(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
25 août 2011 (25.08.2011)

PCT

(10) Numéro de publication internationale
WO 2011/101598 A1

(51) Classification internationale des brevets :
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2011/050336

(22) Date de dépôt international :
17 février 2011 (17.02.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1051190 18 février 2010 (18.02.2010) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE - CNRS** [FR/FR]; 3 rue Michel-Ange, F-75016 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GABORIT, Philippe** [FR/FR]; 15 avenue Martial Valin, Crézin, F-87220 Feytiat (FR). **AGUILAR MELCHOR, Carlos** [ES/FR]; 9 rue François Villon, F-87000 Limoges (FR).

(74) Mandataire : **DERAMBURE Conseil**; 14 avenue d'Eylau, F-75116 Paris (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

[Suite sur la page suivante]

(54) Title : CRYPTOGRAPHIC METHOD FOR COMMUNICATING CONFIDENTIAL INFORMATION

(54) Titre : PROCEDE CRYPTOGRAPHIQUE DE COMMUNICATION D'UNE INFORMATION CONFIDENTIELLE

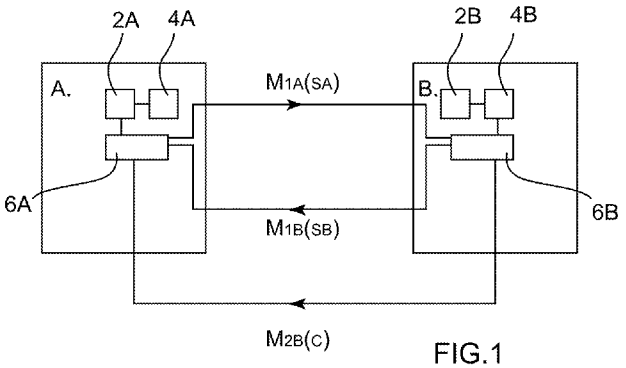

FIG.1

(57) Abstract : The invention relates to a cryptographic method for communicating confidential information m between a first electronic entity (A) and a second electronic entity (B), comprising a distribution step and a reconciliation step, the distribution step comprising a plurality of steps, one of which consists of the first entity (A) and the second entity (B) calculating a first intermediate value PA and a second intermediate value PB, respectively, such that: $P_A = Y_A.S_B = Y_A.X_B + Y_A.f(Y_B)$, and $P_B = Y_B.S_A = Y_B.X_A + Y_B\ f(Y_A)$, such that, during the reconciliation step, the first entity (A) can retrieve the confidential information by a process of decrypting a noisy message composed by the second entity (B) in particular from the second intermediate value PB.

(57) Abrégé :

[Suite sur la page suivante]

WO 2011/101598 A1

L'invention concerne un procédé cryptographique de communication d'une information confidentielle m entre une première entité (A) électronique et une deuxième entité (B) électronique comportant une étape de distribution et une étape de réconciliation, l'étape de distribution comportant plusieurs étapes, dont l'une consiste en ce que la première entité (A) et la deuxième entité (B) calculent respectivement une première valeur intermédiaire PA et une deuxième valeur intermédiaire PB, telles que : $P_A = Y_A.S_B = Y_A.X_B + Y_A.f(Y_B)$, et $P_B = Y_B.S_A = Y_B.X_A + Y_B\ f(Y_A)$, de sorte que, lors de l'étape de réconciliation, la première entité (A) soit capable de retrouver l'information confidentielle par une opération de déchiffrement d'un message bruité composé par la deuxième entité (B) à partir, notamment, de la deuxième valeur intermédiaire PB.

Procédé cryptographique de communication d'une information confidentielle

Domaine technique

L'invention concerne le domaine de la communication cryptographique d'une information confidentielle entre une première entité A et une deuxième entité B.

Plus particulièrement, l'invention concerne le domaine de la communication cryptographique d'une information confidentielle pouvant être réalisée sur un dispositifs cryptographiques à bas coût possédant des capacités de calcul limité, notamment des cartes à puce ou des étiquettes radio fréquence.

Selon un premier aspect l'invention concerne un procédé cryptographique de communication d'une information confidentielle entre une première entité et une deuxième entité.

Selon un autre aspect, l'invention concerne un programme d'ordinateur comprenant une pluralité d'instructions pour la mise en œuvre, à l'exécution, du procédé selon l'invention, un dispositif cryptographique comprenant des moyens de calculs agencés pour mettre en œuvre le procédé selon l'invention ainsi qu'un support de données comprenant un tel dispositif cryptographique.

