ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) BREVET D'INVENTION

(11) N° de publication :
MA 39511 A1

(51) Cl. internationale :
H04L 9/00

(43) Date de publication :
31.05.2018

(21) N° Dépôt :
39511

(22) Date de Dépôt :
07.11.2016

(71) Demandeur(s) :
UNIVERSITE MOHAMMED V - RABAT, Avenue des Nations- Unies Agdal bp 8007 Rabat-Chellah (MA)

(72) Inventeur(s) :
EL YAHYAOUI Ahmed ; ECH-CHERIF El Kettani Mohamed Dafir

(74) Mandataire :
KARTIT ZAID

(54) Titre : **UN EFFICACE CRYPTOSYSTEME ENTIEREMENT HOMOMORPHE A BASE DES QUATERNIONS.**

(57) Abrégé : La présente invention concerne un cryptosystème entièrement homomorphe efficace basé sur une nouvelle transformée homomorphe et probabiliste entre l'anneau Z 2Z / (anneau des entiers résidus modulo 2) et l'anneau des entiers de Lipschitz modulaire. Notre cryptosystème est apte à traiter des messages clairs sous forme de bits en entrée et fournir des cryptogrammes sous forme de matrices de quaternions de Lipschitz modulo un grand nombre entier naturel pair $ d'une manière non déterministe. La sécurité dudit cryptosystème est basée sur la difficulté de résoudre un système d'équations polynomiales multi variées dans un anneau non commutatif. Ce cryptosystème permet de réduire davantage le temps de calcul des multiplications chez les algorithmes de cryptage entièrement homomorphe (EH), comme il permet de minimiser la taille d'une clé secrète et de réduire l'expansion des cryptogrammes.

RESUME

La présente invention concerne un cryptosystème entièrement homomorphe efficace basé sur une nouvelle transformée homomorphe et probabiliste entre l'anneau $\mathbb{Z}/2\mathbb{Z}$ (anneau des entiers résidus modulo 2) et l'anneau des entiers de Lipschitz modulaire. Notre cryptosystème est apte à traiter des messages clairs sous forme de bits en entrée et fournir des cryptogrammes sous forme de matrices de quaternions de Lipschitz modulo un grand nombre entier naturel pair $\boldsymbol{n}$ d'une manière non déterministe. La sécurité dudit cryptosystème est basée sur la difficulté de résoudre un système d'équations polynomiales multi variées dans un anneau non commutatif. Ce cryptosystème permet de réduire davantage le temps de calcul des multiplications chez les algorithmes de cryptage entièrement homomorphe (EH), comme il permet de minimiser la taille d'une clé secrète et de réduire l'expansion des cryptogrammes.

Titre : UN EFFICACE CRYPTOSYSTEME ENTIEREMENT HOMOMORPHE A BASE DES QUATERNIONS.

Domaine technique

La présente invention concerne un cryptosystème symétrique entièrement homomorphe (EH) et probabiliste basé sur l'utilisation des quaternions, plus particulièrement l'utilisation de l'anneau des entiers de Lipschitz. Ce cryptosystème utilise une transformation homomorphe entre l'anneau $\mathbb{Z}/2\mathbb{Z}$ (L'espace des clairs) et l'anneau des entiers de Lipschitz (l'espace des messages chiffrés) pour transformer un nombre binaire $\{0,1\}$ en un quaternion de Lipschitz avant de le chiffrer.

Etat antérieur

Après la conjecture de Rivest et al [R. Rivest, L. Adleman, and M. Dertouzos. "on data banks and privacy homomorphisms", Foundations of Secure Computation, pp 169-180, 1978], la conception d'un schéma de cryptage EH restait l'ambition de chaque cryptologue. L'apparition du cloud computing dans la dernière décennie a excité les efforts des chercheurs pour réaliser ce rêve. En effet, le cloud permet de mutualiser les structures de conservation et de traitement des données. Le traitement des données est considéré comme une force majeure du cloud car ce dernier dispose de puissances de calcul illimitées. Pour bénéficier de ces privilèges on arrive souvent à déléguer aux serveurs du cloud d'effectuer des calculs complexes sur des données privées. Avec le cryptage usuel, le fournisseur du cloud doit décrypter les données avant de faire les calculs demandés. Cependant, l'un des inconvénients de ceci est la préservation de la confidentialité entre le client et le fournisseur. Le cryptage homomorphe est une solution géniale pour ce problème, son idée est très simple : faire le calcul sur des données chiffrées. Si un cryptosystème permet un nombre limité d'opérations sur les données chiffrées, il est dit partiellement homomorphe. Le cas échéant un cryptosystème, permettant d'évaluer n'importe quel traitement sur les données chiffrées, est dit entièrement homomorphe.

Un cryptosystème EH est définit, en général, comme étant un quadruplet d'algorithmes (Gen, Enc, Dec, Eval), s'exécutant en temps polynomial, tels que :

- $Gen(\lambda)$: est un algorithme de génération de clés, prend en entrée un paramètre de sécurité λ et donne en sortie un pair de clés (sk, pk).
- $Enc(m, pk)$: est un algorithme de cryptage, prend en entrée un message clair m et une clé dite publique pk et donne en sortie un cryptogramme c.
- $Dec(c, sk)$: est un algorithme de décryptage, prend en entrée un cryptogramme c et une clé dite secrète sk et donne en sortie le message clair.
- $Eval(C, c_1, .., c_n)$: est un algorithme d'évaluation, prend en entrée un circuit C et des cryptogrammes $c_1, .., c_n$ et vérifie $Dec(Eval(C, c_1, .., c_n), sk) = C(m_1, \ldots, m_n)$.

