ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) DEMANDE DE BREVET

(11) N° de publication :
MA 38128 A1

(51) Cl. internationale :
H04L 9/00

(43) Date de publication :
31.10.2016

(21) N° Dépôt :
38128

(22) Date de Dépôt :
25.05.2015

(71) Demandeur(s) :
BOUFTASS SAMIR, N°11, RUE 284 HAY MLY ABDELLAH AIN CHOCK CASABLANCA (MA)

(54) Titre : **UN PROCEDE D'ECHANGE DE CLES SECRETES 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 a savoir, le chiffrement a clé publique et la génération des signatures numérique. La sécurité de ce procédé est basée sur le problème suivant : Inverserla fonction F(X) =(A x X)Mod(bP)Div(bq). Mod est l'opération modulo, Div est l'opération division entière, A ,b ,p et q sont connus et nombres entiers avec (p > q) . Pour que deux personnes nommées Bob et Alice puissent échanger une clé secrète Ils s'accordent sur les nombres entiers A , b , l, m , p, q et r satisfaisants les conditions suivantes: r > 80, 1+ m > P > m + q + r ,A est un entier de même longueur en bit que b 1 • Bob choisi d'une manière aléatoire un nombre entierX de même longueur en bit que bm . Il calcule U = (A x X)Mod(bP)Div(bq), puis envoie Ua Alice. Alice choisi d'une manière aléatoire un nombre entier Yde même longueur en bit que bm. Elle calcule: V =(A x Y)Mod(bP)Div(bq) puis envoie Va Bob. La clé secrète échangée par Bob et Alice est : w =(Xx V)Mod(b P - q)Div(bm + r) =(Y x U)Mod(bP - q)Div(bm + r)

MA 38128A1

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 $F(X)=(A\times X)Mod(b^{p})Div(b^{q})$.

Mod est l'opération modulo, Div est l'opération division entière , A ,b , p *et* q sont connus et nombres entiers avec $(p > q)$.

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

Ils s'accordent sur les nombres entiers A , b , l , m , p , q *et* r satisfaisants les conditions suivantes :

$r > 80$, $l + m > p > m + q + r$, A est un entier de même longueur en bit que b^{l}.

Bob choisi d'une manière aléatoire un nombre entier X de même longueur en bit que b^{m}.

Il calcule $U=(A\times X)Mod(b^{p})Div(b^{q})$, puis envoie U a Alice.

Alice choisi d'une manière aléatoire un nombre entier Y de même longueur en bit que b^{m}.

Elle calcule : $V=(A\times Y)Mod(b^{p})Div(b^{q})$ puis envoie V a Bob.

La clé secrète échangée par Bob et Alice est :

$$W=(X\times V)Mod(b^{p-q})Div(b^{m+r})=(Y\times U)Mod(b^{p-q})Div(b^{m+r})$$

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 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 A , b , l , m , p , q , r satisfaisant les conditions suivantes :
  $r > 80$, $l + m > p > m + q + r$, A est de même longueur en bits que b^l .

Pour échanger une clé secrète :

- Bob choisi d'une façon aléatoire un nombre entier X de même longueur en bits que b^m .
- Calcule un nombre $U = (A \times X) Mod(b^p) Div(b^q)$.
- Transmet U a Alice.

- De son coté Alice choisi aléatoirement un nombre entier Y de même longueur en bits que b^m.
- Calcule un nombre $V = (A \times Y) Mod(b^p) Div(b^q)$.
- Transmet V a Bob.

- Bob calcule le nombre : $(X \times V) Mod(b^{p-q}) Div(b^{m+r})$.
- Alice calcule le nombre : $(Y \times U) Mod(b^{p-q}) Div(b^{m+r})$.

La clé secrète échangée par Bob et Alice est :

$W = (X \times V) Mod(b^{p-q}) Div(b^{m+r}) = (Y \times U) Mod(b^{p-q}) Div(b^{m+r})$.

W est de même longueur en bits que $b^{(p-(q+m+r))}$.

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 A, b, l, m, p, q, r, U satisfaisant les conditions suivantes : $r > 80$, $l + m > p > m + q + r$, $U = (A \times X) Mod(b^p) Div(b^q)$. X est de même longueur en bits que b^m.
- Elle choisi d'une façon aléatoire un nombres entier positif Y (22) . Y est de même longueur en bits que b^m.
- Elle calcule les nombres $V = (A \times Y) Mod(b^p) Div(b^q)$ (26) puis la clé secrète W (23) $W = (Y \times U) Mod(b^{p-q}) Div(b^{m+r})$.
- 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 $W = (X \times V) Mod(b^{p-q}) Div(b^{m+r})$ (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 .