Présentation de l'état de la technique et du problème technique

Il existe deux types d'approches pour le codage cryptographique.

Une première approche très répandue est basée sur l'algorithme RSA, de River, Shamir et Adleman, dont la sécurité réside dans la difficulté mathématique pour factoriser de grands nombres entiers.

Toutefois, un tel procédé cryptographique présente plusieurs inconvénients. En particulier, dans l'algorithme RSA, il est nécessaire de procéder à des calculs sur des clés publiques de grandes tailles, et notamment des calculs d'exponentielles discrètes. De tels calculs peuvent être lents, tout particulièrement lorsqu'ils sont implémentés sur des dispositifs cryptographiques à bas coût possédant des capacités de calcul limitées, tels que sur les cartes à puce ou les étiquettes radio fréquence.

Parmi les alternatives aux procédés cryptographiques d'authentification basés sur l'algorithme RSA, sont connus les procédés cryptographiques d'authentification utilisant un décodage de code correcteur d'erreurs à partir d'une matrice publique. Ces procédés ont l'avantage d'être la source de problèmes mathématiques NP-complets donc très difficiles à résoudre. Dès lors, ces procédés sont très sécurisés.

L'utilisation des codes correcteurs d'erreurs en cryptographie est connue depuis les années 1980. La demande EP-A-0 661 846 décrit un tel procédé cryptographique d'authentification utilisant un décodage de code correcteur d'erreurs à partir d'une matrice publique. Cette demande, ainsi que la publication du demandeur de cette demande, "A new identification scheme based on syndrome decoding", J. Stern 1993, décrivent un protocole d'authentification dit protocole par syndrome de Stern, utilisant une matrice publique aléatoire de très grande taille, typiquement de l'ordre de cent à mille kilobits. De même, la publication "Improved Identification schemes based on error-correcting codes", Veron, Applicable Alegbra in Engineering , Communication and Computing, 1 997, décrit une variante du protocole par syndrome, toujours dans le cadre d'un procédé cryptographique d'authentification utilisant un décodage de code correcteur d'erreurs à partir d'une matrice publique.

Toutefois, les contraintes de stockage des dispositifs cryptographiques à bas coûts ne permettent pas d'implémenter un tel protocole.

D'autres procédés de cryptographie connus de l'homme du métier sont basés sur le protocole Diffie-Hellman qui a servi de fondation à l'élaboration de nombreux développements concernant la cryptographie moderne.

Ce protocole a été décrit pour la première fois dans la publication « *New Directions in Cryptography* W. Diffie and M. E. Hellman, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976 » et consiste en ce que Alice et Bob partage une information confidentielle exp(ab) après avoir échangé une première information exp(a) et une seconde information exp(b), tels que a et b correspondent à des nombres entiers secrets et exp() à une fonction exponentielle dans le groupe G. La sécurité de ce protocole découle de la difficulté qui existe à inverser la fonction exponentielle de façon efficace et plus particulièrement de la difficulté qui existe à résoudre le problème exp(ab) à partir de exp(a) et exp(b).

Le protocole Diffie-hellman est utilisé dans de nombreuses applications mais présente un coût non négligeable puisque la résolution de problèmes exponentiels est, d'un point de vue algorithmique, l'une des fonctions arithmétiques les plus complexe. Ceux qui ont essayé de limiter ce coût en remplaçant la fonction exponentielle par d'autres fonctions ont rencontré de nombreuses difficultés et n'ont d'ailleurs jamais pu identifier une solution qui soit à la fois peu coûteuse en calculs et suffisamment sécurisée.

Il est également connu d'un domaine technique différent des solutions de cryptographie quantique ayant permis de résoudre des problèmes d'échange de clés confidentielles. Le protocole de communication quantique permet à Alice d'être en possession d'une variable aléatoire X et à Bob d'être en possession d'une version bruitée Y de la variable aléatoire X.

Ainsi, grâce à l'utilisation de protocoles de communication classiques Bob peut, lors d'une phase de réconciliation, écarter le bruit de la version bruitée Y de la variable aléatoire X et en déduire une information confidentielle. L'information confidentielle est ainsi partagée par Alice et Bob de façon inconditionnelle. Ce protocole de communication quantique est donc avantageux puisqu'il permet d'échanger une information confidentielle en ayant la certitude que celle-ci ne sera pas interceptée. Mais il présente l'inconvénient majeur de nécessiter l'utilisation d'un tunnel quantique entre Alice et Bob, ce qui est extrêmement contraignant d'un point de vue pratique.