Après avoir résisté à peu près trois décennies, la conjecture de Rivest et al a été enfin résolue en 2009 par Craig Gentry. Cette invention a fait l'objet du brevet **US20110110525.** En effet, Gentry a donné une renaissance aux recherches de la cryptographie homomorphe par la conception d'un schéma de cryptage EH considéré sémantiquement sûr. La conception de Gentry peut être récapitulée en trois grandes étapes principales :

- Somewhat Homomorphic Encryption Scheme (SWHE) : Gentry part d'un schéma dit SWHE ou simplement homomorphe qui supporte un nombre limité de multiplication homomorphe.
- Squashing du circuit de décryptage : Gentry réduit la complexité du circuit de déchiffrement en publiant un ensemble de vecteurs dont la somme d'une partie d'entre eux est égale à la clé secrète. Ce schéma dit '*squashé*' peut évaluer, en plus de ses capacités SWHE, une porte NAND.
- Bootstrapping : la procédure du bootstrap inventée par Gentry consiste en l'avaluation du circuit de décryptage plus le NAND pour obtenir un schéma dit 'leveled' FHE qui permet d'évaluer n'importe quel circuit avec une profondeur du circuit définit au départ.

Ce premier schéma est basé sur l'ajout de bruit au clair pour obtenir l'homomorphie du cryptosystème. L'inconvénient majeur des schémas bruités est la croissance du bruit après chaque manipulation du cryptogramme (addition et/ou multiplication). En effet, afin de garder la capacité de décryptage on doit contrôler et réduire le bruit généré après chaque traitement. Le contrôle du bruit dans ce type schémas augmente leur complexité spatiale et temporelle ce qui se traduit par une lenteur des calculs (surtout pendant le bootstrapping) et une gourmandise de l'espace mémoire demandé pour le stockage des résultats (amplification de bruit). Une chose qui influence la pratique et l'application du chiffrement EH à la vie quotidienne. Toutes ces causes ont encouragé les chercheurs de trouver d'autres frameworks de conception de schémas de cryptage EH afin de rendre applicable le chiffrement EH.

Parmi les tentatives les plus éminentes de simplification des schémas de cryptage EH, on trouve le cryptosystème MORE. Ce dernier a fait l'objet du brevet WO2014016795A2. C'est un cryptosystème symétrique basé sur l'arithmétique modulaire dont l'homomorphie découle des opérations matricielles usuelles, sa multiplication et son addition sont la multiplication et l'addition matricielles. Dans le schéma de cryptage MORE, l'espace des clairs est l'anneau $\mathbb{Z}/n\mathbb{Z}$ (anneau des entiers résidus modulo n) où n est un modulo choisi comme dans le célèbre algorithme RSA alors que l'espace des cryptogrammes est l'anneau des matrices modulaires $M_2(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$. La clé secrète de ce cryptosystème est une matrice inversible $K \in M_2(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$ choisie aléatoirement par le client et conservée confidentielle avec son inverse K^{-1}.

Toutefois, le cryptosystème MORE ne résiste pas aux attaques de types IND-CPA(Indistinguishability under Chosen Plaintext Attack) et IND-KPA(Indistinguishability under Known Plaintext Attack). En effet, si un tiers de mauvaise foi ait accès à un seul clair et à son cryptogramme il pourra déchiffrer tout message chiffré par la suite sans avoir trouvé la clé secrète. Le cryptosystème MORE a été cryptanalysé plusieurs fois [http://eprint.iacr.org/2014/250.pdf, https://www.academia.edu/26297806/].

Une seconde tentative, pour pallier les failles de sécurité du schéma MORE et construire un cryptosystème EH, est récemment due à Wang et Li [http://eprint.iacr.org/2015/641.pdf]. Les deux auteurs ont gardé presque la même conception de MORE sauf qu'ils ont proposé de changer l'anneau $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ par un anneau $\boldsymbol{R}$ non commutatif et ils ont utilisé des matrices carrées d'ordre 3 au lieu des matrices d'ordre 2. Malgré l'utilisation d'un anneau non commutatif $\boldsymbol{R}$, les messages clairs restent toujours des nombres qui commutent avec les éléments de $\boldsymbol{R}$.

Par conséquent une attaque du schéma de Wang et Li est donné par Kristian Gjøsteen et Martin Strand dans [http://eprint.iacr.org/2016/105.pdf]. En effet, d'après ces auteurs: pour attaquer le cryptosystème de Wang-Li, nous avons seulement besoin de distinguer les cryptages de 0 à partir d'un cryptage aléatoire.

Les deux auteurs ont observé que la diagonale de la matrice cryptogramme détermine complétement l'inversibilité de ladite matrice, car un cryptogramme de ''0'' ne peut être inversible. Donc, avec une grande probabilité, on peut distinguer les éléments inversibles de l'anneau ***R*** des éléments non-inversibles. Si l'anneau R est à division, alors il n'y a pas d'autres éléments non-inversibles que ''0''. Enfin, en utilisant une variante de la décomposition LU adaptée aux anneaux non commutatifs on peut calculer efficacement la matrice clé secrète de l'algorithme.

D'après ce qui est venu avant, on peut signaler qu'il existe deux types de construction de cryptosystèmes EH :

- Une construction à base de bruit qui utilise la technique du bootstrap comme elle est décrite dans le framework de Gentry. L'avantage de cette construction est sa sureté, vu que les schémas conçu jusqu'à présent (à partir de cette démarche) sont basés sur des problèmes mathématiques issus de la théorie des réseaux euclidiens, qui demeure quand même une théorie immune et complexe. Alors que son inconvénient majeur réside dans la lenteur de ses opérations (surtout le bootstrap) et la complexité de ses algorithmes.
- Une construction sans bruit qui utilise les opérations matricielles comme il est décrit dans le framework MORE. Cette construction a l'avantage d'être très simple, facile à implémenter et fournit des opérations très rapides pour tout traitement sur les cryptogrammes. L'inconvénient capital de cette construction réside dans la sureté des schémas conçus jusqu'à présent. Les schémas conçus à base du framework MORE ont fait l'objet des attaques de type IND-CPA et IND-KPA. Un second désavantage issu du cryptosystème MORE c'est qu'il est juste partiellement homomorphe même si ses auteurs déclarent son entière homomorphie dans le brevet WO2014016795A2. En effet, ce schéma est incapable de manipuler tout type de traitement sur les cryptogrammes. Prenons à titre d'exemple le cryptogramme $C = MORE(m)$ du message clair $m = N - 1$, où N est le modulo utilisé dans ce cryptosystème, si on calcule $C' = C^2$ et on décrypte le résultat on obtient $m' = 1 \neq m^2 = (N-1)^2$, car les opérations sont effectuées modulo N.

