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 37367 B1

(51) Cl. internationale :
H04L 9/30; H04L 1/00

(43) Date de publication :
30.11.2016

(21) N° Dépôt :
37367

(22) Date de Dépôt :
19.09.2014

(71) Demandeur(s) :
SAMIR BOUFTASS, . (MA) BP 15379, CASABLANCA PRINCIPALE

(72) Inventeur(s) :
SAMIR BOUFTASS

(54) Titre : **UN PROCEDE D'ECHANGE DE CLES DECRETES ET SES APPLICATIONS DANS LA CRYPTOGRAPHIE ASYMETRIQUE**

(57) Abrégé : L'invention concerne un procédé d'échange de clés secrètes et ses applications dans la cryptographie asymétrique à savoir, le chiffrement a clé publique et la génération des signatures numérique. La sécurité de ce procédé est basée sur le problème suivant :inverser la fonction f=(x) = (a x x)mod(2r)div(2s).Mod est l'opération modulo, div est l'opération division entière, a, r et s sont connus et nombres entiers avec (r > s).; Ce problème est équivalent au problème np complet sat.Pour que deux personnes nommées bob et alice puissent échanger une clé secrète :ils s'accordent sur les nombres entiers 1, m, p, q et z satisfaisants les conditions suivantes : p = (l + m -q), p > (m + q),1a 1ongueur en bits de z est l.Bob choisi d'une manière aléatoire les nombre entiers x, rl et r2.X est de longueur m bits alors que rl et r2 sont de longueur q bits.Il calcule rx = rl x 2p + r2 et u = (z x x) + rx, puis envoie u a alice.Alice choisi d'une manière aléatoire les nombres entiers y, rl et r2. Y est de longueur m bits alors que r3 et r4 sont de longueur q bits.Elle calcule ry = r3 x 2p + r4 et v = (z x y) + ry , puis envoie v à bob.La clé secrète échangée par bob et alice est 2w = (x x v)mod(2p)div(2q) = (y x u)mod(2p)div(2q)

Pour que Bob déchiffre le message d'Alice :

- A partir de l'élément X de sa clé privée et le nombre V reçue d'Alice, il obtient la clé secrète W en calculant $W = (X \times V)Mod(M)Div(D)$.
- A l'aide de la clé secrète W et par le même circuit ou algorithme symétrique utilisé dans le chiffrement, il déchiffre le message chiffré reçu d'Alice.

Revendication 4 :

Une application du procédé d'échange de clés secrètes selon les revendications 1 et 2 dans la génération des signatures numériques, caractérisée en ce que la clé publique est composée des nombres entiers positifs [l , m , p , q , M , D , Z ,U] , et que la clé privée est composée des nombres entiers positifs [X , r1 , r2] , satisfaisant les relations suivantes : $q = l + m - p$, $p > m + q$, $M = 2^p$, $D = 2^q$, $Rx = r1 \times 2^p + r2$ et $U = X \times Z + Rx$.

Z est de longueur l bits , X est de longueur m bits , alors que r1 et r2 sont de longueur q bits.

Pour qu'une personne nommée Bob signe un fichier F destiné a une personne nommée Alice :

- Il choisi d'une façon aléatoire des nombres entiers r3 et r4 de longueur q bits.
- Calcule le nombre : $Ry = r3 \times 2^p + r4$.
- Hache le fichier F a l'aide d'une fonction de hachage sécurisée FH et obtient une emprunte H de même longueur en bits que de l'élément Z de sa clé publique.
- Il calcule a partir de l'élément X de sa clé privée une signature $S = (X \times H) + Ry$.
- Envoie le fichier F et la signature S a Alice.

Pour qu'Alice vérifie que le fichier F est bien de Bob :

- Elle Hache le fichier F a l'aide de la fonction de hachage FH et obtient une emprunte H de même longueur en bits que Z.
- A partir de H , la signature S et les éléments de la clé publique (U, Z, M, D) de Bob, elle calcule deux nombres $Wx = (H \times U)Mod(M)Div(D)$ et $Wy = (Z \times S)Mod(M)Div(D)$

Pour vérifier si le fichier F est bien envoyé par Bob il faut que Wx soit égal a Wy.

Un procédé d'échange de clés secrètes et ses applications dans la cryptographie asymétrique.

Descriptif :

I) Domaine de l'invention :

Cette invention rentre dans le domaine du chiffrement des données et la sécurisation des canaux de communication.