Il existe donc un besoin non satisfait dans le domaine de la cryptographie pour la réalisation d'un protocole de communication qui permette d'échanger une information confidentielle sans être trop coûteux à la fois en terme de ressources et d'exécution, afin de pouvoir être intégré sur des dispositifs de cryptographie à bas coûts tels que des cartes à puce ou des puces d'identification radiofréquences (RFID) mais qui assure, néanmoins, un degré de sécurité qui soit suffisamment fiable et un temps de réponse suffisamment court.

Exposé de l'invention

L'invention vise donc à répondre à ces besoins non satisfaits.

A cet effet, l'invention vise un procédé cryptographique de communication d'une information confidentielle m entre une première entité (A) électronique et une deuxième entité (B) électronique comportant une étape de distribution et une étape de réconciliation, l'étape de distribution comportant plusieurs étapes consistant en ce que :

- d'une part, la première entité (A) :
  - calcule un premier syndrome $S_A = X_A + f(Y_A)$ à partir d'une première information secrète composée de deux éléments primaires X_A et Y_A appartenant à un anneau R et présentant une norme sensiblement petite vis-à-vis d'un élément $f(X_A)$ ou $f(Y_A)$,
    - l'anneau R possédant l'addition et la multiplication, et
    - f étant une loi de composition interne associant à tout élément X_I de l'anneau R un autre élément $f(X_I)$ de l'anneau R, et possédant la propriété que pour toute paire d'éléments X_I et Y_I de R, tels que X_I et Y_I ont une petite norme vis-à-vis des éléments $f(X_I)$ et $f(Y_I)$, alors $X_I.f(Y_I) - Y_I.f(X_I)$ est de petite norme, et
  - émet un premier message composé à partir de ce premier syndrome S_A de sorte que ledit premier syndrome S_A soit accessible par la deuxième entité (B),
- d'autre part, la deuxième entité (B) :
  - calcule un deuxième syndrome $S_B = X_B + f(Y_B)$ à partir d'une deuxième information secrète composée de deux éléments secondaires X_B et Y_B appartenant à l'anneau R et présentant une norme sensiblement petite vis-à-vis d'un élément $f(X_B)$ ou $f(Y_B)$,

- transmet à la première entité (A) un deuxième message composé à partir du deuxième syndrome S_B de sorte que ledit deuxième syndrome S_B soit accessible par la première entité (A),

- dans lequel lors de cette première étape de distribution, la première entité (A) et la deuxième entité (B) calculent respectivement une première valeur intermédiaire P_A et une deuxième valeur intermédiaire P_B, telles que :
  - $P_A = Y_A.S_B = Y_A.X_B + Y_A.f(Y_B)$, et
  - $P_B = Y_B.S_A = Y_B.X_A + Y_B\, f(Y_A)$,
  - de sorte que, lors de l'étape de réconciliation, la première entité (A) soit capable de retrouver l'information confidentielle par une opération de déchiffrement d'un message bruité composé par la deuxième entité (B) à partir, notamment, de la deuxième valeur intermédiaire P_B.

Selon une réalisation, le premier message émis par la première entité (A) est transmis directement à destination de la deuxième entité (B).

Selon une réalisation, le message bruité composé par la deuxième entité (B) lors de la phase de réconciliation comprend une donnée C obtenue à partir notamment de la deuxième valeur intermédiaire P_B et de l'information confidentielle m.

Selon une réalisation, la première entité (A) décode l'information confidentielle m à partir notamment du message bruité et de la première valeur intermédiaire P_A.

Selon une réalisation, l'information confidentielle m est encodée dans la donnée C du message bruité, par un code correcteur d'erreur.

Selon une réalisation, la donnée C du message bruité est telle que C = m.G + PB + e, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

Selon une réalisation, la donnée C du message bruité est telle que C = m.G + v[PB], avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p.

Selon une réalisation, la donnée C du message bruité est telle que C = m.G + v[PB] + e, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées,
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p,
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

Selon une réalisation, la première entité (A) compose une clé de chiffrement soit à partir de l'information confidentielle m, soit à partir de la deuxième valeur intermédiaire P_B, soit à partir d'une combinaison de l'information confidentielle et de la deuxième valeur intermédiaire P_B.

Selon une réalisation, après avoir émis le premier message composé à partir du premier syndrome S_A, la première entité (A) met ce premier message à disposition de la deuxième entité (B) dans un espace publique accessible au moins à une autre entité électronique.

