection 5F du dispositif de détection d'intrusions détermine si une intrusion a été commise sur le réseau NW (étape F90). Plus précisément, il détermine ici qu'il existe une intrusion sur le réseau si $det(m)$ est égal à 1, et déduit l'absence d'intrusion si $det(m)$ est égal à 0.

Dans le premier mode de réalisation décrit ici, si aucune intrusion n'a été détectée par le module de détection 5F (réponse non à l'étape test F90), le dispositif de détection d'intrusions MB 5 transmet le chiffré T du message m au dispositif récepteur RX pour déchiffrement. Le dispositif de réception RX 3, via son module de déchiffrement 3A, peut alors déchiffrer le chiffré T en lui appliquant la procédure de déchiffrement SYM-DEC de l'algorithme de chiffrement/déchiffrement symétrique ALG-SYM paramétrée par sa clé privée de déchiffrement $sk(PG)$.

Si au contraire, une intrusion est détectée par le module de détection 5F (réponse oui à l'étape test F90), différentes actions peuvent être entreprises par le dispositif de détection d'intrusions MB 5 en fonction de sa configuration (étape F110). Par exemple, il peut, via ses moyens de communication 11, notifier l'administrateur du réseau NW de cette détection. En variante ou en complément, le dispositif de détection d'intrusions MB 5 peut supprimer le message chiffré T et ne pas les transmettre au dispositif récepteur RX 3, celui-ci étant corrompu, etc.

L'invention permet donc, grâce à l'utilisation de l'algorithme de chiffrement homomorphe ALG-FHE, d'appliquer une procédure d'inspection en profondeur full IDS sur le trafic chiffré échangé entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 sans que le dispositif de détection d'intrusions MB 5 n'ait connaissance des mots-clés définis par le dispositif de sécurité RG 6. L'invention permet ainsi de garantir la confidentialité des échanges entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 et leur vie privée, tout en permettant la détection d'intrusions sur le réseau emprunté par ces dispositifs.

On note que le premier mode de réalisation est un mode interactif en ce qu'il s'appuie sur un échange entre le dispositif de détection d'intrusions MB 5 et le dispositif de sécurité RG 6 pour que le dispositif de détection d'intrusions MB 5 puisse accéder au résultat de détection déchiffré $\text{det}(m)$. Ce mode interactif permet au dispositif de sécurité RG 6 de ne pas divulguer sa clé de déchiffrement privée $\text{sk}(\text{RG})$.

Toutefois, en variante, l'invention peut être mise en œuvre selon un mode non interactif. A cet effet par exemple, la clé privée de déchiffrement $\text{sk}(\text{RG})$ du dispositif de sécurité RG 6 peut être stockée dans un module matériel de sécurité (ou HSM pour Hardware Secure Module), accessible par le dispositif de détection d'intrusions MB 5. De façon connue, un tel module HSM est un module électronique considéré comme inviolable offrant des fonctions cryptographiques, comme notamment le stockage de clé cryptographiques. Ainsi, dans une variante du premier mode de réalisation, on peut envisager que le dispositif de détection d'intrusions MB 5 obtient la clé privée de déchiffrement $\text{sk}(\text{RG})$ du module HSM puis déchiffre le résultat de détection chiffré B au moyen de cette clé privée de déchiffrement afin d'obtenir le résultat de détection $\text{det}(m)$. Dans une autre variante, on peut envisager que ce soit le module HSM qui déchiffre lui-même le chiffré B et fournit en retour le résultat de détection $\text{det}(m)$ au dispositif de détection d'intrusions MB 5. On peut bien entendu envisager en outre de compléter ces variantes de réalisation par des mécanismes additionnels permettant de se protéger contre un comportement malhonnête du dispositif de détection d'intrusions MB 5 (tels que par exemple une vérification par le module HSM de la cohérence de ce qui est déchiffré par le dispositif de détection d'intrusions MB 5).

Dans le premier mode de réalisation qui vient d'être décrit, la clé secrète K partagée entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 et utilisée pour chiffrer les échanges entre ces deux dispositifs, est chiffrée par le dispositif émetteur TX 2 au moyen de la clé publique de chiffrement du dispositif de sécurité RG 6. Il en résulte qu'un dispositif de sécurité RG 6 peu scrupuleux peut écouter les échanges entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3, accéder au message chiffré T et au chiffré S de la clé partagée K, déchiffrer le chiffré S et accéder au message m en clair. Pour pallier cet inconvénient, dans un second mode de réalisation de l'invention, la clé secrète K partagée entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 n'est plus chiffrée par le dispositif émetteur TX 2 au moyen de la clé publique de chiffrement $\text{pk}(\text{RG})$ du dispositif de sécurité RG 6 mais au moyen d'une clé publique de chiffrement $\text{pk}(\text{RX})$ du dispositif récepteur RX 3, publiée préalablement. Le second mode de réalisation s'appuie par ailleurs sur une procédure de rechiffrement de la clé secrète, comme détaillé maintenant.

La **figure 8** illustre les étapes mises en œuvre par le dispositif émetteur TX 2 dans ce second mode de réalisation. Les étapes portant les mêmes références que les étapes illustrées à la figure 7 sont identiques aux étapes mises en œuvre dans le premier mode de réalisation.