Un premier objectif de la présente invention est d'améliorer le temps d'exécution des cryptosystèmes EH. Pour cette raison nous allons adopter le framework MORE comme base de construction au lieu du framework de Gentry qui exige une étape de bootstrap très lente. Notre second objectif est de franchir l'entrave saisissante de la sécurité dans les cryptosystèmes antérieurs. Nous proposons un cryptosystème EH plus sûr que ses précédents et résistant aux attaques IND-CPA et IND-KPA. Finalement nous visons que notre cryptosystème soit entièrement homomorphe, c'est-à-dire il permet d'exécuter tout type de traitement sur les messages chiffrés aux antipodes du schéma MORE. Par conséquent, le choix d'un espace de clairs bien adapté est primordial pour concrétiser l'entière homomorphie de notre cryptosystème. Nous envisageons utiliser l'espace binaire, sanctionné par les deux opérations XOR et AND, (c'est l'anneau $\mathbb{Z}/2\mathbb{Z}$) comme espace de clairs pour notre schéma de cryptage. En plus de çà, nous utilisons une transformée homomorphe qui convertit un bit en un quaternion de Lipschitz. Cela permet de randomiser les bits afin de garantir que la diagonale ne donne aucune information utile sur le clair (éviter l'attaque du cryptosystème de Li-Wang).

Notre cryptosystème résiste aux attaques IND-CPA et IND-KPA par la non-commutativité de l'anneau des quaternions de Lipschitz et par l'utilisation d'un espace de clair plus réduit (l'anneau $\mathbb{Z}/2\mathbb{Z}$). Il hérite son homomorphie d'une part des opérations matricielles et d'autre part d'une nouvelle transformation homomorphe, entre l'anneau $\mathbb{Z}/2\mathbb{Z}$ et l'anneau des entiers de Lipschitz, que nous avons inventée. Son entière homomorphie est obtenue par la manipulation de ces entiers de Lipschitz à l'aide d'un modulo pair $(n = 2.p.q)$.

Description des figures

La figure 1 représente, en général, le fonctionnement d'un cryptosystème EH. Elle explique comment on peut utiliser l'algorithme Eval dans un contexte de calcul à données chiffrées.

La figure 2 représente les deux chaînes de cryptage et de décryptage pour notre cryptosystème EH.

La figure 3 représente comment on peut utiliser notre cryptosystème dans une situation de délégation de calcul chez un cloud.

Le corps des quaternions $\mathbb{H}$

Un quaternion est un nombre dans un sens généralisé. Les quaternions englobent les nombres réels et complexes dans un système de nombres où la multiplication n'est plus une loi commutative.

Les quaternions furent introduits par le mathématicien irlandais William Rowan Hamilton en 1843. Ils trouvent aujourd'hui des applications en mathématiques, en physique, en informatique et en sciences de l'ingénieur.

Mathématiquement, l'ensemble des quaternions $\mathbb{H}$ est une algèbre associative non-commutative sur le corps des nombres réels $\mathbb{R}$ engendrée par trois éléments i, j *et* k satisfaisant les relations: $i^2 = j^2 = k^2 = i.j.k = -1$. Concrètement, tout quaternion q s'écrit de manière unique sous la forme : $q = a + bi + cj + dk$ où a, b, c *et* d sont des nombres réels.

Les opérations d'addition et de multiplication par un scalaire réel se font termes à termes, alors que La multiplication entre deux quaternions se fait termes à termes en respectant la non-commutativité et les règles propres à $, j$ *et* k. Ainsi pour $q = a + bi + cj + dk$ et $q' = a' + b'i + c'j + d'k$ on a $qq' = a_0 + b_0 i + c_0 j + d_0 k$ avec: $a_0 = aa' - (bb' + cc' + dd')$, $b_0 = ab' + a'b + cd' - c'd$, $c_0 = ac' - bd' + ca' + db'$ et $d_0 = ad' + bc' - cb' + a'd$.

Le quaternion $\bar{q} = a - bi - cj - dk$ est le conjugué de q. $|q| = \sqrt{q\bar{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$ est le module de q. La partie réelle de q est $Re(q) = \frac{q+\bar{q}}{2} = a$ et la partie imaginaire est $Im(q) = \frac{q-\bar{q}}{2} = bi + cj + dk$.

Un quaternion q est inversible si et seulement si son module est non nulle, et on a $q^{-1} = \frac{1}{|q|^2}\bar{q}$.

Forme réduite d'un quaternion :

On peut représenter un quaternion d'une manière plus économique, ce qui allège considérablement les calculs et met en valeur des résultats intéressants. En effet, il est aisé de voir que $\mathbb{H}$ est un $\mathbb{R}$-espace vectoriel de dimension 4, dont $(1, i, j, k)$ constitue une base orthonormale directe. On peut donc séparer la composante réelle des composantes pures, et on a pour $q \in \mathbb{H}, q = (a, \boldsymbol{u})$ avec $\boldsymbol{u}$ vecteur de $\mathbb{R}^3$. On a donc pour $q = (a, \boldsymbol{u}), q' = (a', \boldsymbol{v}) \in \mathbb{H}$ et $\lambda \in \mathbb{R}$:

1. $q + q' = (a + a', \boldsymbol{u} + \boldsymbol{v})$ et $\lambda q = (\lambda a, \lambda \boldsymbol{u})$
2. $qq' = (aa' - \boldsymbol{u}.\boldsymbol{v}, a\boldsymbol{v} + a'\boldsymbol{u} + \boldsymbol{u} \wedge \boldsymbol{v})$ où $\wedge$ est le produit vectoriel de $\mathbb{R}^3$.
3. $\bar{q} = (a, -\boldsymbol{u})$ et $|q|^2 = a^2 + \boldsymbol{u}^2$.

Anneau des entiers de Lipschitz

L'ensemble des quaternions définit comme suit : $\mathbb{H}(\mathbb{Z}) = \{q = a + bi + cj + dk/\mathrm{a,b,c,d} \in \mathbb{Z}\}$ possède une structure d'anneau appelé anneau des entiers de Lipschitz. $\mathbb{H}(\mathbb{Z})$ est trivialement non-commutatif.