La clé publique (30) de Bob est composée des nombres entiers A , b , l , m , p , q , r , U.
sa clé privée est composée d'un nombre entier X. Ces nombres remplissent les conditions suivantes :

$l + m > p > m + q + r$, $r > 80$ et $U = (A \times X) Mod(b^p) Div(b^q)$.

A est de même longueur en bits que b^l , alors que X est de même longueur en bits que b^m.

Signature :

Pour signer un fichier Bob effectue les étapes suivantes :

- Il choisi d'une façon aléatoire un nombres Y de même longueur en bits que b^m.
- 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 b^l.
- Il calcule $S1 = (A \times Y) Mod(b^p) Div(b^q)$ et $S2 = (H \times (X + Y)) Mod(b^p) Div(b^q)$.
- Envoie a Alice le fichier F et une signature $(S1, S2)$.

Vérification :

Pour vérifier que le fichier F est bien envoyé par Bob, Alice effectue les étapes suivantes :

- 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 b^l.
- A partir de H , la signature $(S1, S2)$. et les éléments (U, A) de la clé publique de Bob , elle calcule deux nombres $Wx = (H \times (S1 + U)) Mod(b^{p-q}) Div(b^{l+r})$ et $Wy = (A \times S2) Mod(b^{p-q}) Div(b^{l+r})$

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

III-4) Sécurité et efficacité :

La sécurité du procédé d'échange de clés secrète objet de cette invention est basée sur un nouveau problème computationnel difficile qui consiste a inverser la fonction non linéaire suivante :

$F(X) = (A \times X) Mod(b^p) Div(b^q)$. Mod est opération modulo , Div est opération division entière A , p et q sont connus et des nombres entiers avec $(p > q)$.

En comparaison avec les procédés d'échanges de clés secrètes standardisés comme le procède de Diffie-Hellman dans le groupe multiplicatif qui nécessite pour échanger une clé secrète en moyenne N 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 6 opérations arithmétiques a savoir deux multiplications , deux modulos et deux divisions entière
Ce qui prouve qu'il est plus rapide et plus efficient que les procédés standardisés.

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 : Valeur choisie d'une manière aléatoire .
- 33 : Fichier a signer.
- 34 : Fonction de Hachage.
- 35 : L'emprunte digitale correspondant au Fichier a signer (32).
- 36 : Une signature numérique du Fichier (32).
- 37 : Equation a vérifier .

Revendications

Revendication 1 :

Un procédé d'échange de clés secrètes et ses applications dans le chiffrement asymétrique.
Ce procédé est caractérisé en ce que sa sécurité est basée sur la difficulté d'inverser

la fonction $F(X) = (A \times X) Mod(b^p) Div(b^q)$. Mod est opération modulo
Div est opération division entière, A, b, p et q sont des entiers connus avec $(p > q)$.

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 A, b, l, m, p, q et r satisfaisants les conditions suivantes :

$r > 80$, $l + m > p > m + q + r$, A est un nombre entier de même longueur en bits que b^l.

- Bob choisi d'une manière aléatoire un nombre X de même longueur en bits que b^m.

Calcule $U = (A \times X) Mod(b^p) Div(b^q)$, puis envoie U a Alice.

- Alice choisi d'une manière aléatoire un nombre Y de même longueur en bits que b^m.

Calcule $V = (A \times Y) Mod(b^p) Div(b^q)$, puis envoie V a Bob.

La clé secrète échangée par Bob et Alice est :
$W = (X \times V) Mod(b^{p-q}) Div(b^{m+r}) = (Y \times U) Mod(b^{p-q}) Div(b^{m+r})$.

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
A, b, l, m, p, q, r, U, et en ce que la clé privée est composée d'un nombre entier X.
Ces nombres remplissent les conditions suivantes : $r > 80$, $l + m > p > m + q + r$,

$U = (A \times X) Mod(b^p) Div(b^q)$, A est de même longueur en bits que b^l, alors que X est de même

longueur en bits que b^m. Pour qu'Alice envoie un message chiffré a Bob :

- Elle obtient sa clé publique.

- Elle choisi d'une manière aléatoire un nombre entier positif Y de même longueur en bits que b^m.

- A partir des éléments A, b, p, q, r, U de la clé publique de Bob, Elle calcule les nombres : $V = (A \times Y) Mod(b^p) Div(b^q)$ et la clé secrète $W = (Y \times U) Mod(b^{p-q}) Div(b^{m+r})$.