Ainsi, en référence à la figure 8, en préparation de l'envoi du message m, le dispositif émetteur TX 2 génère une clé secrète K de chiffrement, qu'il partage avec le dispositif récepteur

RX 3 (étape G10). Puis, suite à la réception de l'aléa x_0 (étape G20), il génère le contenu CONT en concaténant l'aléa x_0 avec le message m qu'il souhaite envoyer au dispositif récepteur RX 3 (étape G30). Le dispositif émetteur TX 2 génère au moyen de son module 2A le chiffré T du contenu CONT en lui appliquant la procédure de chiffrement SYM-ENC de l'algorithme de chiffrement symétrique ALG-SYM paramétrée par la clé de chiffrement secrète K (étape G40).

Le dispositif émetteur TX 2 génère par ailleurs, dans le second mode de réalisation décrit ici, par l'intermédiaire de son module 2B, un chiffré dit intermédiaire S' de la clé de chiffrement secrète K (étape G50'). Le chiffré intermédiaire S' est généré dans le second mode de réalisation en appliquant à la clé secrète K la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE, paramétrée par la clé de chiffrement publique $pk(RX)$ du dispositif récepteur RX 3.

Puis, le dispositif émetteur TX 2 par le biais de son module d'émission 2C, émet le chiffré T du contenu CONT et le chiffré intermédiaire S' de la clé secrète K à destination du dispositif récepteur RX 3 (étape G60').

En d'autres mots, le procédé mis en œuvre par le dispositif émetteur TX 2 diffère dans ce second mode de réalisation du procédé mis en œuvre par le dispositif émetteur TX 2 dans le premier mode de réalisation par les étapes G50' et G60'.

La **figure 9** illustre les étapes mises en œuvre par le dispositif de détection d'intrusions MB 5 dans le second mode de réalisation. Les étapes portant les mêmes références que les étapes illustrées à la figure 5 sont identiques aux étapes mises en œuvre dans le premier mode de réalisation. On note que le dispositif de sécurité RG 6 n'est pas impacté par les modifications apportées dans le second mode de réalisation de sorte que les étapes mises en œuvre par le dispositif de sécurité RG 6 dans le second mode de réalisation sont identiques aux étapes E10 à E90 représentées à la figure 4 et mises en œuvre dans le premier mode de réalisation.

En particulier, les étapes E10 à E50 de génération et de transmission des circuits arithmétiques CIRC-REG $_j$, $j=1,...,J$ des expressions régulières et des chiffrés FHE-SIG $_i$, $i=1,...,I$ des signatures par le dispositif de sécurité RG 6 au dispositif de détection d'intrusions MB 5 sont identiques à celles mises en œuvre dans le premier mode de réalisation. Il en est de même à la figure 10 des étapes F10 et F20 mises en œuvre par le dispositif de détection d'intrusions MB 5.

Le chiffré T et le chiffré intermédiaire S' émis par le dispositif émetteur TX 2 à destination du dispositif récepteur RX 3 sont interceptés par le dispositif de détection d'intrusions MB 5, et plus particulièrement par son second module de réception 5B (étape F30').

Sur réception du chiffré intermédiaire S' , dans le second mode de réalisation, le dispositif de détection d'intrusions MB 5 obtient alors du dispositif récepteur RX 3 une clé de rechiffrement $rk(RX \rightarrow RG)$ du dispositif récepteur RX 3 vers le dispositif de sécurité RG 6 (étape F31'). Dans le second mode de réalisation décrit ici, cette clé de rechiffrement $rk(RX \rightarrow RG)$ comprend :

- une première partie $rk1$ égale à la clé de chiffrement publique $pk(RG)$ du dispositif de sécurité RG 6, soit

$$k1=pk(RG) ; \text{ et}$$

- une seconde partie $rk2$ obtenue en chiffrant une clé de déchiffrement secrète $sk(RX)$ associée à la clé publique de chiffrement $pk(RX)$ du dispositif récepteur RX 3 au moyen de la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE paramétrée par la clé publique de chiffrement $pk(RG)$ du dispositif de sécurité RG 6, soit :

$$k2=FHE.ENC(sk(RX),pk(RG)).$$

Suite à l'obtention de la clé de rechiffrement $rk(RX \rightarrow RG)$, le dispositif de détection d'intrusions MB 5 rechiffre le chiffré intermédiaire S' de la clé secrète S au moyen de la clé de rechiffrement $rk(RX \rightarrow RG)$ et de la procédure de chiffrement FHE.ENC de l'algorithme de chiffrement homomorphe ALG-FHE (étape F32'). Il obtient via cette étape de rechiffrement un chiffré S de la clé partagée K chiffrée au moyen de la clé publique de chiffrement $pk(RG)$ du dispositif de sécurité RG 6, soit :

$$S=FHE.ENC(K,pk(RG)).$$

Les notions de clé de rechiffrement et de rechiffrement d'un chiffré sont connues en soi et ne sont pas décrites en détail ici.

Les étapes F30', F31' et F32' constituent dans leur ensemble une étape d'obtention d'un chiffré S de la clé partagée K au sens de l'invention.

Les étapes mises en œuvre ensuite par le dispositif de détection d'intrusions MB 5 et par le dispositif de sécurité RG 6 respectivement dans le second mode de réalisation sont identiques aux étapes F40 à F110 et E60 à E90 décrites précédemment dans le premier mode de réalisation. Il en est de même du déchiffrement du chiffré T par le dispositif récepteur RX 3.