II) Etat de la technique :

Le standard actuel dans le domaine des procèdes d'échange de clés secrètes est le procède de Diffie-Hellman dans le groupe multiplicatif ou dans les groupes associés aux courbes elliptique.
Le procédé d'échange de clés secrètes objet de cette invention se caractérise par le fait qu'il demande beaucoup moins de calcul donc plus rapide, tout en étant sécurisé.

III) Principe et Description de l'invention :

L'objet de cette invention est un procédé d'échange de clés secrètes et ses applications dans la cryptographie asymétrique, a savoir le chiffrement a clé publique et la génération des signatures numériques .

III-1) Le procède d'échange de clés secrètes :

La figure 1, représente un schéma synoptique de ce procédé.

Au préalable Alice et Bob connaissent :

- Des nombres entiers [l, m, p, q, M, D, Z] satisfaisant les conditions suivantes :
  $p > m + q$, $q = l + m - p$, $M = 2^p$, $D = 2^q$, Z est de longueur l bits.

Pour échanger une clé secrète :

- Bob choisi d'une façon aléatoire les nombres [X , r1 , r2].
  X est de longueur m bits alors que r1 et r2 sont de longueur q bits.
- Calcule les nombres : $Rx = r1 \times 2^p + r2$ et $U = X \times Z + Rx$.
- Transmet U a Alice.

- De son coté Alice choisi d'une façon aléatoire les nombres [Y , r3 , r4].
  Y est de longueur m bits alors que r3 et r4 sont de longueur q bits.
- Calcule les nombres : $Rx = r3 \times 2^p + r4$ et $V = Y \times Z + Ry$
- Transmet V a Bob.

- Bob calcule le nombre : $(X \times V)Mod(M)Div(D)$.
- Alice calcule le nombre : $(Y \times U)Mod(M)Div(D)$.

La clé secrète échangée par Bob et Alice est :
$W = (X \times V)Mod(M)Div(D) = (Y \times U)Mod(M)Div(D)$ et sa longueur en bits est $p - (m + q)$.

III-2) L'application dans le chiffrement a clé publique :

La figure 2, représente un schéma synoptique d'une application du procédé d'échange de clés secrètes objet de cette invention, dans le chiffrement a clé publique.

Le chiffrement :

Pour qu'Alice envoie un message chiffré a Bob :

- Elle obtient sa clé publique (20) composée des nombres entiers positif [l, m, p, q, M, D, Z, U], satisfaisant les conditions suivantes : $p > m + q$, $q = l + m - p$, $M = 2^p$, $D = 2^q$, $U = X \times Z + Rx$ et $Rx = r1 \times 2^p + r2$.
  X est de longueur m bits alors que r1 et r2 sont de longueur q bits.
- Elle choisi d'une façon aléatoire des nombres entiers positif (22) [Y, r3, r4]
  Y est de longueur m bits alors que r3 et r4 sont de longueur q bits.
- Elle calcule les nombres $Ry = r3 \times 2^p + r4$ et $V = Y \times Z + Ry$ (26) puis la clé secrète W (23)
  $W = (Y \times U)Mod(M)Div(D)$.
- Elle chiffre à l'aide de la clé secrète (23) et un circuit ou un algorithme de chiffrement symétrique (25) le message en claire (24), puis envoie a Bob le message chiffré (27) et le nombre V (26).

Le déchiffrement :

Pour que Bob déchiffre le message chiffré reçu d'Alice :

- A partir de l'élément X de sa clé privée (21) et le nombre V (26) reçu d'Alice, il calcule la clé secrète $W = (X \times V)Mod(M)Div(D)$ (23).
- Il obtient le message en claire (24) en déchiffrant le message chiffré (27), a l'aide de la clé secrète W et par le même circuit ou algorithme de chiffrement symétrique utilisé dans le chiffrement (28).

III-3) L'application dans la génération des signatures numérique :

La figure 3, représente un schéma synoptique d'une application du procédé d'échange de clés secrète objet de cette invention dans la génération des signatures numérique .

Signature :

Pour signer un fichier :

- Bob choisi d'une façon aléatoire des nombres entiers r3 et r4 de longueur q bits.
- Calcule le nombre $Ry = r3 \times 2^p + r4$.
- Hache un fichier F (32) a l'aide d'une fonction de hachage FH (33) et obtient une emprunte H (34) de même largeur en bits que Z . Puis a partir de l'élément X de sa clé privée (31) il calcule une signature $S = (X \times H) + Ry$.
- Envoie le fichier F et la signature S a Alice.