Pour $n \in \mathbb{N}^*$, l'ensemble des quaternions: $\mathbb{H}(\mathbb{Z}/n\mathbb{Z}) = \{q = a + bi + cj + dk/\mathrm{a,b,c,d} \in \mathbb{Z}/n\mathbb{Z}\}$ possède une structure d'anneau non-commutatif.

Un quaternion modulaire de Lipschitz $q \in \mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$ est inversible si et seulement si son module est premier avec $\boldsymbol{n}$, c'est-à-dire $|q|^2 \wedge n = 1$.

Matrices quaternioniques de $\mathbb{M}_2(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$:

L'ensemble des matrices $\mathbb{M}_2(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$ décrit les matrices à quatre entrées (deux lignes et deux colonnes) qui sont des quaternions de $\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$. Cet ensemble possède une structure d'anneau non commutatif.

Il existe deux manières de multiplier les matrices quaternioniques : le produit hamiltonien, qui respecte l'ordre des facteurs, et le produit octonionique, qui ne le respecte pas.

- Le produit hamiltonien est défini comme pour toutes les matrices à coefficients dans un anneau (non nécessairement commutatif). Par exemple :

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}, \quad V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \Rightarrow UV = \begin{pmatrix} u_{11}v_{11} + u_{12}v_{21} & u_{11}v_{12} + u_{12}v_{22} \\ u_{21}v_{11} + u_{22}v_{21} & u_{21}v_{12} + u_{22}v_{22} \end{pmatrix}$$

- Le produit octonionique ne respecte pas l'ordre des facteurs : sur la diagonale principale, il y a commutation des deuxièmes produits et sur la deuxième diagonale il y a commutation des premiers produits.

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}, \quad V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} \Rightarrow UV = \begin{pmatrix} u_{11}v_{11} + v_{21}u_{12} & v_{12}u_{11} + u_{12}v_{22} \\ v_{11}u_{21} + u_{22}v_{21} & u_{21}v_{12} + v_{22}u_{22} \end{pmatrix}$$

Dans notre rapport nous allons adopter le produit hamiltonien comme opération de multiplication des matrices quaternioniques.

Complément de Schur et inversibilité des matrices quaternioniques

Soit $\mathcal{R}$ un anneau associatif quelconque, une matrice $M \in \mathcal{R}^{n\times n}$ est dite inversible si $\exists N \in \mathcal{R}^{n\times n}$ tel que $MN = NM = I_n$ où N est nécessairement unique.

La méthode du complément de Schur est un outil très puissant pour le calcul des inverses des matrices dans des anneaux. Soit $M \in \mathcal{R}^{n\times n}$ une matrice par bloc vérifiant : $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ telle que $A \in \mathcal{R}^{k\times k}$.

Supposant A est inversible, on a : $M = \begin{pmatrix} I_k & 0 \\ CA^{-1} & I_{n-k} \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A_s \end{pmatrix}\begin{pmatrix} I_k & A^{-1}B \\ 0 & I_{n-k} \end{pmatrix}$ où $A_s = D - CA^{-1}B$ est le complément de Schur de A dans M.

L'inversibilité de A assure que la matrice M est inversible si est seulement si A_s l'est. L'inverse de M est: $M^{-1} = \begin{pmatrix} I_k & -A^{-1}B \\ 0 & I_{n-k} \end{pmatrix}\begin{pmatrix} A^{-1} & 0 \\ 0 & A_s^{-1} \end{pmatrix}\begin{pmatrix} I_k & 0 \\ -CA^{-1} & I_{n-k} \end{pmatrix} = \begin{pmatrix} A^{-1} + A^{-1}BA_s^{-1}CA^{-1} & -A^{-1}BA_s^{-1} \\ -A_s^{-1}CA^{-1} & A_s^{-1} \end{pmatrix}$.

Pour une matrice quaternionique $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{R}^{2\times 2} = \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$ où le quaternion a est inversible ainsi que son complément de Schur $a_s = d - ca^{-1}b$ on a M est inversible et:

$$M^{-1} = \begin{pmatrix} a^{-1} + a^{-1}ba_s^{-1}ca^{-1} & -a^{-1}ba_s^{-1} \\ -a_s^{-1}ca^{-1} & a_s^{-1} \end{pmatrix} \qquad (**)$$

Donc pour générer aléatoirement une matrice quaternionique inversible, il suffit de : (***)

- Choisir aléatoirement trois quaternions a, b *et* c dont a est inversible.
- Sélectionner aléatoirement le quatrième quaternion d de telle sorte que le complément de Schur $a_s = d - ca^{-1}b$ de a dans M soit inversible.

Description de la transformée et du cryptosystème

- **Transformée homomorphe entre $(\mathbb{Z}/2\mathbb{Z}, XOR, AND)$ et $(\mathbb{H}(\mathbb{Z}), +, \times)$** (*)

Tout bit $\sigma \in \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ peut être transformé en un quaternion de Lipschitz selon une transformée homomorphe dont les opérations sur les quaternions conservent celles sur les bits. On peut donner cette transformée comme suit :

$bitToQuatern$: $\sigma \in \mathbb{Z}/2\mathbb{Z} \mapsto bitToQuatern(\sigma) = m + 2\ell i + pj + qk \in \mathbb{H}(\mathbb{Z})$ tels que m, ℓ, p, q sont des entiers relatifs choisis aléatoirement respectant les deux conditions: $m \equiv \sigma[2]$ et $p \equiv q[2]$. La transformée inverse qui sera nommée $quaternToBit$ est donnée par : $quaternToBit(q) = Re(q)[2]$.

On peut vérifier facilement l'homomorphie de la transformée $bitToQuatern$:

- pour l'addition on a bien : $bitToQuatern(\sigma) + bitToQuatern(\sigma') = bitToQuatern(\sigma XOR \sigma')$.
- Pour la multiplication, en passant à la notation réduite des quaternions, on a $bitToQuatern(\sigma) * bitToQuatern(\sigma') = (m, \boldsymbol{u}) * (m', \boldsymbol{v}) = (mm' - \boldsymbol{u}.\boldsymbol{v}, m\boldsymbol{v} + m'\boldsymbol{u} + \boldsymbol{u} \wedge \boldsymbol{v})$,donc on peut vérifier facilement que $mm' - \boldsymbol{u}.\boldsymbol{v} \equiv (\sigma AND \sigma')[2]$ et que $m\boldsymbol{v} + m'\boldsymbol{u} + \boldsymbol{u} \wedge \boldsymbol{v}$ a bien la forme $(2L, P, Q)$ tel que $P \equiv Q[2]$. Alors $bitToQuatern(\sigma) * bitToQuatern(\sigma') = bitToQuatern(\sigma AND \sigma')$.