L'invention permet donc, dans ce second mode de réalisation comme dans le premier mode de réalisation, de permettre d'appliquer une procédure d'inspection en profondeur full IDS sur le trafic chiffré échangé entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 sans que le dispositif de détection d'intrusions MB 5 n'ait connaissance des mots-clés définis par le dispositif de sécurité RG 6. Elle permet en outre de garantir la confidentialité des échanges entre le dispositif émetteur TX 2 et le dispositif récepteur RX 3 et leur vie privée, non seulement à l'égard du dispositif de détection d'intrusions MB 5 mais également du dispositif de sécurité RG 6.

REVENDEICATIONS

1. Procédé de détection d'intrusions sur un réseau (NW) via lequel sont aptes à communiquer un dispositif émetteur (TX 2) et un dispositif récepteur (RX 3) en utilisant un
- 5 algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre le dispositif émetteur et le dispositif récepteur, ledit procédé de détection étant destiné à être mis en œuvre par un dispositif de détection d'intrusions (MB 5) et comprenant :
- une étape de réception (F10), en provenance d'un dispositif de sécurité (RG 6) ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter le réseau,
 - 10 ladite au moins une règle de détection comprenant au moins une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion :
 - d'au moins une fonction (CIRC-REGj) décrivant ladite au moins une expression régulière (REGj) et pouvant être évaluée au moyen d'une fonction d'évaluation homomorphe d'un algorithme de chiffrement homomorphe ; et
 - 15 ○ d'un chiffré (FHE-SIGi) de chaque signature (SIGi) caractéristique de ladite au moins une intrusion, obtenu en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ;
 - une étape de réception (F30,F30') en provenance du dispositif émetteur d'un chiffré T d'un
 - 20 contenu dérivé d'un message destiné au dispositif récepteur, ce chiffré T ayant été obtenu en utilisant une procédure de chiffrement de l'algorithme de chiffrement/déchiffrement symétrique paramétrée par ladite clé de chiffrement secrète ;
 - une étape d'obtention (F40,F30,F32') d'un chiffré T' du chiffré T et d'un chiffré S de la clé de chiffrement secrète, lesdits chiffrés T' et S correspondant à l'application sur le chiffré T et sur
 - 25 la clé de chiffrement secrète de la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé de chiffrement publique du dispositif de sécurité ;
 - une première étape d'évaluation (F50) d'une procédure de déchiffrement de l'algorithme de chiffrement/déchiffrement symétrique sur le chiffré T' en utilisant ladite fonction d'évaluation homomorphe dudit algorithme de chiffrement homomorphe et le chiffré S de la clé de
 - 30 chiffrement secrète, cette première étape d'évaluation fournissant un chiffré V du message destiné au dispositif récepteur par la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé publique de chiffrement du dispositif de sécurité ;
 - une seconde étape d'évaluation (F60) de ladite au moins une fonction décrivant ladite au
 - 35 moins une expression régulière sur le chiffré V du message en utilisant les chiffrés des signatures, cette seconde étape d'évaluation fournissant un chiffré d'un résultat de détection indiquant l'existence ou non d'une dite expression régulière correspondant au message ; et

- une étape de détection (F90) d'une intrusion sur le réseau si le résultat de détection déchiffré indique qu'il existe au moins une dite expression régulière correspondant au message.

2. Procédé de détection selon la revendication 1 dans lequel le chiffré S de la clé de chiffrement secrète est obtenu (F30) du dispositif émetteur (TX 2).

3. Procédé de détection selon la revendication 1 dans lequel l'étape d'obtention (F30'-F32') du chiffré S de la clé de chiffrement secrète comprend :

- une étape de réception (F30'), en provenance du dispositif émetteur, d'un chiffré dit intermédiaire S' de la clé de chiffrement secrète obtenu en utilisant la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé de chiffrement publique du dispositif récepteur ;
- une étape d'obtention (F31') d'une clé de rechiffrement du dispositif récepteur vers le dispositif de sécurité ; et
- une étape de rechiffrement (F32') du chiffré intermédiaire S' en utilisant ladite clé de rechiffrement, cette étape de rechiffrement fournissant ledit chiffré S de la clé de chiffrement secrète.

4. Procédé de détection selon l'une quelconque des revendications 1 à 3 comprenant en outre :

- une étape de transmission (F70) du chiffré du résultat de détection au dispositif de sécurité pour déchiffrement en utilisant une procédure de déchiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé privée de déchiffrement associée à la clé publique de chiffrement du dispositif de sécurité ; et
- une étape de réception (F80) du résultat de détection déchiffré en provenance du dispositif de sécurité.

5. Procédé de détection selon l'une quelconque des revendications 1 à 3 comprenant en outre :

- une étape d'obtention d'une clé privée de déchiffrement associée à la clé publique de chiffrement du dispositif de sécurité et stockée dans un module matériel de sécurité ; et
- une étape de déchiffrement du chiffré du résultat de détection en utilisant la procédure de déchiffrement dudit algorithme de chiffrement homomorphe paramétrée par cette clé privée de déchiffrement.

6. Procédé de détection selon l'une quelconque des revendications 1 à 5 dans lequel au moins une fonction décrivant au moins une expression régulière reçue du dispositif émetteur est un circuit arithmétique (CIRC-REGj).

7. Procédé de détection selon l'une quelconque des revendications 1 à 6 dans lequel le contenu (CONT) dérivé du message est constitué du message (m) destiné au dispositif récepteur ou d'une concaténation de ce message (m) et d'un aléa (x0) connu du dispositif de sécurité et du dispositif de détection d'intrusions.