Vérification :

Pour vérifier que le fichier F est bien envoyé par Bob

- Alice obtient la clé publique (30) de Bob composée des nombres entiers positif : $[l, m, p, q, M, D, Z, U]$, satisfaisant les conditions suivantes : $p > m + q$, $q = l + m - p$, $M = 2^p$, $D = 2^q$, $Rx = r1 \times 2^p + r2$, $U = X \times Z + Rx$, X est de longueur m bits alors que r1 et r2 sont de longueur q bits.
- Hache un fichier F (32) a l'aide d'une fonction de hachage FH (33) et obtient une emprunte H (34) de même longueur en bits que Z.
- A partir de l'emprunte H , la signature S et les éléments de la clé publique [U, Z, M, D] elle calcule deux nombres $Wx = (H \times U)Mod(M)Div(D)$ et $Wy = (Z \times S)Mod(M)Div(D)$

Le fichier F est bien envoyé par Bob Si Wx est égal à Wy.

III-4) Efficacité et sécurité :

Efficacité :

En comparaison avec les procédés d'échanges de clés secrètes standardisés comme le procède de Diffie-Hellman dans le groupes multiplicatif qui nécessite pour échanger une clé secrète en moyenne N / 2 multiplications modulo (N étant la longueur en bits de la clé privée).
Le procédé d'échange de clés secrètes objet de cette invention ne nécessite que 3 opérations arithmétiques a savoir une multiplication , une modulo et une division entière
Ce qui prouve qu'il est plus rapide et plus efficient que les procédés standardisés.

Sécurité :

La sécurité du procédé d'échange de clés secrète objet de cette invention est basée sur la difficulté de trouver X et Y connaissant Z , p , q , $U = (X \times Z)\text{Mod}(2^p)\text{Div}(2^q)$ et $V = (Y \times Z)\text{Mod}(2^p)\text{Div}(2^q)$. Autrement dit , elle est basée sur la difficulté d'inverser la fonction suivante : $F(X) = (X \times A)\text{Mod}(2^p)\text{Div}(2^q) = (Y)\text{Mod}(2^p)\text{Div}(2^q)$. A , X , p et q sont des nombres entiers connus , A et X sont long respectivement de n et m bits , $(n > m)$ et $(p > q)$.

La représentation binaire de A => $a_{(n)}.....a_{(i+1)}a_{(i)}.....a_0$.

La représentation binaire de X => $x_{(m)}.....x_{(i+1)}x_{(i)}.....x_0$.

La représentation binaire de Y => $y_{(n+m)}.....y_{(i+1)}y_{(i)}.....y_0$.

Y étant le produit de A et X , donc notre problème consiste a résoudre ce système d'équations :

Si $(j \le m)$ =>

$$y_j = \left(\sum_{i=0}^{j}(a_{(j-i)} \times x_i) + r_j\right) \text{Mod}(2) \quad \text{et} \quad r_j = \left(\sum_{i=0}^{j-1}(a_{(j-1-i)} \times x_i) + r_{j-1}\right) \text{Div}(2)$$

Si $(m \le j \le n)$ =>

$$y_j = \left(\sum_{i=j-m}^{j}(a_{(j-i)} \times x_i) + r_j\right) \text{Mod}(2) \quad \text{et} \quad r_{j-1} = \left(\sum_{i=j-m}^{j-1}(a_{(j-1-i)} \times x_i) + r_{j-1}\right) \text{Div}(2)$$

Si $(n \le j \le n+m)$ =>

$$y_j = \left(\sum_{i=j-n}^{n}(a_{(j-i)} \times x_i) + r_j\right) \text{Mod}(2) \quad \text{et} \quad r_{j-1} = \left(\sum_{i=j-n}^{n}(a_{(j-1-i)} \times x_i) + r_{j-1}\right) \text{Div}(2)$$

r_j étant le bit retenue de la multiplication $(X \times A)$ a la colonne j.

Résoudre ce système d'équations est équivalent a trouver des valeur booléennes $x_{i=0 \to m}$ satisfaisant les équations combinatoires suivantes :

$$r_j = F(x_{(j-1)},.....x_{(i+1)}, x_{(i)},.....x_{(0)}, r_{(j-1)})$$

$$\wedge_{j=0}^{m} \left(\left(\oplus \sum_{i=0}^{j} (a_{(j-i)} \wedge x_i) \oplus r_j\right) = y_j\right) = \text{true}$$

$$\wedge_{j=m}^{n} \left(\left(\oplus \sum_{i=j-m}^{j} (a_{(j-i)} \wedge x_i) \oplus r_j\right) = y_j\right) = \text{true}$$

$$\wedge_{j=n}^{n+m} \left(\left(\oplus \sum_{i=j-n}^{n} (a_{(j-i)} \wedge x_i) \oplus r_j\right) = y_j\right) = \text{true}$$

F étant une fonction combinatoire .