Le fait que la réduction modulo un nombre pair d'un entier relatif conserve sa parité (c'est-à-dire $\boxed{\forall (m,n) \in \mathbb{Z} \times \mathbb{N}^*, m \bmod 2 = (m \bmod 2n) \bmod 2}$), permet de changer l'ensemble d'arrivée $\mathbb{H}(\mathbb{Z})$ de la transformée $bitToQuatern$ par l'ensemble $\mathbb{H}(\mathbb{Z}/2n\mathbb{Z})$ en conservant son homomorphie et en obtenant les mêmes propriétés. Dans le reste de ce rapport la transformée $bitToQuatern$ représente la transformée $bitToQuatern$ dont l'ensemble d'arrivée est $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ pour un entier n qui sera définit.

Remarque : toute permutation σ du triplet $(2\ell, p, q)$ engendre une transformée $bitToQuatern_\sigma$ ayant les même propriétés que la transformée $bitToQuatern$. La transformée inverse pour $bitToQuatern_\sigma$ reste inchangeable.

- **Cryptosystème entièrement homomorphe et efficace**

On se place dans un contexte où Bob veut stocker des données confidentielles dans un cloud très puissant mais non confiant. Bob aura besoin plus tard de faire des traitements complexes, sur ses données, dont il ne dispose pas des puissances de calcul nécessaires pour les effectuer. A ce niveau il pense, à priori, au chiffrement de ses données sensibles pour éviter toute action frauduleuse. Mais le chiffrement usuel, qu'il connaisse, ne permet pas au cloud de traiter ses requêtes de calcul sans avoir déchiffré les données stockées au préalable, ce qui met en cause leur confidentialité. Bob demande s'il

existe un type de chiffrement pratique et efficace permettant de traiter ses données sans les révéler au cloud. La réponse à la demande de Bob est favorable, en effet depuis 2009 il existe des cryptosystèmes dits entièrement homomorphes, dont le principe est assez simple : faire les calculs sur les données chiffrées sans penser à aucun préalable déchiffrement.

Pour être entièrement homomorphe, il suffit qu'un cryptosystème permette de réaliser les deux opérations d'addition et de multiplication une multitude de fois sur les cryptogrammes. Depuis leur première apparition en 2009, les cryptosystèmes EH permettent de réaliser facilement les additions alors que la multiplication reste très couteuse en terme du temps de calcul et épuisante en terme du bruit généré. Réellement, en moyen, une addition double le bruit d'un message chiffré alors qu'une multiplication l'enlève au carré.

Afin de bénéficier agréablement de l'avancée technologique du cloud et externaliser ses calculs lourds confortablement, Bob a besoin d'un cryptosystème EH robuste en termes de sécurité, dont les opérations d'addition et de multiplication se font en un temps judicieux et dont le bruit généré lors d'un traitement est maitrisable.

Pour aider Bob à profiter pleinement des puissances du cloud, nous avons inventé un cryptosystème symétrique probabiliste EH sans bruit. Les opérations d'addition et de multiplication ne génèrent aucun bruit. La multiplication est très rapide et se fait en moins d'une milliseconde. La sécurité du cryptosystème est basée sur la difficulté de résoudre un système d'équations multi-variées dans un anneau non commutatif.

On peut décrire notre cryptosystème comme suit :

Génération de clé :

-Bob génère aléatoirement deux grands nombres premiers p et q.

-puis, il calcule $\boldsymbol{n} = 2.\mathrm{p}.\mathrm{q}$.

-Bob génère aléatoirement une matrice inversible $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$ comme il est décrit dans (***).

-Bob calcule l'inverse de K, qui sera noté K^{-1}, comme il est décrit dans (**).

-la clé secrète est (K, K^{-1}).

Chiffrement :

Soit $\sigma \in \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ un message clair. Pour chiffrer σ Bob procède comme suit :

-A l'aide de la transformée $bitToQuatern$, décrite dans (*), Bob transforme σ en un quaternion $m = bitToQuatern(\sigma) \in \mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$.

-Bob génère une matrice $M = \begin{pmatrix} m & r_1 \\ 0 & r_2 \end{pmatrix} \in \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$ Tels que r_1 et $r_2 \in \mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$ sont générés aléatoirement.

-Le cryptogramme de σ est : $C = Enc(\sigma) = KMK^{-1} \in \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}))$.

Déchiffrement :

Soit un cryptogramme $C \in \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$. Pour déchiffrer C, Bob procède comme suit :

-Il calcule $M = K^{-1}CK$.

-Puis il prend la première entrée de la matrice $m = (M)_{1,1}$.

-Enfin il retrouve son message clair en calculant $\sigma = quaternToBit(m)$.

Addition et multiplication :

Soient $\sigma_1 et\ \sigma_2$ deux messages clairs et $C_1 = Enc(\sigma_1) et\ C_2 = Enc(\sigma_2)$ leurs cryptogrammes respectivement.

On peut vérifier facilement, grâce à la transformée $bitToQuatern$, que :

(1) $C_{mult} = C_1 + C_2 = Enc(\sigma_1) + Enc(\sigma_2) = Enc(\sigma_1 \oplus \sigma_2)$. Où $\oplus$ représente le XOR informatique.
(2) $C_{add} = C_1 . C_2 = Enc(\sigma_1).Enc(\sigma_2) = Enc(\sigma_1 \otimes \sigma_2)$. Où $\otimes$ représente le AND.

Pour notre cryptosystème, la réduction de quaternions modulo un grand nombre n a l'avantage de donner un cryptosystème sans expansion de bruit. Mais si on utilise un modulo impair, l'entière homomorphie peut être mise en cause. En effet, un modulo impair ne préserve pas, en général, la parité des entiers après un traitement (additions et/ou multiplications) ce qui donne un cryptosystème partiellement homomorphe alors qu'un modulo pair préserve toujours la parité des entiers et donne un schéma entièrement homomorphe.