8. Procédé de détection selon la revendication 7 dans lequel le contenu dérivé du message est constitué d'une concaténation du message (m) et d'un aléa (x0) connu du dispositif de sécurité et du dispositif de détection d'intrusions, et dans lequel la première étape d'évaluation (F50) fournit en outre un chiffré V' de l'aléa par la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé publique de chiffrement du dispositif de sécurité, ledit procédé de détection comprenant en outre une étape de transmission (F70) dudit chiffré V' de l'aléa au dispositif de sécurité pour vérification.

9. Procédé de communication d'un dispositif de sécurité (RG 6) avec un dispositif de détection d'intrusions (MB 5) sur un réseau, ledit dispositif de sécurité ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter le réseau, ladite au moins une règle de détection comprenant au moins une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion, ledit procédé de communication comprenant :

- une étape de transformation (E30) de ladite au moins une expression régulière (REGj) en une fonction (CIRC-REGj) décrivant ladite au moins une expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation homomorphe d'un algorithme de chiffrement homomorphe ;
- une étape de génération (E40) d'un chiffré (FHE-SIGi) de chaque signature (SIGi) caractéristique de ladite au moins une intrusion en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ; et
- une étape de transmission (E50) de ladite au moins une fonction décrivant ladite au moins une expression régulière et de chaque chiffré de chaque signature caractéristique de ladite au moins une intrusion à un dispositif de détection d'intrusions sur le réseau.

10. Procédé de communication selon la revendication 9 dans lequel lors de l'étape de transformation, au moins une fonction décrivant au moins une expression régulière est un circuit arithmétique obtenu au moyen d'un automate à nombre fini d'états non déterministe modélisant ladite au moins une expression régulière et d'une fonction de sélection des états dudit automate.

11. Procédé de communication selon la revendication 9 ou 10 comprenant en outre :

- une étape de réception (E60) en provenance du dispositif de détection d'un chiffré d'un résultat de détection ;
- une étape de déchiffrement (E70) dudit chiffré du résultat de détection en utilisant une procédure de déchiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé privée de déchiffrement associée à la clé publique de chiffrement du dispositif de sécurité ;
- et
- une étape de transmission (E80) du résultat de détection déchiffré au dispositif de détection d'intrusions.

12. Programme d'ordinateur (PROG1,PROG2) comportant des instructions pour l'exécution des étapes du procédé de détection d'intrusions selon l'une quelconque des revendications 1 à 8 ou du procédé de communication selon l'une quelconque des revendications 9 à 11 lorsque ledit programme est exécuté par un ordinateur.

13. Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes du procédé de détection d'intrusions selon l'une quelconque des revendications 1 à 8 ou du procédé de communication selon l'une quelconque des revendications 9 à 11.

14. Dispositif de détection d'intrusions (MB 5) sur un réseau via lequel sont aptes à communiquer un dispositif émetteur (TX 2) et un dispositif récepteur (RX 3) en utilisant un algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre le dispositif émetteur et le dispositif récepteur, ledit dispositif de détection étant destiné à être localisé entre le dispositif émetteur et le dispositif récepteur et comprenant :

- un premier module de réception (5A), apte à recevoir en provenance d'un dispositif de sécurité ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter le réseau, ladite au moins une règle de détection comprenant une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion :
 - au moins une fonction décrivant ladite au moins une expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation homomorphe d'un algorithme de chiffrement homomorphe ; et
 - un chiffré de chaque signature caractéristique de ladite au moins une intrusion, obtenu en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ;
- un second module de réception (5B), apte à recevoir en provenance du dispositif émetteur un chiffré T d'un contenu dérivé d'un message destiné au dispositif récepteur, ce chiffré T ayant

été obtenu en utilisant une procédure de chiffrement de l'algorithme de chiffrement/déchiffrement symétrique paramétrée par ladite clé de chiffrement secrète ;

- un module d'obtention (5C) d'un chiffré T' du chiffré T et d'un chiffré S de la clé de chiffrement secrète, lesdits chiffrés T' et S correspondant à l'application sur le chiffré T et sur la clé de chiffrement secrète de la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé de chiffrement publique du dispositif de sécurité ;
- un premier module d'évaluation (5D) d'une procédure de déchiffrement de l'algorithme de chiffrement/déchiffrement symétrique sur le chiffré T' configuré pour utiliser ladite fonction d'évaluation homomorphe dudit algorithme de chiffrement homomorphe et le chiffré S de la clé de chiffrement secrète, ce premier module d'évaluation étant en outre configuré pour fournir un chiffré V du message destiné au dispositif récepteur par la procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par la clé publique de chiffrement du dispositif de sécurité ;
- un second module d'évaluation (5E) configuré pour évaluer ladite au moins une fonction décrivant ladite au moins une expression régulière sur le chiffré V du message en utilisant les chiffrés des signatures, ce second module d'évaluation étant en outre configuré pour fournir un chiffré d'un résultat de détection indiquant l'existence ou non d'une dite expression régulière correspondant au message ; et
- un module de détection (5F) d'une intrusion sur le réseau activé si le résultat de détection déchiffré indique qu'il existe au moins une dite expression régulière correspondant au message.