Autrement dit la sécurité du procédé d'échange de clés secrètes objet de cette invention est basée sur un problème difficile a savoir le problème NP Complet SAT.

IV) Figures

Figure 1, illustre un schéma synoptique du procédé d'échange de clés symétrique objet de cette invention.

Figure 2, illustre un schéma synoptique de l' application du procédé d'échange de clés symétrique objet de cette invention dans le chiffrement asymétrique .

- 20 : Clé publique.
- 21 : Clé privée.
- 22 : Valeur choisie d'une manière aléatoire .
- 23 : Clé secrète.
- 24 : Message en claire.
- 25 : Un circuit chiffreur ou une implémentation d'un algorithme symétrique de chiffrement.
- 26 : Valeur entière en fonction de (22) .
- 27 : Message chiffré.
- 28 : Un circuit déchiffreur ou une implémentation d'un algorithme symétrique de déchiffrement.

Figure 3, illustre un schéma synoptique de l' application du procédé d'échange de clés secrète objet de cette invention dans la génération des signatures numériques .

- 30 : Clé publique.
- 31 : Clé privée.
- 32 : Fichier a signer.
- 33 : Fonction de Hachage.
- 34 : L'emprunte digitale correspondant au Fichier a signer (32).
- 35 : Une signature numérique du Fichier (32).
- 36 : Equation a vérifier .

Revendications

Revendication 1 :

Un procédé d'échange de clés secrètes et ses applications dans le chiffrement asymétrique.
La sécurité de ce procédé est basée sur la difficulté d'inverser la fonction suivante :

$F(X) = (A \times X)\text{Mod}(2^r)\text{Div}(2^s)$. Mod est opération modulo , Div est opération division entière
A , r et s sont connus et des nombres entiers avec ($r > s$) .

Revendication 2 :

Un procédé d'échange de clés secrètes selon la revendication 1 caractérisé en ce que
Pour que deux personnes nommées Bob et Alice échangent une clé :

- Ils s'accordent sur des nombres l , m , p , q et Z satisfaisants les conditions suivantes :
  $p = (l + m - q)$, $p > (m + q)$, Z est un nombre entier de longueur l bits .
- Bob choisi d'une manière aléatoire les nombres X de longueur m bits, r1 et r2 de longueur q bits,
  calcule $Rx = r1 \times 2^p + r2$ et $U = (Z \times X) + Rx$, puis envoie U a Alice .
- Alice choisi d'une manière aléatoire les nombres Y de longueur m bits, r3 et r4 de longueur q bits,
  calcule $Ry = r3 \times 2^p + r4$ et $V = (Z \times Y) + Ry$, puis envoie V a Bob .

La clé secrète échangée par Bob et Alice est :
$W = (X \times V)\text{Mod}(2^p)\text{Div}(2^q) = (Y \times U)\text{Mod}(2^p)\text{Div}(2^q)$

Revendication 3 :

Une application du procédé d'échange de clés secrètes selon les revendications 1 et 2, dans le chiffrement a clé publique, caractérisée en ce que la clé publique est composée des nombres entiers positifs [l , m , p , q , M , D , Z ,U] , et que la clé privée est composée des nombres entiers positifs [X , r1 , r2] satisfaisant les relations suivantes : $q = l + m - p$, $p > m + q$, $M = 2^p$, $D = 2^q$, $Rx = r1 \times 2^p + r2$ et $U = X \times Z + Rx$.
X est de longueur m bits alors que r1 et r2 sont de longueur q bits.
Pour qu'Alice envoie un message chiffré a Bob :

- Elle obtient sa clé publique.
- Elle choisi d'une manière aléatoire des nombres entiers positif Y, r3 et r4 .
  Y est de longueur m bits alors que r3 et r4 sont de longueur q bits.
- A partir des éléments [p, Z , Y, M , D] de la clé publique de Bob, Elle calcule les nombres :
  $Ry = r3 \times 2^p + r4$, $V = Y \times Z + Ry$ et la clé secrète $W = (Y \times U)\text{Mod}(M)\text{Div}(D)$.
- A l'aide de la clé secrète W et par un circuit ou un algorithme de chiffrement symétrique
  elle chiffre un message en claire puis envoie a Bob le message chiffré correspondant
  et le nombre V.

MA 37367B1

Un procédé d'échange de clés secrètes et ses applications dans la cryptographie asymétrique.