- 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.

Pour que Bob déchiffre le message d'Alice :

- A partir de l'élément X de sa clé privée et le nombre V reçu d'Alice, il obtient la clé secrète en calculant $W = (X \times V) Mod(b^{p-q}) Div(b^{m+r})$.
- 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 A, b, l, m, p, q, r, U , et en ce que la clé privée est composée d'un nombre entiers X
Ces nombres remplissent les conditions suivantes :

$r > 80, l + m > p > l + q + r$, et $U = (A \times X) Mod(b^p) Div(b^q)$.

A est de même longueur en bits alors que b^l, alors que X est de même longueur en bits que b^m.

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

- Il choisi d'une façon aléatoire un nombres Y est de même longueur en bits que b^m.
- 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 b^l.
- Il calcule $S1 = (A \times Y) Mod(b^p) Div(b^q)$ et $S2 = (H \times (X + Y)) Mod(b^p) Div(b^q)$.
- Envoie a Alice le fichier F et une signature $(S1, S2)$.

Pour qu'Alice vérifie que le fichier F est envoyé par 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 b^l.

- A partir de H , la signature $(S1, S2)$. et les éléments de la clé publique (U, A) de Bob, elle calcule deux nombres $Wx = (H \times (S1 + U)) Mod(b^{p-q}) Div(b^{l+r})$ et $Wy = (A \times S2) Mod(b^{p-q}) Div(b^{l+r})$

Le fichier F est bien envoyé par Bob si Wx est égal a Wy.

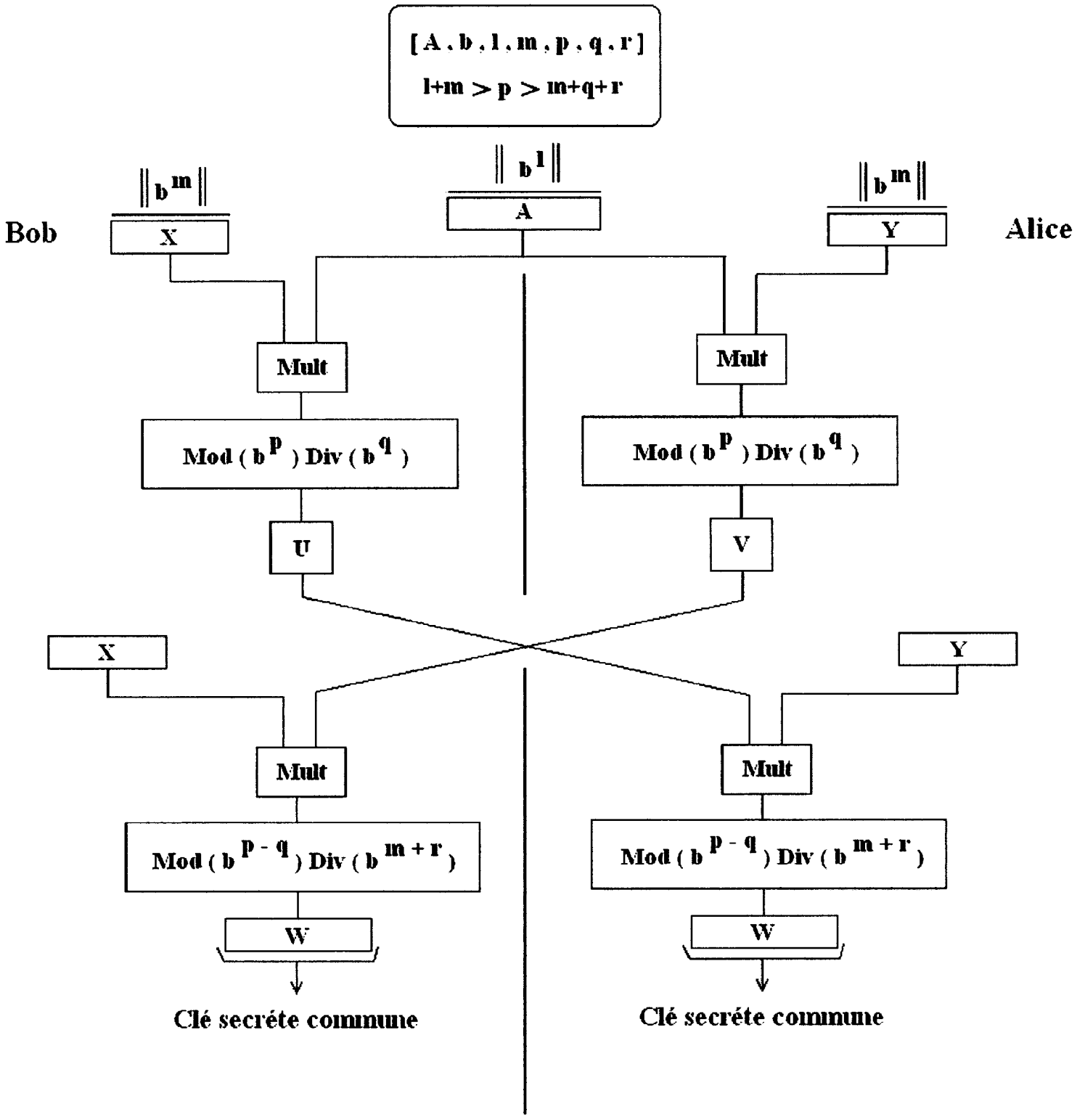
[A , b , l , m , p , q , r]
l+m > p > m+q+r
Bob
Alice
A
X
Y
Mult
Mult
Mod (b p) Div (b q)
Mod (b p) Div (b q)
U
V
X
Y
Mult
Mult
Mod (b p - q) Div (b m + r)
Mod (b p - q) Div (b m + r)
W
W
Clé secréte commune
Clé secréte commune