15. Dispositif de sécurité (6) ayant accès à au moins une règle de détection d'au moins une intrusion susceptible d'affecter un réseau, ladite au moins une règle de détection comprenant une expression régulière établie à partir d'au moins une signature caractéristique de ladite au moins une intrusion, ledit dispositif de sécurité comprenant :

- un module de transformation (6B), configuré pour transformer ladite au moins une expression régulière en une fonction décrivant ladite au moins une expression régulière et pouvant être évaluée au moyen d'une fonction d'évaluation homomorphe d'un algorithme de chiffrement homomorphe ;
- un module de chiffrement (6C), configuré pour générer un chiffré de chaque signature caractéristique de ladite au moins une intrusion en appliquant une procédure de chiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé publique de chiffrement du dispositif de sécurité ; et
- un module de transmission (6D), configuré pour transmettre ladite au moins une fonction décrivant ladite au moins une expression régulière et chaque chiffré de chaque signature caractéristique de ladite au moins une intrusion à un dispositif de détection d'intrusions sur le réseau.

16. Dispositif de sécurité selon la revendication 15 comprenant en outre :

- un module de réception (6E), apte à recevoir en provenance du dispositif de détection un chiffré d'un résultat de détection ;
- 5 — un module de déchiffrement (6F), configuré pour déchiffrer ledit chiffré du résultat de détection en utilisant une procédure de déchiffrement dudit algorithme de chiffrement homomorphe paramétrée par une clé privée de déchiffrement associée à la clé publique de chiffrement du dispositif de sécurité ; et
- un module de transmission (6D), configuré pour transmettre le résultat de détection déchiffré
- 10 au dispositif de détection d'intrusions.

17. Système de détection (4) d'intrusions sur un réseau via lequel sont aptes à communiquer un dispositif émetteur et un dispositif récepteur en utilisant un algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre

15 le dispositif émetteur et le dispositif récepteur, ledit système de détection d'intrusions comprenant :

- un dispositif de détection d'intrusions (MB 5) conforme à la revendication 14 ; et
- un dispositif de sécurité (RG 6) conforme à la revendication 15 ou 16.

20 18. Système de communications (1) comprenant :

- au moins un dispositif émetteur (TX 2) et au moins un dispositif récepteur (RX 3) aptes à communiquer sur un réseau en utilisant un algorithme de chiffrement/déchiffrement symétrique paramétré par une clé de chiffrement secrète partagée entre le dispositif émetteur et le dispositif récepteur ; et
- 25 — un système de détection d'intrusions (4) selon la revendication 17, le dispositif de détection d'intrusions dudit système de détection étant destiné à être localisé entre ledit au moins un dispositif émetteur et ledit au moins un dispositif récepteur.