Abrégé :

L'invention concerne un procédé d'échange de clés secrètes et ses applications dans la cryptographie asymétrique a savoir, le chiffrement a clé publique et la génération des signatures numérique. La sécurité de ce procédé est basée sur le problème suivant :

Inverser la fonction $F(X) = (A \times X)\text{Mod}(2^r)\text{Div}(2^s)$.

Mod est l'opération modulo, Div est l'opération division entière , A , r et s sont connus et nombres entiers avec (r > s) . Ce problème est équivalent au problème NP Complet SAT.

Pour que deux personnes nommées Bob et Alice puissent échanger une clé secrète :

Ils s'accordent sur les nombres entiers l , m , p , q et Z satisfaisants les conditions suivantes : p = (l + m - q) , p > (m + q) , la longueur en bits de Z est l.

Bob choisi d'une manière aléatoire les nombre entiers X, r1 et r2.
X est de longueur m bits alors que r1 et r2 sont de longueur q bits.
Il calcule $Rx = r1 \times 2^p + r2$ et $U = (Z \times X) + Rx$, puis envoie U a Alice.

Alice choisi d'une manière aléatoire les nombres entiers Y, r1 et r2. Y est de longueur m bits alors que r3 et r4 sont de longueur q bits.
Elle calcule $Ry = r3 \times 2^p + r4$ et $V = (Z \times Y) + Ry$, puis envoie V a Bob.

La clé secrète échangée par Bob et Alice est :

$$W = (X \times V)\text{Mod}(2^p)\text{Div}(2^q) = (Y \times U)\text{Mod}(2^p)\text{Div}(2^q)$$

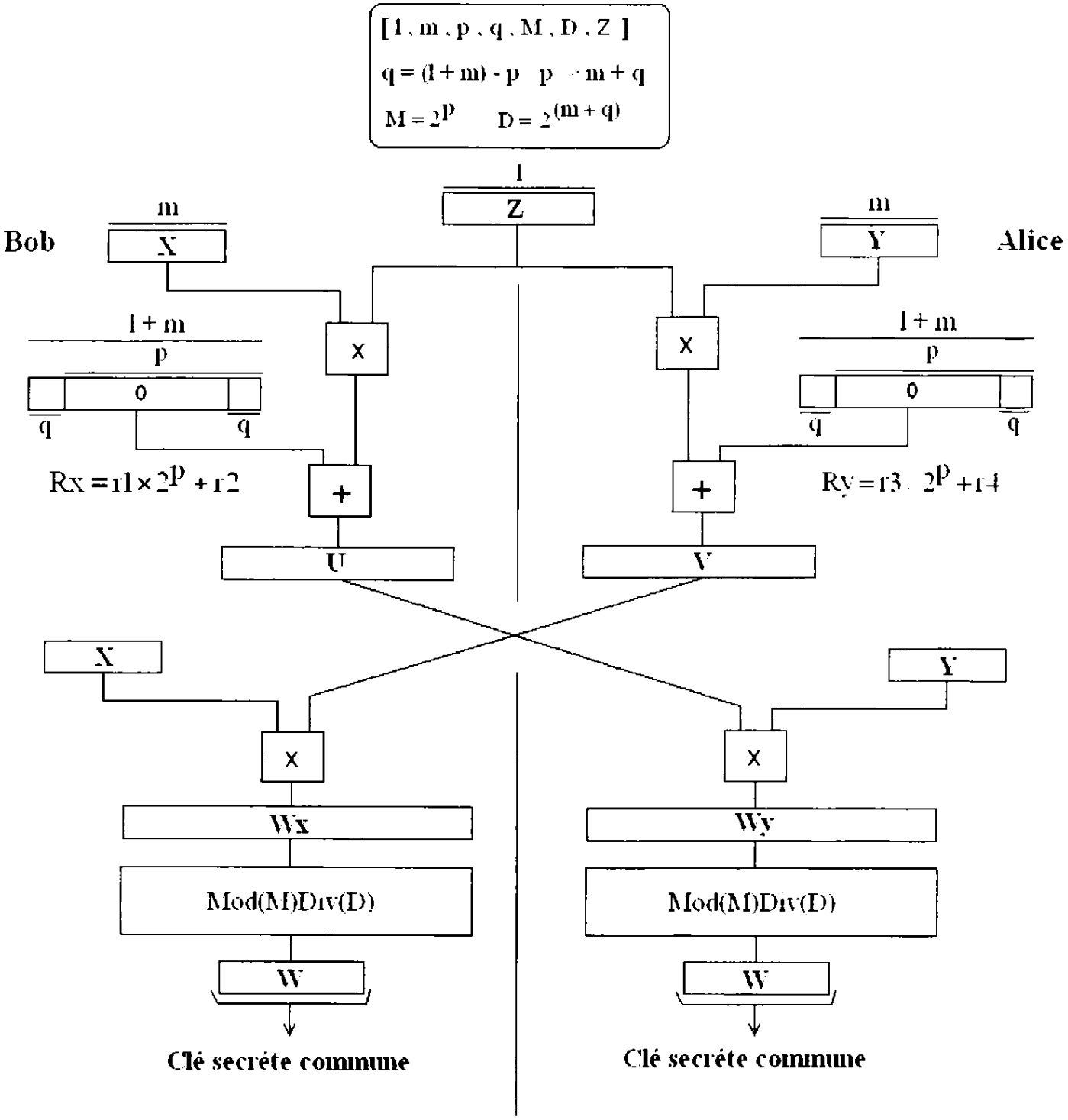
[l , m , p , q , M , D , Z]
q = (l + m) - p p = m + q
M = 2^p D = 2^(m + q)
l
Z
m
Bob
X
m
Y
Alice
l + m
p
0
q
q
X
X
l + m
p
0
q
q
Rx = r1 × 2^p + r2
+
+
Ry = r3 × 2^p + r4
U
V
X
Y
X
X
Wx
Wy
Mod(M)Div(D)
Mod(M)Div(D)
W
W
Clé secrète commune
Clé secrète commune