Figure 1

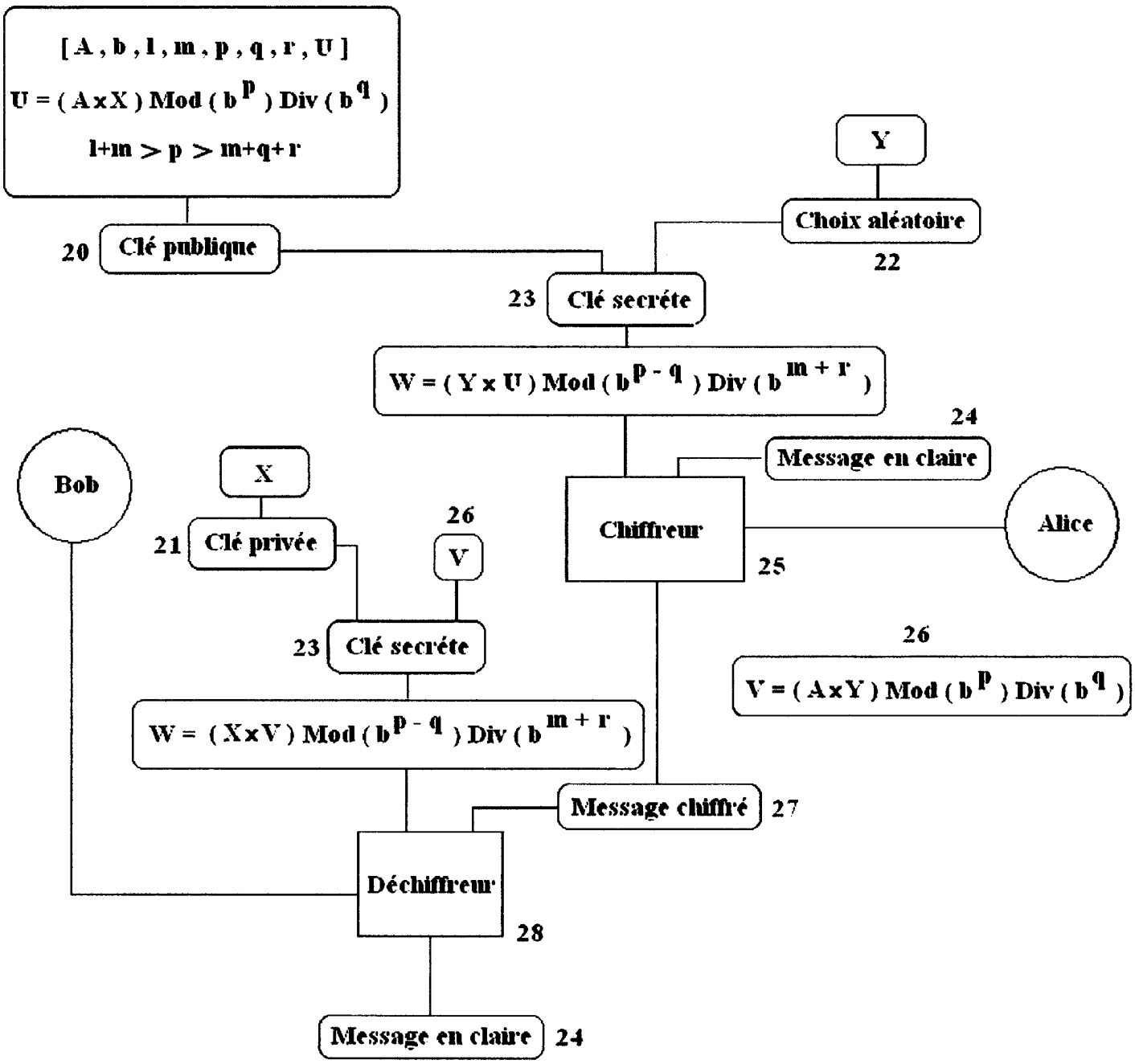
[A , b , l , m , p , q , r , U]
U = (A x X) Mod (b^p) Div (b^q)
l+m > p > m+q+r
20 Clé publique
Y
Choix aléatoire
22
23 Clé secréte
W = (Y x U) Mod (b^(p - q)) Div (b^(m + r))
24
Message en claire
Bob
X
21 Clé privée
26
V
Chiffreur
25
Alice
23 Clé secréte
26
V = (A x Y) Mod (b^p) Div (b^q)
W = (X x V) Mod (b^(p - q)) Div (b^(m + r))
Message chiffré 27
Déchiffreur
28
Message en claire 24