1/4

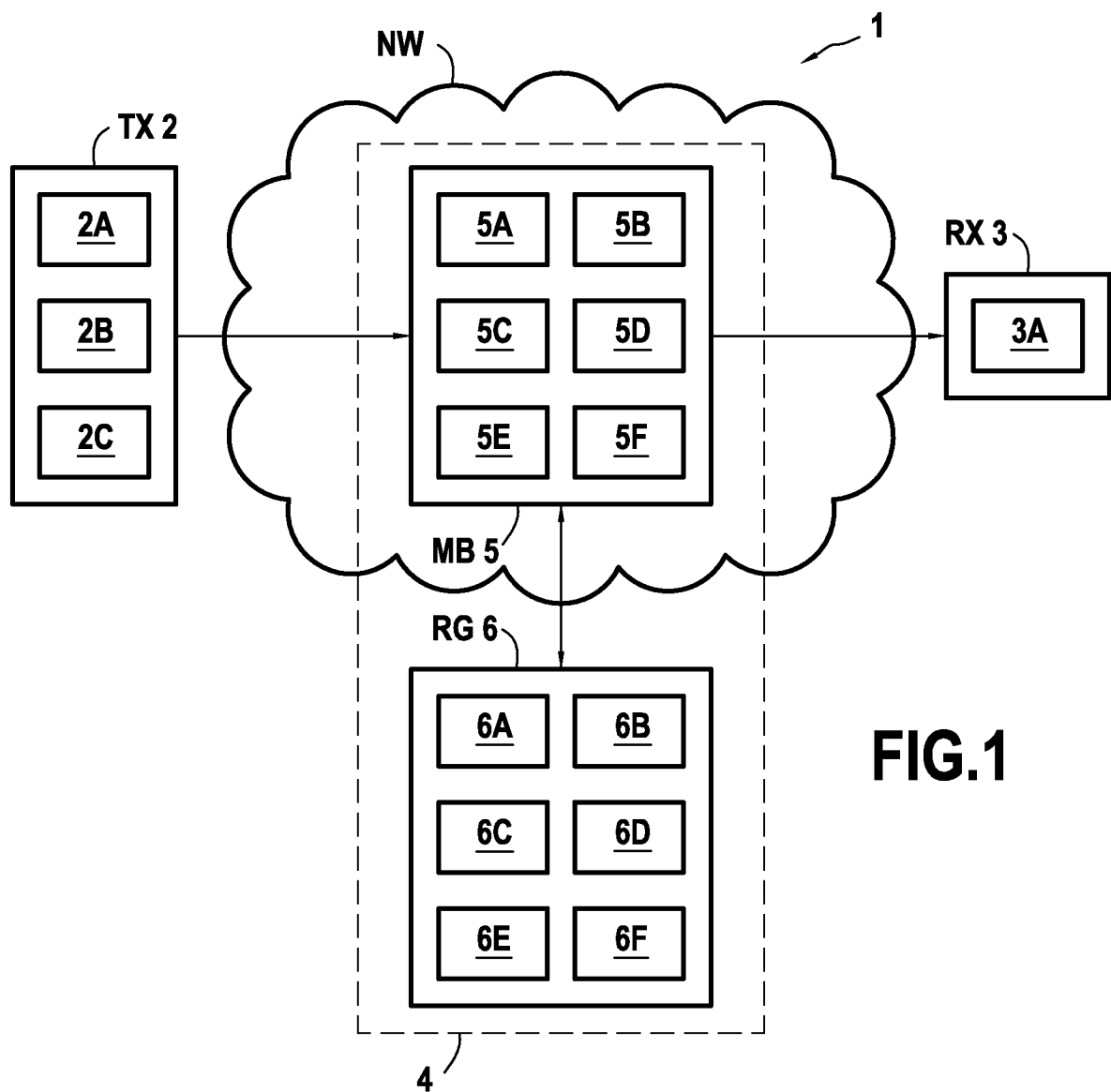


FIG.1

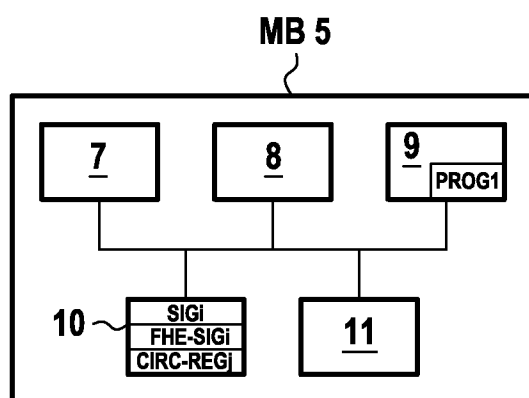


FIG.2

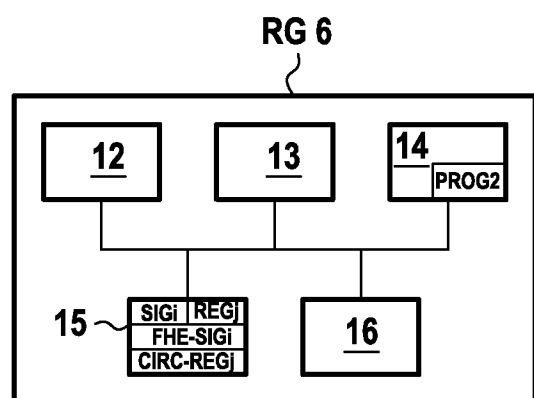
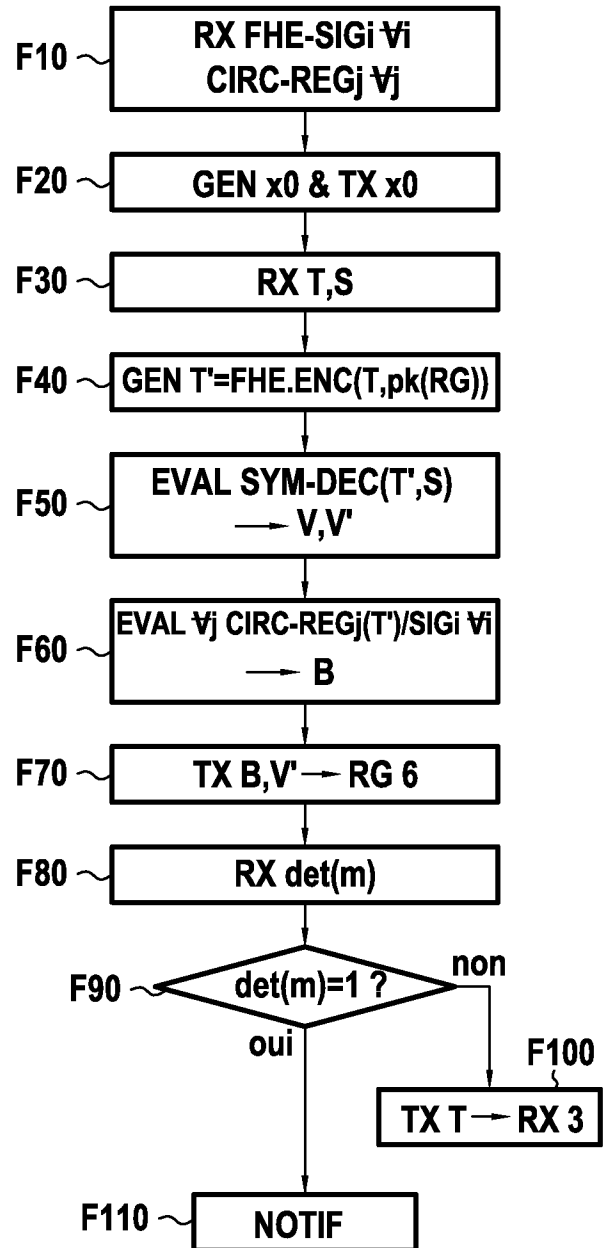
