ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19) OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 39664 B1

(51) Cl. internationale :
G09C 1/00

(43) Date de publication :
28.09.2018

(21) N° Dépôt :
39664

(22) Date de Dépôt :
30.12.2016

(71) Demandeur(s) :
Université Mohammed V RABAT , Avenue des Nations Unies, Agdal, bp 8007 NU, Rabat, 10000, Maroc (MA)

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

(74) Mandataire :
KARTIT ZAID

(54) Titre : **Une méthode pratique de cryptage entièrement homomorphe et vérifiable.**

(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.

ABREGE

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 : une méthode pratique de cryptage entièrement homomorphe et vérifiable.

Description :

Domaine technique

L'invention relève du domaine technique de la cryptographie, et plus précisément de la cryptographie entièrement homomorphe et vérifiable, elle concerne un procédé cryptographique permettant de déléguer un calcul à une machine potentiellement non fiable, en lui demandant de fournir une preuve permettant de vérifier en temps constant que les calculs ont été effectués correctement avec une garantie très forte reposant sur des arguments cryptographiques. Il s'agit d'une méthode pratique de cryptographie symétrique entièrement homomorphe (EH), probabiliste et vérifiable basés sur l'utilisation d'une approche matricielle dans un anneau non commutatif. L'anneau utilisé est celui des quaternions entiers dit aussi anneau des entiers de Lipschitz.Cetteméthode 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$Dec(Eval(C, c_1, .., c_n), sk) = C(m_1, \dots, m_n)$.

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 déchiffrementen 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.

Dans la littérature 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.

En sa nature, un cryptosystème EH n'est pas forcément vérifiable- c'est-à-dire ne permet pas de présenter des preuves d'exactitude des calculs effectués sur les données chiffrées-. La vérifiabilité est une propriété de plus que peut avoir un schéma de cryptage EH. Si le cryptosystème EH a le caractère de vérifiabilité ou si nous intégrons la vérifiabilité dans le schéma EH, nous pouvons l'utiliser dans la délégation de calcul ou tout autre calcul dans l'Internet directement comme une unité indépendante, sans aucun autre protocole ou calcul de redondance pour supporter sa vérifiabilité.

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 deuxième objectif est d'élargir les capacités d'un cryptosystème homomorphe afin de permettre la vérification du calcul effectué. Alors que notre troisième objectif s'agit de franchir l'entrave saisissante de la sécurité dans les cryptosystèmes antérieurs. Nous proposons un cryptosystème EH vérifiable 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 et la vérifiabilité 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.

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 et sa vérifiabilité 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 ($n = 2.p.q$).

Le corps des quaternions $\mathbb{H}$

Un quaternion est un nombre dans un sens généralisé. Les quaternions englobent les nombres réels et complexesdans 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 qs'écrit de manière unique sous la forme : $q = a + bi + cj + dk$ où $a, b, cetd$ 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 baseorthonormale 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:

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

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 du cryptosystème

- **Transformée homomorphe entre** $(\mathbb{Z}/2\mathbb{Z}, \boldsymbol{XOR}, \boldsymbol{AND})$ **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$m, \ell, p, q$ 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.

- **Cryptosystème entièrement homomorphe et vérifiable**

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.

Comme le cloud est non confiant, les calculs sur les données chiffrées peuvent être non exacts ou s'effectuer incorrectement. Bob doit disposer d'un moyen de vérification pour s'assurer de la véracité des calculs effectués. Pour cet effet, le cloud doit montrer à Bob une preuve, simplement vérifiable par Bob à la réception, d'exactitude des opérations effectuées. Cette preuve est un service de plus offert par le cryptosystème entièrement homomorphe utilisé.

Afin de bénéficier agréablement de l'avancée technologique du cloud et externaliser ses calculs lourds confortablement, Bob a besoin d'un cryptosystème entièrement homomorphevérifiable et robuste en termes de sécurité, dont les opérations d'addition et de multiplication se font en un temps judicieux, dont le bruit généré lors d'un traitement est maitrisable et dont il dispose d'une preuve d'exactitude des opérations effectuées sur les données chiffrées.

Pour aider Bob à profiter pleinement des puissances du cloud, nous avons inventé un cryptosystème symétrique probabiliste EH vérifiable et 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 premiersp et q.

-puis, il calcule$n = 2.p.q.$

-Bob génère aléatoirement une matrice inversible $K = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \in \mathbb{M}_4(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$ tel que la matrice k_1 soit inversible.