Figure 2

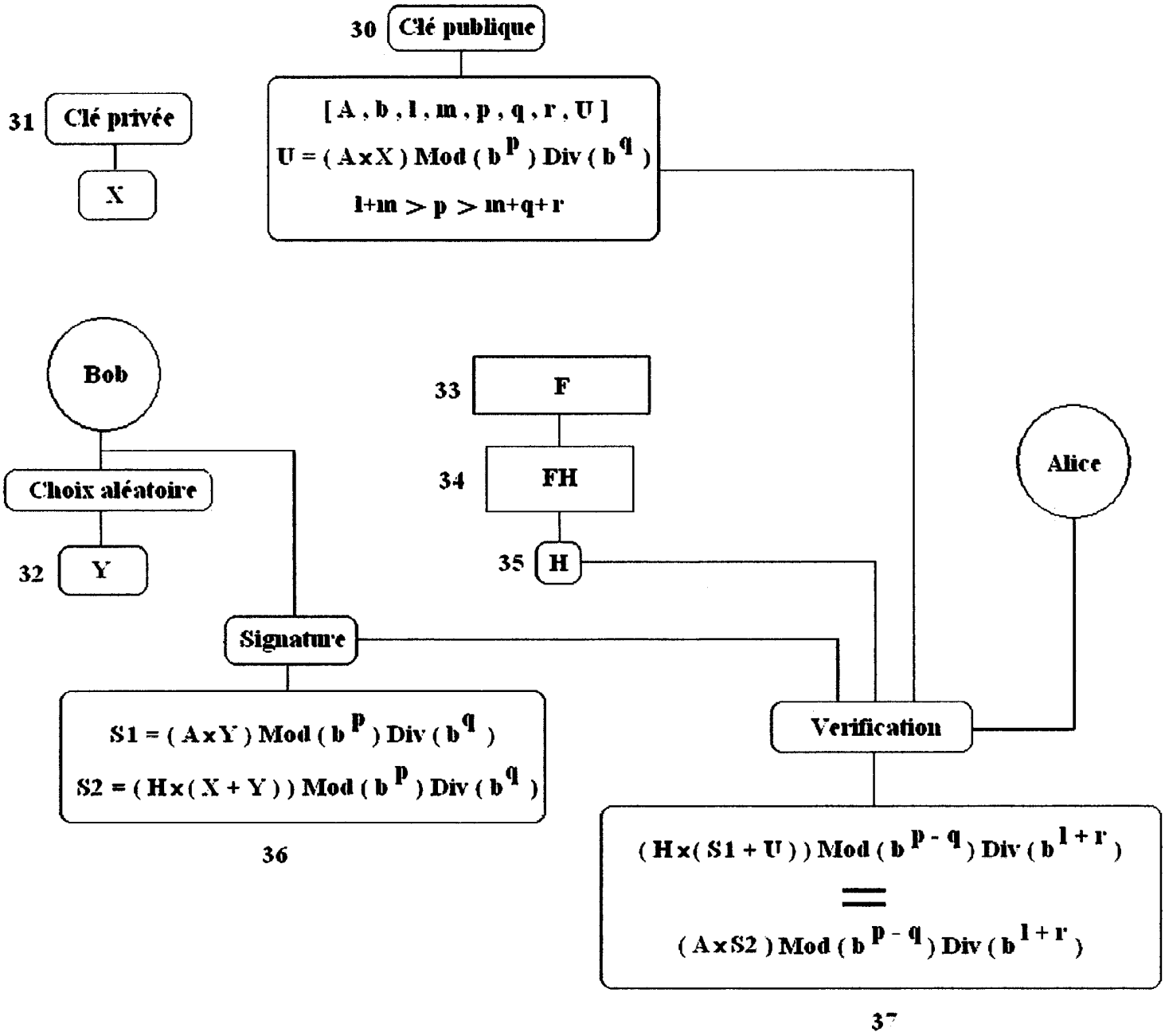
30 Clé publique
[A , b , l , m , p , q , r , U]
U = (A x X) Mod (b p) Div (b q)
l+m > p > m+q+r
31 Clé privée
X
Bob
Choix aléatoire
32 Y
33 F
34 FH
35 H
Alice
Signature
S1 = (A x Y) Mod (b p) Div (b q)
S2 = (H x (X + Y)) Mod (b p) Div (b q)
36
Verification
(H x (S1 + U)) Mod (b p - q) Div (b l + r)
=
(A x S2) Mod (b p - q) Div (b l + r)
37