Figure 1

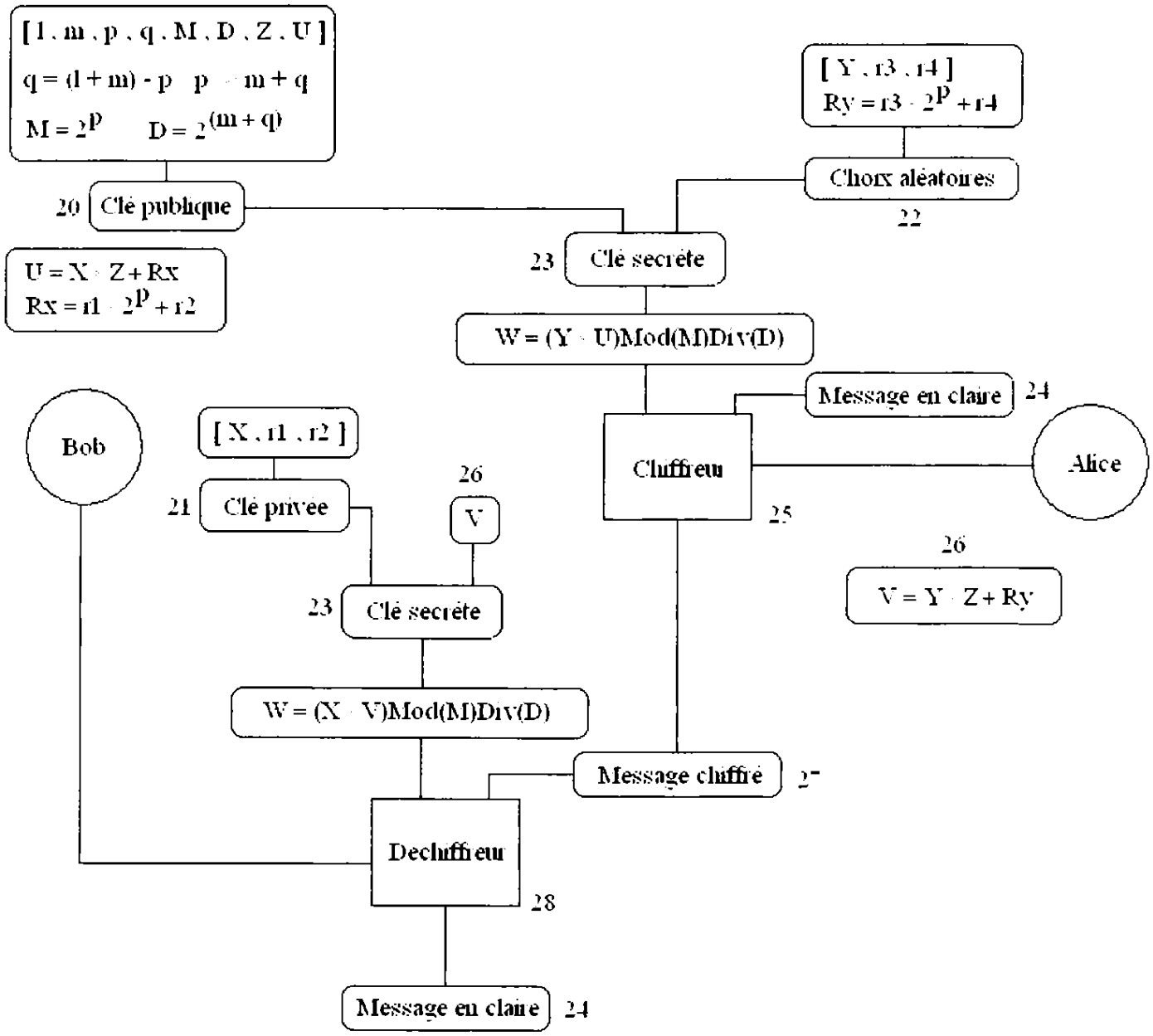
[l , m , p , q , M , D , Z , U]
q = (l + m) - p p m + q
M = 2^p D = 2^(m + q)
20 Clé publique
[Y , r3 , r4]
Ry = r3 2^p + r4
Choix aléatoires
22
U = X Z + Rx
Rx = r1 2^p + r2
23 Clé secrète
W = (Y U)Mod(M)Div(D)
Message en claire 24
Bob
[X , r1 , r2]
Cluffieu
Alice
21 Clé privée
26
V
25
26
V = Y Z + Ry
23 Clé secrète
W = (X V)Mod(M)Div(D)
Message cluffié
Decluffieu
28
Message en claire 24