Selon une réalisation, après avoir calculé le deusième syndrome SB, la deuxième entité (B) transmet, à la première entité (A) :

- le deuxième message composé à partir du deuxième syndrome S_B, et
- le message bruité composé à partir d'une donnée C obtenue à partir de la deuxième valeur intermédiaire P_B et de l'information confidentielle m.

Selon une réalisation, la première entité A décode l'information confidentielle à partir de du deuxième message et du message bruité.

Selon une réalisation, la première entité A décode l'information confidentielle m à partir de du deuxième syndrome SB composant le deuxième message, de la deuxième valeur intermédiaire PB composant le message bruité et de la première valeur intermédiaire PA.

Selon une réalisation, l'information confidentielle m est encodée dans la donnée C du message bruité, par un code correcteur d'erreur.

Selon une réalisation, la donnée C du message bruité est telle que C = m.G + PB + e, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

Selon une réalisation, la donnée C du message bruité est telle que C = m.G + v[PB], avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p.

Selon une réalisation, la donnée C du message bruité est telle que C = m.G + v[PB] + e, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées,
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p,
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

Selon une réalisation, la première entité (A) compose message d'authentification soit à partir de l'information confidentielle m, soit à partir de la deuxième valeur intermédiaire PB, soit à partir d'une combinaison de l'information confidentielle m et de la deuxième valeur intermédiaire PB.

Selon une réalisation, l'anneau R est l'anneau $F_q[x] / (X^n - 1)$, c'est-à-dire l'ensemble des polynômes à coefficients dans le corps F_q à q éléments pour lesquels on considère le reste par la division du polynôme $(X^n - 1)$.

Selon une réalisation, l'anneau R est l'anneau $F_q[x] / (X^n - 1)$, c'est-à-dire l'ensemble des polynômes à coefficients dans le corps F_q à q éléments pour lesquels on considère le reste par la division du polynôme $(X^n - 1)$.

Selon une réalisation, la norme correspond à la distance de hamming.

Selon une réalisation:

- n est sensiblement égale à 6000, et
- X_A, X_B, Y_A, Y_B présentent une norme égale à 35
- de sorte que la norme de $P_A - P_B$ est sensiblement égale à 2400.

Selon une réalisation, l'anneau R est l'anneau Z/pZ, c'est-à-dire l'ensemble des entiers modulo p moins le reste de la division par p.

Selon une réalisation, la norme est une norme euclidienne.

Selon une réalisation:

- p est sensiblement égale à 2500,
- f(x)=h.x modulo p avec h un nombre aléatoire plus petit que p, et/ou
- X_A, X_B, Y_A, Y_B sont des éléments de R de norme plus petite que racine (p).

Selon un autre aspect, l'invention concerne un programme d'ordinateur comprenant une pluralité d'instructions pour la mise en œuvre, à l'exécution, du procédé selon l'une quelconque des réalisations 1 à 24.

Selon un autre aspect, l'invention concerne dispositif cryptographique comprenant des moyens de calculs agencés pour mettre en œuvre le procédé selon l'une des réalisations 1 à 24.

Selon un autre aspect, l'invention concerne support de données comprenant un dispositif cryptographique selon l'invention.

Description des figures

Des exemples détaillés de réalisation de l'invention sont décrits, ci-dessous, en références aux figures annexées, dans lesquelles :

- la figure 1 est une représentation schématique d'une première réalisation du procédé cryptographique selon l'invention par lequel une première entité et une deuxième entité s'échangent une clé de chiffrement ;

- la figure 2 est une représentation schématique d'une deuxième réalisation du procédé cryptographique selon l'invention, par lequel une première entité communique un message chiffré à une deuxième entité ; et

- la figure 3 est une représentation schématique d'une troisième réalisation du procédé cryptographique selon l'invention, par lequel une première entité s'authentifie vis-à-vis d'une deuxième entité.

Il convient en premier lieu de souligner que dans le cadre de l'invention de terme de « message » correspond à tout type de signal ou bloc d'information véhiculé au travers d'un support physique ou d'ondes radiofréquences. Ces messages sont, par exemple, formés par une trame de données constituée d'une succession de « 0 » et de « 1 » caractérisant au moins une information pouvant être déduite d'une opération appropriée.

D'autre part, un « anneau » R peut être entendu comme toute structure algébrique sur laquelle deux opérations satisfont certaines des propriétés de l'addition et la multiplication. A cet égard, l'invention

propose d'utiliser comme structure algébrique, un anneau (R, +, x) connu publiquement plutôt qu'un groupe tel que l'utilisait le protocole traditionnel de Diffie-Hellman.