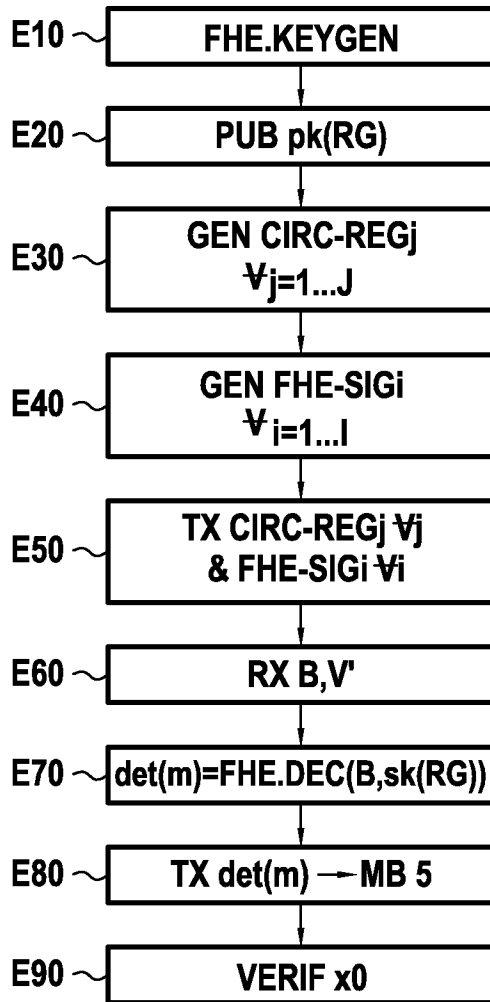
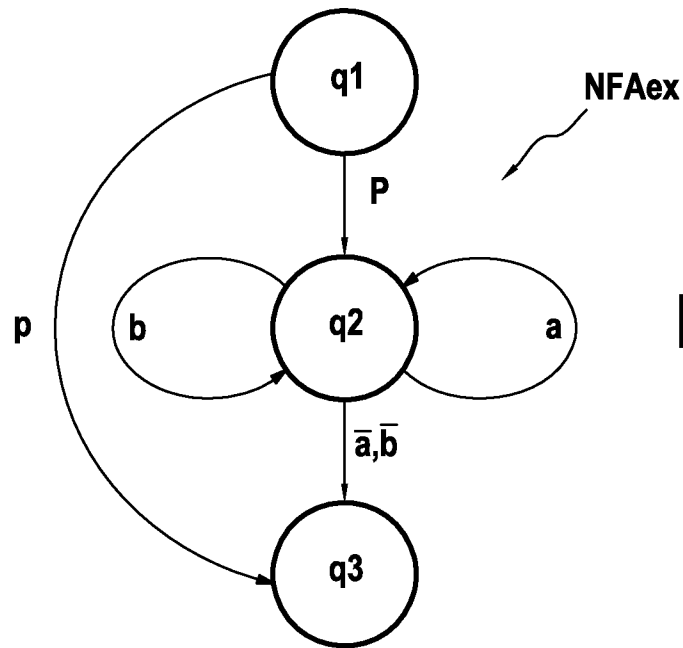
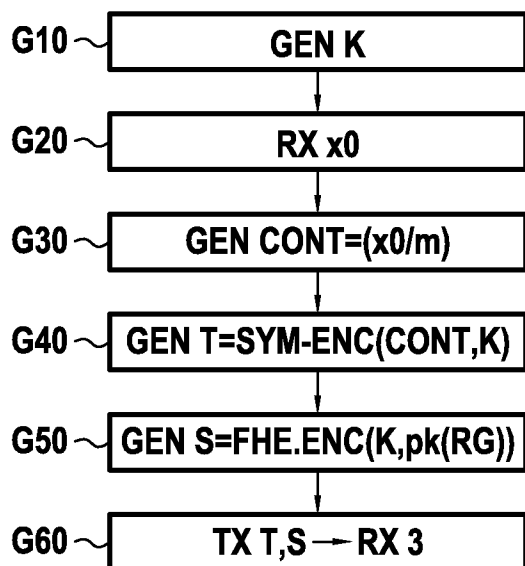
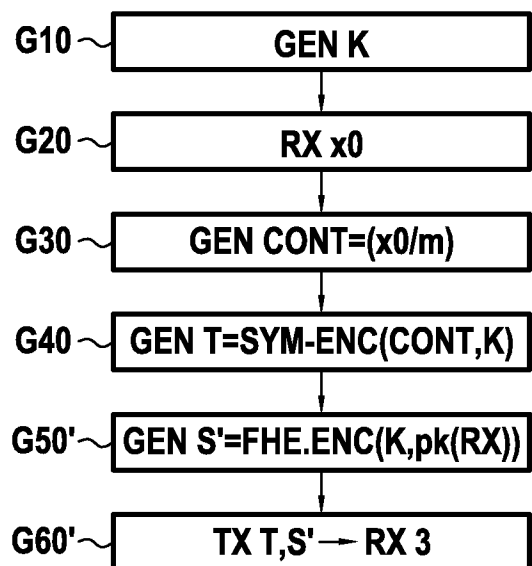