Figure 2

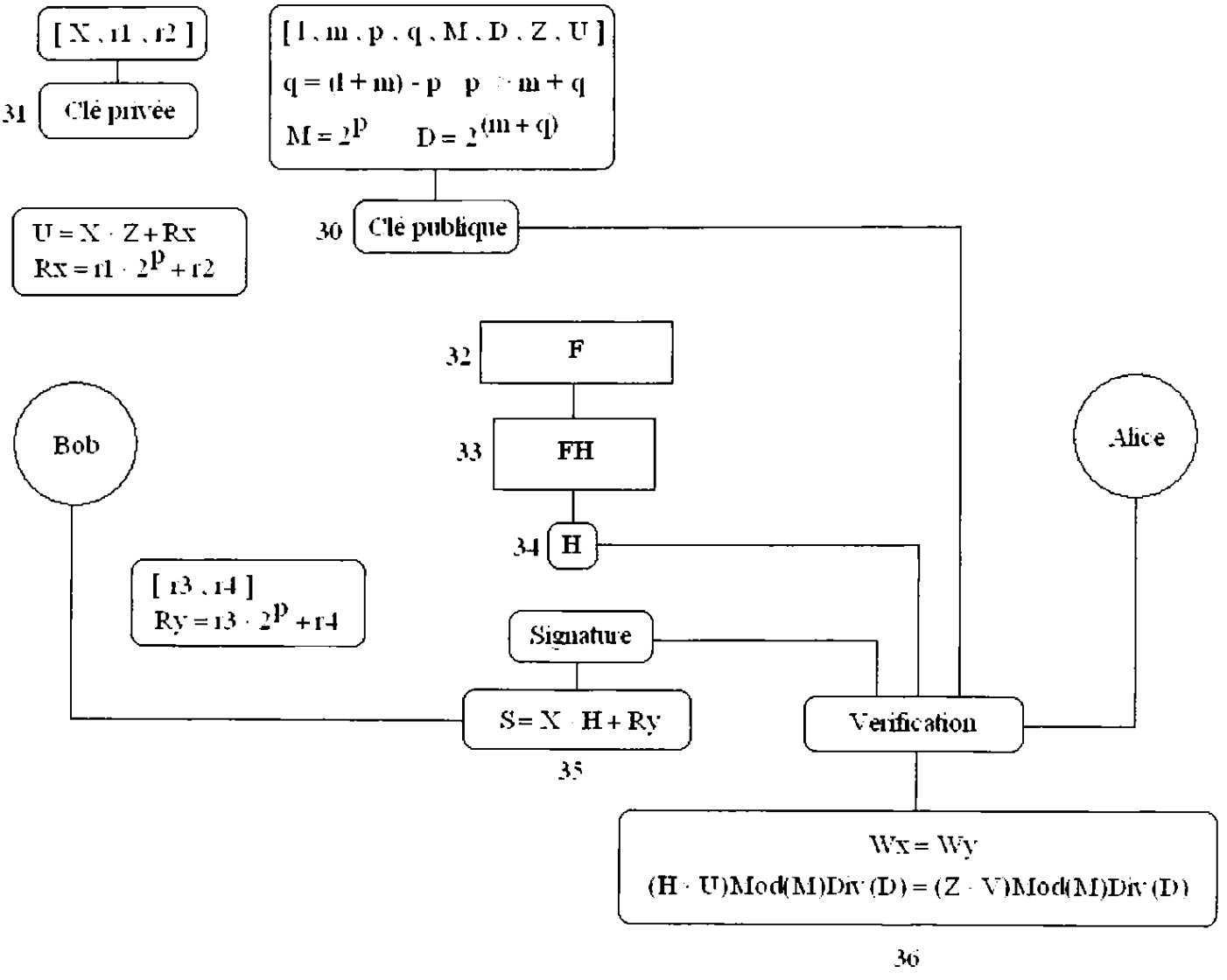
[X , r1 , r2]
31
Clé privée
[l , m , p , q , M , D , Z , U]
q = (l + m) - p p = m + q
M = 2^p D = 2^(m + q)
U = X · Z + Rx
Rx = r1 · 2^p + r2
30
Clé publique
32
F
33
FH
34
H
Bob
Alice
[r3 , r4]
Ry = r3 · 2^p + r4
Signature
S = X · H + Ry
35
Verification
Wx = Wy
(H · U)Mod(M)Div(D) = (Z · V)Mod(M)Div(D)
36