Version asymétrique :

Notre cryptosystème admet une version asymétrique en lui appliquant la transformation de Rothblum [https://www.iacr.org/archive/tcc2011/65970216/65970216.pdf].

Utilité de l'invention

Le champ d'application de notre cryptosystème est très vaste. Son utilité dans le domaine du cloud computing est évidente. Parmi les applications de notre cryptosystème on trouve:

1. En général, la délégation de calculs complexes sur des données sensibles à un cloud puissant mais non confiant. En effet, l'externalisation de calcul devient une solution efficace pour ceux qui possèdent des données gigantesques hébergées chez un sous-traitant. Ces données sont confidentielles dans la majorité des cas et nécessitent une manipulation particulière. Grâce aux alternatives de calcul qu'offre notre cryptosystème, les clients peuvent stocker leurs données chiffrées et demander aux sous-traitants de faire des calculs sur ces données à la demande. En particulier ce cryptosystème peut être très utile, en délégation de calcul, dans les deux cas suivants:
   - ❖ Chiffrer des données d'un opérateur bancaire avant leur stockage dans un cloud. Assurément, le secteur bancaire est réputée pour le volume et la vitesse des données qu'il produit, transporte et stocke. La nature des données d'une banque telle que les numéros des comptes bancaires des clients, les sommes d'argent et les transactions effectuées sont d'une grande sensibilité alors que les fournisseurs du cloud ne fournissent aucune garantie sur la protection de la vie privée et sur la confidentialité de ce type de données. Le stockage des masses de données dans un cloud est d'un gain très important pour une banque. La possibilité de faire des traitements sur ces données, sans les divulguer, en un temps pratique en épuisant moins de

ressources est très utile. Notre cryptosystème est une solution adéquate à cette problématique. Il permet, pour une banque, de stocker ses données chiffrées dans un cloud avec la possibilité d'effectuer n'importe quel traitement sans procéder à leur déchiffrement.

- ❖ Chiffrer des données médicales des patients avant leur stockage dans un cloud. En effet dans un cloud médical, les données des patients tels que l'identifiant biométrique, le numéro de la sécurité sociale, l'âge et l'état de santé sont des données à caractère personnel. L'exploitation de ces données à des fins de recherches médicales et en pharmacovigilance lève la question de confidentialité de ce type de données, avec les règles de déontologie et de respect de la vie privée. Dans ce contexte, on n'est intéressé que par les résultats des traitements qu'on peut effectuer sur ces données. Notre schéma de cryptage permet de faire des traitements sur les données médicales et fournir les résultats demandés tout en préservant la confidentialité des données et la vie privée des patients.

2. Le retrait d'information privé : En cryptographie, le retrait d'informations privé (RIP) est un protocole qui permet à un utilisateur de récupérer un élément d'une base de données sans révéler au serveur quel élément a été récupéré. Le cryptage homomorphe permet facilement de réaliser tels protocoles. Notre cryptosystème possède la propriété homomorphique qui lui permet de réaliser facilement le protocole RIP.
3. Le calcul multi-parties : dans les systèmes de calcul multi-parties, plusieurs parties sont intéressées à calculer une fonction commune, sans arriver à divulguer leurs données privées. La fonction qui doit être calculée est publiquement connue alors que les entrées individuelles des différents utilisateurs doivent rester inconnues pour les autres parties du système. Ce problème provient du problème de calcul avec les données chiffrées, d'où l'utilité de l'usage de la cryptographie homomorphe. La version asymétrique de notre cryptosystème permet de mettre en œuvre les calculs multipartis.
4. Le vote électronique : Le vote électronique est un cas spécial de délégation de calcul à un tiers capable de calculer le résultat des élections sans divulguer les identités des différents candidats. Dans cette situation le cryptage homomorphe permet aux autorités électorales de compter les votes et présenter les résultats définitifs sans passer par le processus du déchiffrement des votes et les compter après. Dans un système de vote basé sur le cryptage homomorphe les électeurs sont autorisés juste à incrémenter un décompte chiffré par 1 (indiquant un vote pour le candidat) où 0 (indiquant le cas du non vote). Lors des élections où chaque électeur vote pour un des candidats parmi ℓ candidats, les électeurs modifient les pointages cryptés en ajoutant un vecteur ℓ bits, où exactement une entrée est 1 et le reste sont tous des 0. Et ils sont incapables de modifier les compteurs de toute autre manière. La version asymétrique de notre cryptosystème permet de mettre en œuvre un système de vote électronique sécurisé.