En outre, une « norme », ou distance, est une application sur l'anneau R à valeurs réelles positives et satisfaisant les hypothèses suivantes : séparation, homogénéité, sous additivité et sous multiplicative.

Un premier mode de réalisation du procédé selon l'invention est décrit en référence à la figure 1.

Selon cette première réalisation, le procédé cryptographique selon l'invention est utilisé pour réaliser un échange de clé de chiffrement permettant à une première entité A électronique, nommée Alice, et une deuxième entité B électronique, nommée Bob, d'échanger des informations confidentielles chiffrées. Pour lui permettre d'émettre, de recevoir et de stocker des données, Alice comporte une un processeur 2A, un espace mémoire 4A et une unité de communication 6A. De façon similaire, Bob comporte également un processeur 2B, un espace mémoire 4B et une unité de communication 6B.

Une première étape du procédé correspond à une étape dite de distribution.

Selon cette première étape, Alice et Bob s'échangent des données afin de se mettre d'accord sur un anneau R, un entier n et un élément h de l'anneau R. L'élément h est choisi de façon aléatoire et peut être considéré comme un équivalent du générateur utilisé dans le cadre de l'étape d'élévation de puissance du protocole de Diffie-Hellman.

Selon un exemple de réalisation, l'anneau R sélectionné correspond à $F_2[x]/(X^n-1)$, c'est-à-dire l'ensemble des polynômes à coefficients dans le corps F_2 à deux éléments pour lesquels on considère le reste par la division du polynôme $(X^n -1)$. On utilise alors comme fonction norme la distance de hamming.

Il convient de souligner que, de façon alternative, il serait également possible de sélectionner d'autres couples d'anneau R et de norme, parmi lesquels :

- l'anneau Z/pZ et la norme euclidienne ;
- l'anneau $(Z/pZ)[x]/(x^n-1)$ et la norme euclidienne également ; et
- l'anneau $(Z/p^rZ)[X]/(x^n-1)$ et pour norme le rang métrique.

Dans ce mode de réalisation, il est possible d'utiliser un code binaire doublement circulant C [2n, n] comprenant une matrice de vérification de parité de la forme $[I_n|H]$ où I_n est la matrice identité de taille n x n et h est telle que :

$$H = \begin{bmatrix} h_0 & h_{n-1} & \dots & h_1 \\ h_1 & h_0 & \dots & h_2 \\ h_2 & h_1 & \dots & h_3 \\ \dots & \dots & \dots & \dots \\ h_{n-1} & h_{n-2} & \dots & h_0 \end{bmatrix}$$

Après avoir sélectionnés l'anneau R, le générateur h et l'entier n, Alice et Bob sélectionnent séparément et de façon secrète un couple d'éléments primaires X_A, Y_A pour Alice et X_B, Y_B pour Bob de sorte que ces éléments primaires X_A, Y_A, X_B et Y_B sont de petite norme, et présentent donc une petite distance de Hamming, par rapport à un nombre réel positif w. Par exemple, pour un anneau R : F2[x]/(x^n-1) une telle petite distance de Hamming peut être de l'ordre de racine_carré(n)/10.

Alternativement, pour un mode de réalisation où l'anneau R sélectionné serait Z/pZ, un exemple de petite norme correspondant à la distance min(x,p-x) petit serait racine_carrée (p) / 100.

Alice et bob calculent ensuite respectivement les syndromes S_A et S_B à partir d'une fonction f telle que : $S_A = f(X_A,Y_A) = X_A.h + Y_A$ et $S_B = f(X_B,Y_B) = X_B.h + Y_B$, où f est une loi de composition interne associant à tout élément X_I de l'anneau R un autre élément $f(X_I)$ de l'anneau R et possédant la propriété que pour toute paire d'éléments X_I et Y_I de R, tels que X_I et Y_I ont une petite norme vis-à-vis des éléments $f(X_I)$ et $f(Y_I)$, alors $X_I.f(Y_I) - Y_I.f(X_I)$ est de petite norme.

Alice transmet à Bob un premier message $M_{1A}(S_A)$ composé notamment à partir du premier syndrome S_A de sorte que ledit premier syndrome S_A puisse être récupéré par Bob. Parallèlement, Bob transmet à Alice un deuxième message $M_{1B}(S_B)$ composé notamment à partir du deuxième syndrome S_B de sorte que ledit deuxième syndrome S_B puisse être récupéré par Alice.