Figure 3

MA 37367B1

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)

Renseignements relatifs à la demande

N° de la demande : 37367	Date de dépôt : 19/09/2014
Déposant : SAMIR BOUFTASS	

Intitulé de l'invention : UN PROCEDE D'ECHANGE DE CLES SECRETES ET SES APPLICATIONS DANS LA CRYPTOGRAPHIE ASYMETRIQUE

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 cités par l'examinateur dans la partie rapport de recherche sont joints au présent document

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** : 22/04/2016
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
  5 Pages
- Revendications
  4
- Planches de dessin
  3 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L9/30, H04L9/28

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	WO2006051402 18/05/2006 Certicom Corp, Daniel R L Brown, Robert P Gallant, Scott A Vanstone	1-4
A	US8094823 10/01/2012 Rockstar Bidco, LP	1-4

***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

L'objet de la revendication 1 ne spécifie pas les étapes du procédé d'échange de clés secrètes, qui sont essentielles à la définition de l'invention. Il en ressort une discordance entre l'objet de ladite revendication et la description de l'invention. Par conséquent, l'examen de la revendication a porté sur toutes les caractéristiques essentielles à la définition de l'objet de l'invention.

L'utilisation des parenthèses est réservée aux signes de référence, une possibilité pour définir et délimiter les équations mathématiques présentées dans les revendications 1-4 serait donc d'utiliser des crochets.

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

Nouveauté (N)	Revendications 1-4 Revendications aucune	Oui Non
Activité inventive (AI)	Revendications 1-4 Revendications aucune	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1-4 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 : WO2006051402

1. **Nouveauté (N) :**

Aucun document ne divulgue l'objet des revendications 1-4. L'objet desdites revendications est donc nouveau au sens de l'article 26 de la loi 17-97 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 divulgue un procédé d'échange de clés secrètes basé sur l'algorithme de Diffie Hellman et la difficulté de résoudre l'équation NP complet SAT caractérisé en ce que :

- Alice choisit un entier x et envoie gx à Bob
- Bob choisit un entier y et envoie gy à Alice
- Alice calcule z = (gx) y et Bob calcule z' = (gy)x
- La clé générée étant z=z'

Par conséquent, l'objet de la revendication 1 diffère de ce document en ce que :
La clé échangée est W = (X x V) Mod (2p) Div (2q)= (Y x U) Mod (2p) Div (2q)
L'effet technique de cette différence réside en ce que le procédé d'échange de clés secrètes ne nécessite que 3 opérations arithmétiques à savoir une multiplication, une modulo et une division et donc est plus rapide.
Le problème objectif que la présente demande se propose de résoudre peut donc être considéré comme : améliorer l'efficacité du procédé d'échange de clés secrètes de Diffie-Hellman.
L'objet de la revendication 1 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. Aucun document de l'état de la technique ne contient une incitation qui aurait motivé l'homme du métier à simplifier le procédé de Diffie-Hellman de la même manière que la présente invention afin d'améliorer l'efficacité du procédé.
L'objet de la revendication 2 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.
Les revendications 3 et 4 sont des revendications d'utilisation correspondantes aux revendications de procédé 1 et 2. L'objet des revendications 3 et 4 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