FIG.3

2/4



3/4

**FIG.6****FIG.7****FIG.8**

4/4

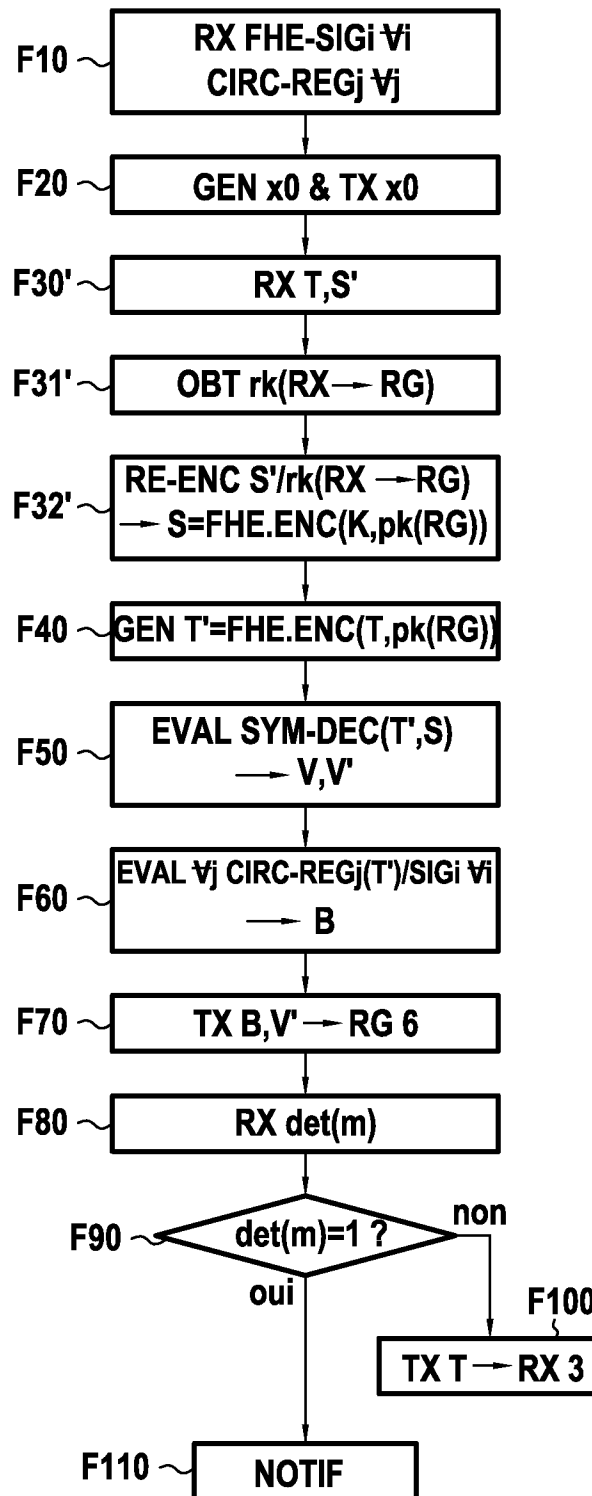


FIG.9

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/052690

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 H04L29/06
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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Hirohito Sasakawa: "Faster Pattern Matching Algorithms for Massive Regular Expression Matching and Its Applications", Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP, 1 February 2016 (2016-02-01), XP055378270, DOI: 10.14943/doctoral.k12183 Retrieved from the Internet: URL: http://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/61620/1/Hirohito_Sasakawa.pdf [retrieved on 2017-06-02] abstract Chapitre 1: "Introduction"; pages 1-5 Chapitre 5: "Oblivious Evaluation of Non-deterministic Finite Automata with Application to Privacy-Preserving Virus Genome Detection"; Sections 5.1 - 5.4.3; -/--	1-18



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

2 January 2018

Date of mailing of the international search report

11/01/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Di Felice, M

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/052690

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	pages 59-75 ----- LUCA MELIS ET AL: "Private Processing of Outsourced Network Functions: Feasibility and Constructions", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 25 January 2016 (2016-01-25), XP080680088, DOI: 10.1145/2876019.2876021 the whole document -----	1-18
	JUSTINE SHERRY ET AL: "BlindBox: Deep Packet Inspection over Encrypted Traffic", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20160411:194057, 11 April 2016 (2016-04-11), pages 1-22, XP061020597, cited in the application the whole document -----	1-18
	YUAN XINGLIANG ET AL: "Privacy-preserving deep packet inspection in outsourced middleboxes", IEEE INFOCOM 2016 - THE 35TH ANNUAL IEEE INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATIONS, IEEE, 10 April 2016 (2016-04-10), pages 1-9, XP032930160, DOI: 10.1109/INFOCOM.2016.7524526 the whole document -----	1-18

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2017/052690

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04L9/00 H04L29/06 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		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	Hirohito Sasakawa: "Faster Pattern Matching Algorithms for Massive Regular Expression Matching and Its Applications", Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP, 1 février 2016 (2016-02-01), XP055378270, DOI: 10.14943/doktoral.k12183 Extrait de l'Internet: URL: http://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/61620/1/Hirohito_Sasakawa.pdf [extrait le 2017-06-02] abrégé Chapitre 1: "Introduction"; pages 1-5 Chapitre 5: "Oblivious Evaluation of Non-deterministic Finite Automata with Application to Privacy-Preserving Virus Genome Detection"; Sections 5.1 - 5.4.3; -/--	1-18
☒ 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 2 janvier 2018		Date d'expédition du présent rapport de recherche internationale 11/01/2018
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Di Felice, M

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	pages 59-75 ----- LUCA MELIS ET AL: "Private Processing of Outsourced Network Functions: Feasibility and Constructions", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 25 janvier 2016 (2016-01-25), XP080680088, DOI: 10.1145/2876019.2876021 le document en entier -----	1-18
	JUSTINE SHERRY ET AL: "BlindBox: Deep Packet Inspection over Encrypted Traffic", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20160411:194057, 11 avril 2016 (2016-04-11), pages 1-22, XP061020597, cité dans la demande le document en entier -----	1-18
	YUAN XINGLIANG ET AL: "Privacy-preserving deep packet inspection in outsourced middleboxes", IEEE INFOCOM 2016 - THE 35TH ANNUAL IEEE INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATIONS, IEEE, 10 avril 2016 (2016-04-10), pages 1-9, XP032930160, DOI: 10.1109/INFOCOM.2016.7524526 le document en entier -----	1-18