Figure 3

MA 38128A1

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 : 38128	Date de dépôt : 25/05/2015 ;
Déposant : BOUFTASS SAMIR	
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: F.Belafkih	**Date d'établissement du rapport** : 08/09/2016
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 : 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	**On a new fast public key cryptosystem** ; Samir Bouftass ; 17 Novembre 2014 ; http://cm.1-s.es/11-2014/fast-pk-crypto.pdf	1-4
A	New Directions in Cryptography ; Whitfield Diffie et Martin E. Hellman ; Novembre 1976; http://cs.unc.edu/~fabian/course_papers/diffie.hellman.pdf	1-4
A	A Method for Obtaining Digital Signatures and PublicKey Cryptosystems ; R. L. Rivest, A. Shamir, L. Adleman MIT Laboratory for Computer Science and Department of Mathematics ; Février 1978 https://people.csail.mit.edu/rivest/RivestShamirAdleman-AMethodForObtainingDigitalSignaturesAndPublicKeyCryptosystems.pdf	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 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 : On a new fast public key cryptosystem
D2 : New Directions in Cryptography
D3 : A Method for Obtaining Digital Signatures and PublicKey Cryptosystems

1. Nouveauté (N) :

Le document D1 divulgue une publication scientifique de l'inventeur de cette demande qui a exposé l'invention objet de la présente demande avant le dépôt du brevet, dans un cadre non confidentiel. Par ailleurs, la divulgation de l'invention par l'inventeur n'est pas opposable à la demande de brevet d'invention déposée par ce dernier pendant une période de un an dite "délai de grâce" précédant le dépôt de la demande, conformément à l'article 27 de la loi 17/97 qui stipule : « ...la divulgation de l'invention n'est pas prise en considération dans les cas suivants :

- Si elle a lieu dans les douze mois précédant la date du dépôt de la demande de brevet d'invention et a été effectuée, autorisée ou obtenue du titulaire de la demande de brevet d'invention..... ».

Toutefois, il convient de noter que ce délai de grâce n'est pas accordé par certains organismes de propriété industrielle.
Aucun des documents ci-dessus ne divulgue l'ensemble des caractéristiques techniques des revendications 1-4, ainsi l'objet desdites revendications est 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 D2 qui est considéré comme l'état de la technique le plus proche de l'objet de la présente demande divulgue un procédé d'échange de clés secrètes et ses applications dans le chiffrement asymétrique, caractérisé en ce que sa sécurité est basée sur la difficulté d'inverser une fonction à sens unique ; toutefois, l'utilisation de la fonction $f(x) = (A \times X)Mod(2^p)Div(2^q)$ n'a pas été divulgué dans l'état de la technique susmentionné et n'en découle pas de manière évidente.

Par conséquent, l'objet de la revendication 1 implique une activité inventive au sens de l'article 28 de la loi 17-97 modifiée et complétée par la loi 23-13.

Les revendications dépendantes 2-4 impliquent également, en tant que telles, une activité inventive au sens de l'article 28 de la loi 17-97 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.