Revendications

1. Il s'agit d'un cryptosystème symétrique probabiliste entièrement homomorphe et rapide dont l'espace des clairs est {0,1} muni des opérations ***XOR et AND*** alors que les cryptogrammes sont des matrices de quaternions de Lipschitz modulo un grand nombre entier naturel pair $\boldsymbol{n}$.
2. Un cryptosystème symétrique probabiliste entièrement homomorphe et rapide caractérisé en ce que dans un mode de réalisation les messages en clair selon la revendication (1) sont codés par une transformée homomorphe inversible $bitToQuatern$ entre $(\mathbb{Z}/2\mathbb{Z}, \boldsymbol{XOR}, \boldsymbol{AND})$ et $(\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}), +, \times)$. Cette transformée permet de conserver les deux opérations de ***XOR et AND*** sur les bits et de les remplacer par les opérations d'addition et de multiplication sur les quaternions de Lipschitz modulaires$\mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$. Pour coder un bit σ par un quaternion de Lipschitz modulaire on procède comme suit :
   -Choisir aléatoirement un entier $m \in \mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ tel que $m \equiv \sigma[2]$.
   -Choisir aléatoirement un entier $l \in \mathbb{Z}/\boldsymbol{n}\mathbb{Z}$.
   -Choisir aléatoirement deux entiers $p, q \in \mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ tels que $p \equiv q[2]$.
   -On a $bitToQuatern(\sigma) = m + 2\ell i + pj + q\not{k} \in \mathbb{H}(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})$.
   Ladite transformée se réalise, autrement, par toute permutation du triplet $(2\ell, p, q)$ et garde les mêmes propriétés d'homomorphie.
3. Un cryptosystème symétrique probabiliste entièrement homomorphe et rapide caractérisé en ce que dans un mode de réalisation la transformée inverse $quaternToBit$ selon la revendication (2) permettant de retrouver un bit σ, randomisé à partir de la transformée $bitToQuatern$ où résultat d'un traitement (additions et/ou multiplications) de plusieurs bits randomisés à partir de la transformée $tToQuatern$. La transformée inverse est calculée comme suit : $\sigma = quaternToBit(q) = Re(q)[2]$. Où q est un quaternion de Lipschitz obtenu selon la revendication (2) et Re est sa partie réelle.
4. Un cryptosystème symétrique probabiliste entièrement homomorphe et rapide selon la revendication (1) caractérisé en ce que la matrice quaternionique K, choisie aléatoirement, forme la clé secrète et en ce que cette matrice doit être inversible.
5. Un cryptosystème symétrique probabiliste entièrement homomorphe et rapide selon les revendications (1) et (4) caractérisé en ce que dans un mode de réalisation, le chiffrement d'un binaire (0 où 1) qui représente le message en clair se fait en la transformation de ce binaire en un quaternion selon la revendication (2), le résultat de cette transformation est inséré à la première entrée d'une matrice quaternionique triangulaire supérieure d'ordre deux dont les deux entrées restantes sont des quaternions choisies aléatoirement (c'est la matrice M). La continuation du chiffrement se fait en multipliant la matrice M par la matrice K à gauche et par la matrice K^{-1} à droite. La matrice résultante du produit KMK^{-1} constitue le message chiffré.
6. Un cryptosystème symétrique probabiliste entièrement homomorphe selon les revendications précédentes caractérisé en ce que dans un mode de réalisation, le déchiffrement d'un cryptogramme C (qui est une matrice quaternionique) se fait en multipliant la matrice C par la matrice K^{-1} à gauche et par la matrice K à droite. La continuation du déchiffrement se fait en prenant la première entrée de la matrice résultante du produit $K^{-1}CK$ et en lui appliquant la transformé inverse selon la revendication (3). Le résultat de ces opérations constitue le message clair après déchiffrement.
7. Une méthode de multiplication de deux cryptogrammes C_1 et C_2. Cette méthode prend en entrée deux matrices cryptogrammes C_1 et C_2 de deux messages clairs σ_1 et σ_2 selon la revendication (5), fait une multiplication matricielle $C_1.C_2$ et donne en sortie une matrice

quaternionique cryptogramme du clair $\sigma = \sigma_1.\sigma_2$. Ledit produit matriciel peut se faire dans n'importe quel ordre (c'est-à-dire on peut calculer $C_1.C_2$ comme on peut calculer $C_2.C_1$).

8. Une méthode d'addition de deux cryptogrammes C_1 et C_2. Cette méthode prend en entrée deux matrices cryptogrammes C_1 et C_2 de deux messages clairs σ_1 et σ_2 selon la revendication (5), fait une addition matricielle C_1+C_2 et donne en sortie une matrice quaternionique cryptogramme du clair $\sigma = (\sigma_1 + \sigma_2) mod\ 2$.
9. Un cryptosystème symétrique probabiliste entièrement homomorphe selon les revendications précédentes caractérisé en ce que si on lui applique la transformée de Rothblum il devient asymétrique.