-Bob calcule les inverses de K et k_1, qui seront notés K^{-1} et k_1^{-1} respectivement.

-la clé secrète est $(k_1, k_1^{-1}, K, K^{-1})$.

Chiffrement vérifiable:

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$bitToQuatern$, Bob transforme σ en un quaternion $m = bitToQuatern(\sigma) \in \mathbb{H}(\mathbb{Z}/n\mathbb{Z})$.

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

-Bob calcule $N = k_1 M k_1^{-1}$

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

-Bob génère une matrice $M' = \begin{pmatrix} m' & r_1' \\ 0 & r_2' \end{pmatrix} \in \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$ Tels que r_1'et $r_2' \in \mathbb{H}(\mathbb{Z}/n\mathbb{Z})$à condition que$|r_2'| \equiv 0[n]$.

-Le cryptogramme de σ est : $C = Enc(\sigma) = K \begin{pmatrix} N & R \\ 0 & M' \end{pmatrix} K^{-1} \in \mathbb{M}_4(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$ tel que $R \in \mathbb{M}_2(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$ est choisie aléatoirement.

Déchiffrement et vérification:

Soit un cryptogramme $C \in \mathbb{M}_4(\mathbb{H}(\mathbb{Z}/n\mathbb{Z}))$. Pour déchiffrer C, Bob procède comme suit :

-Il calcule$\begin{pmatrix} N & R \\ 0 & M' \end{pmatrix} = K^{-1}CK$.

-Il calcule$M = k_1^{-1} N k_1$.

-Puis il prend les premières entrées des matrices $m = (M)_{1,1}$et $m' = (M')_{1,1}$.

-Et il vérifie que$\sigma = quaternToBit(m) = quaternToBit(m')$. Si la vérification est vraie, alors le message clair retourné est σ sinon le message chiffré n'est pas intègre.

Homomorphie:

Soient σ_1 *et* σ_2 deux messages clairs et $C_1 = Enc(\sigma_1) et\ C_2 = Enc(\sigma_2)$ leurs cryptogrammes respectivement.

On peut vérifier aisément, 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 $\boldsymbol{n}$ 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.

Utilité de l'invention

La méthode de cryptage présentée dans ce manuscrit est très utile pour différents contextes de masses de données sensibles. Deux domaines très importants d'application de notre invention peuvent être cités dans ce sens :

-Délégation de calculs complexes sur de données sensibles à un cloud non confiant et présentation des preuves d'exactitude des calculs effectués pour le client. Par exemple, les données peuvent être issues d'un opérateur bancaire comme ils peuvent être des données médicales à propos de la santé des citoyens.

-Sécurisation du big data et extraction de décisions sur données confidentielles sans divulguer leur confidentialité et permission de vérification des calculs au client concerné.

Revendications

1. Un cryptosystème symétrique probabiliste entièrement homomorphe et vérifiable dont l'espace des clairs est {0,1} muni des opérations ***XOR et AND*** alors que les cryptogrammes sont des matrices d'ordre quatre dont les entrées sont des quaternions de Lipschitz modulo un grand nombre entier naturel pair$n$) caractérisé en ce que les matrice quaternioniques K et sa sous matrice k_1 choisies aléatoirement, forment la clé secrète et en ce que ces matrices doivent être inversibles.
2. Le cryptosystème selon la revendication (1) 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 de Lipschitz et 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_1 à gauche et par la matrice ${k_1}^{-1}$ à droite, le même message binaire en clair est retransformé en un autre quaternion de Lipschitz et inséré à la première entrée d'une deuxième matrice quaternionique triangulaire supérieure d'ordre deux (c'est la matrice M') dont les deux autres entrées non nulles sont choisies aléatoirement tel que le quaternion de la diagonale soit un diviseur de zéro(c'est le quaternion ${r_2}'$), les deux matrices d'ordre deux $N = k_1 M {k_1}^{-1}$ et M' constituent, respectivement, la première et la deuxième entrée de la diagonale d'une matrice triangulaire supérieure par blocs dont le bloc non nul restant est une matrice quaternionique d'ordre deux R choisie aléatoirement, La continuation du chiffrement se fait en multipliant la matrice par blocs d'ordre quatre $\begin{pmatrix} N & R \\ 0 & M' \end{pmatrix}$ par la matrice K à gauche et par la matrice K^{-1} à droite, La matrice, d'ordre quatre, résultante du produit $K\begin{pmatrix} N & R \\ 0 & M' \end{pmatrix}K^{-1}$ constitue le message chiffré.
3. Le cryptosystème selon les revendications précédentes caractérisé en ce que dans un mode de réalisation, le déchiffrement d'un cryptogramme C (qui est une matrice quaternionique d'ordre quatre) 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 matrice par bloc de la matrice résultante du produit $K^{-1}CK$ et en la multipliant à gauche par la matrice ${k_1}^{-1}$et à droite par la matrice k_1 puis on prend la première entrée de la matrice d'ordre deux résultante et en lui applique la transformé inverse QuaternToBit, le résultat de ces opérations constitue le message clair après déchiffrement.
4. Le cryptosystème selon les revendications précédentes 1 et 2 caractérisé en ce que la multiplication de deux cryptogrammes C_1 et C_2 prend en entrée deux matrices dudit cryptogrammes C_1 et C_2 de deux messages clairs σ_1 et σ_2 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.
5. Le cryptosystème selon les revendications 1 et 2 caractérisé en ce que l'addition de deux cryptogrammes prend en entrée deux matrices cryptogrammes *dudit* C_1 et C_2 de deux messages clairs σ_1 et σ_2, donne en sortie une matrice quaternionique cryptogramme du clair $\sigma = (\sigma_1 + \sigma_2) mod\ 2$.
6. Le cryptosystème selon les revendications 1 et 3 caractérisé en ce que la vérification de la validité d'un cryptogramme se fait en prenant en entrée deux bits et tester leur égalité puis rend en sortie vrai ou faux,le premier bit est issu du déchiffrement alors que le deuxième bit

est issu en appliquant la transformée QuaternToBit à la troisième entrée de la diagonale de la matrice $K^{-1}CK$.

MA 39664B1

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

OMPIC

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE DEFINITIF AVEC OPINION SUR LA BREVETABILITE

Établi conformément à l'article 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 : 39664	Date de dépôt : 30/12/2016
Déposant : Université Mohammed V RABAT	
Intitulé de l'invention : Une méthode pratique de cryptage entièrement homomorphe et vérifiable.	
Classement de l'objet de la demande : CIB : H04L 9/00	

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales

- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité

Partie 2 : Opinion sur la brevetabilité

- ☐ Cadre 3 : Remarques de clarté
- ☐ Cadre 4 : Observations à propos de revendications modifiées qui s'étendent au-delà du contenu de la demande telle qu'initialement déposée
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Défaut d'unité d'invention

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 11/09/2018
Téléphone: **(+212) 5 22 58 64 14**	

ROYAUME DU MAROC OFFICE MAROCAIN de la PROPRIETE INDUSTRIELLE et COMMERCIALE CASABLANCA

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

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

☒ Demande telle qu'initialement déposée

☒ Demande modifiée suite à la notification du rapport de recherche préliminaire :

- Revendications
  1-5

☐ Observations à l'appui des revendications maintenues

☐ Observations des tiers suite à la publication de la demande

☐ Réponses du déposant aux observations des tiers

☐ Nouveaux documents constituant des antériorités :

- Suite à la recherche complémentaire *(Couvrant les documents de l'état de la technique qui n'étaient pas disponibles à la date de la recherche préliminaire)*

  ~~Référence document ; Déposant ; Date~~

- Suite à la recherche additionnelle *(couvrant les éléments n'ayant pas fait l'objet de la recherche préliminaire)*

  Référence document ; Déposant ; Date

☐ Observations à l'encontre de la décision de rejet

Partie 2 : Opinion sur la brevetabilité

Cadre 5: Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications 1-5 Revendications aucune	Oui Non
Activité inventive (AI)	Revendications 1-5 Revendications aucune	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-5 Revendications aucune	Oui Non

D1 : WO2014016795

1. **Nouveauté (N) :**

Aucun document ne divulgue l'objet des revendications 1-5 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 1 et divulgue :
Un procédé de chiffrement dans un espace 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 1 diffère essentiellement de D1 par la clé secrète générée et les étapes de chiffrement.

Le problème objectif que la présente demande se propose de résoudre peut donc être considéré comme : Améliorer le temps d'exécution du chiffrement.

Aucun document de l'état de la technique ne contient un enseignement ou une suggestion qui aurait incité l'homme du métier à résoudre le problème posé en adoptant la même solution sans faire preuve d'esprit inventif.

L'objet des revendications 1-5 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.