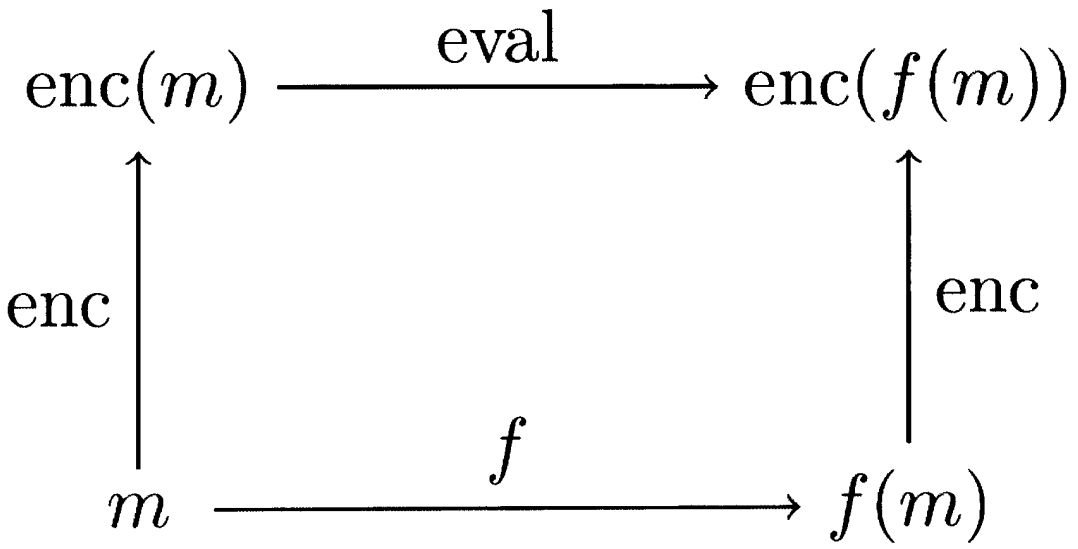

Figure 1

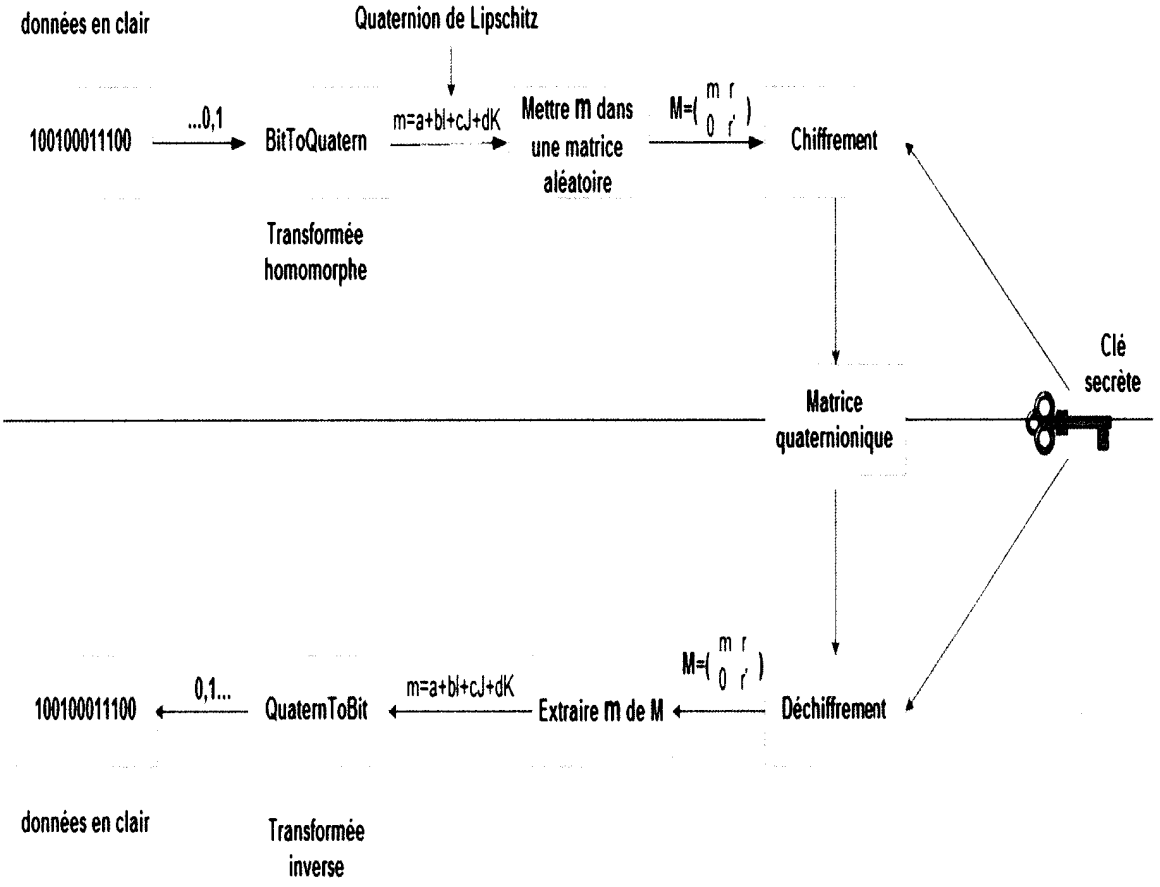
données en clair
Quaternion de Lipschitz
100100011100
...0,1
BitToQuatern
m=a+bI+cJ+dK
Mettre m dans une matrice aléatoire
M=(m r 0 r')
Chiffrement
Transformée homomorphe
Clé secrète
Matrice quaternionique
M=(m r 0 r')
100100011100
0,1...
QuaternToBit
m=a+bI+cJ+dK
Extraire m de M
Déchiffrement
données en clair
Transformée inverse

Figure 2

MA 39511A1

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 39511	Date de dépôt : 07/11/2016
Déposant : UNIVERSITÉ MOHAMMED V RABAT	
Intitulé de l'invention : UN EFFICACE CRYPTOSYSTEME ENTIEREMENT HOMOMORPHE A BASE DES QUATERNIONS.	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☒ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☒ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 12/12/2017
Téléphone: **212 5 22 58 64 14/00**	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  9 Pages
- Revendications
  1-9
- Planches de dessin
  2 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L 9/00

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
A	WO2014016795 ; 30/01/2014 ; NDS LIMITED	2-3,5-9

***Catégories spéciales de documents cités :**

-« **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
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de clarté

Les revendications 2-3, 5-9 ne sont pas rédigées en deux parties, de sorte que l'objet de la protection demandée n'est pas clair. Lesdites revendications portent essentiellement sur des méthodes de traitement de l'information pour des fins de sécurité. Dans ce sens, il est recommandé de procéder à la modification de ces revendications pour spécifier que l'objet de la protection demandée concerne des méthodes avec des séries d'étapes bien déterminées.
L'objet des revendications 2-3, 5-9 manque donc de clarté au sens de l'article 35 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle		
Nouveauté (N)	Revendications 2-3,5-9 Revendications aucune	Oui Non
Activité inventive (AI)	Revendications 2-3,5-9 Revendications aucune	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 2-3,5-9 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : WO2014016795

1. Nouveauté (N) :

Aucun document ne divulgue l'objet des revendications 2-3,5-9 qui est donc nouveau au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

2. Activité inventive (AI) :

Le document D1 est considéré comme l'état de la technique le plus proche de l'objet de la revendication 2 et divulgue :
Un procédé de cryptage entièrement homomorphe pour des données spécifiques dans ZN (ZN est l'anneau de résidus modulo N; N est factorisé par deux premiers, p et q)) pour les applications crypto. L'espace des clairs étant l'anneau Z/nZ et l'espace des cryptogrammes étant l'anneau des matrices modulaires M (Z/nZ).
L'objet de la revendication 2 diffère de D1 en ce que : les messages sont codés par une transformée homomorphe inversible bitToQuatern entre (Z/2Z, XOR, AND) et (H (Z/nZ), +,x). Ladite transformée permet de conserver les deux opérations de XOR et AND sur les bits et de les remplacer par les opérations d'addition et de multiplication sur les quaternions de Lipshitz. L'espace des clairs étant l'anneau Z/2Z.
L'effet technique de cette différence réside en ce que le crypto système est non commutatif résistant aux attaques IND-CPA et IND-KPA.
Le problème objectif que la présente demande se propose de résoudre peut donc être considéré comme : Développer un procédé de cryptographie homomorphe sécurisé contre les attaques IND-CPA et IND-KPA.
La solution proposée implique une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13 parce que aucun élément de l'état de la technique ne contient un enseignement ou une suggestion qui aurait incité l'homme du métier à opter pour ladite solution.
L'objet des revendications dépendantes 3,5-9 implique une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

3. Possibilité d'application industrielle (PAI) :

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.

Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée

L'objet des revendications 1,4 porte essentiellement sur une méthode mathématique qui ne produit aucun résultat technique. Par conséquent l'objet desdites revendications est rejeté au sens de l'article 23 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.