Alice calcule alors une première valeur intermédiaire P_A, telle que :

- $P_A = Y_A.S_B = Y_A.X_B + Y_A.h.Y_B$.

Et Bob calcule de façon similaire une deuxième valeur intermédiaire P_B, telle que :

- $P_B = Y_B.S_A = Y_B.X_A + Y_B.h.Y_A$.

Dès lors, Alice et Bob sont respectivement en possession d'une première valeur intermédiaire P_A et d'une deuxième valeur intermédiaire P_B qui diffèrent l'une de l'autre par la valeur $Y_A.X_B - Y_B.X_A$. Or, puisque les éléments primaires X_A, Y_A, X_B et Y_B ont été sélectionnés de sorte qu'ils aient une petite norme vis-à-vis du paramètre w, et puisque la distance de hamming est sous multiplicative dans $F_2[x]/(X^n-1)$, alors la première valeur intermédiaire P_A détenue par Alice diffère de la deuxième valeur intermédiaire P_B détenue par Bob d'une valeur dont la norme est nécessairement inférieure à $2\ w^2$.

À l'issue de l'étape de distribution, Alice et Bob sont donc en possession de deux messages $M_{1A}(S_A)$ et $M_{1B}(S_B)$ correspondant à deux trames de données dont la première comporte le premier syndrome S_A et la deuxième comporte le deuxième syndrome S_B.

Intervient alors une seconde étape dite de réconciliation.

Selon un premier mode de réalisation la phase de réconciliation consiste en ce qu'Alice et Bob choisissent de manière publique une opération v[] consistant à sélectionner de façon aléatoire p bits parmi les n bits constituant les première et deuxième valeur intermédiaire P_A et P_B, tel qu'il existe une probabilité suffisante que ces p bits sélectionnés par Alice et Bob permettent d'en déduire une information commune.

Pour ce faire, Bob transmet à Alice un message bruité $M_{2B}(C)$ composé à partir d'une donnée C correspondant à un code correcteur d'erreur de longueur p permettant de corriger une erreur d'une valeur inférieure ou égale à $2w^2$ et tel que :

$$C = m.G + v[P_B] \text{ où}$$

- m représente alors une information confidentielle
- G représente la matrice génératrice d'un code correcteur d'erreur sur lesquels Alice et Bob se sont préalablement publiquement accordés
- v[]représente une opération de troncature consistant à extraire p bits parmi les n bits d'un vecteur.

Du fait de la construction ci-dessus, m.G est très bruité par rapport à $v[P_B]$.

Alice peut donc calculer la valeur de $C - v[P_A]$ et en déduire $m.G + v[P_B-P_A]$. Mais comme $v[P_B-P_A]$ est relativement petit, Alice est capable en utilisant le code correcteur d'erreur de corriger cette erreur $v[P_B-P_A]$ qui a été ajoutée à m.G et donc de retrouver l'information confidentielle m ainsi que $v[P_B]$.

Alice peut alors avantageusement composer une clé de chiffrement soit à partir de l'information confidentielle m. Mai s de façon alternative, il est également possible que cette clé de chiffrement soit composée à partir de la deuxième valeur intermédiaire P_B ou à partir d'une combinaison de l'information confidentielle m et de la deuxième valeur intermédiaire P_B.

Sont décrits dans le tableau ci-dessous, plusieurs exemples de paramètres pouvant être utilisés dans le protocole selon l'invention, dans lesquels :

- le paramètre n correspond au nombre de coordonnées des syndrome S_A et S_B ;
- le paramètre sb correspond au nombre de bits échangés de façon sécurisée dans le procédé ;

- code est le petit code C utilisé où BCH(255,55) X 1_3 correspond à la concaténation du code binaire BCH d'une distance de 55 concaténée avec un code de répétition de taille 3 ;
- ε est une majoration de la probabilité que le décodage soit erroné, obtenu à partir du taux d'erreur induit par $2w^2/n$ et de la capacité de correction de C ;
- security correspond à la sécurité du paramètre ; et
- complexity correspond au nombre de binaire nécessaire pour faire tourner le procédé d'un coté.

Ces paramètres sont choisis de sorte que $n2^{2w-r} = 2^{80}$.

n	w	sb	code C	ϵ	complexity	security
5000009	56	78	$BCH(127,15)$	3.10^{-3}	2^{23}	2^{80}
313603	100	131	$BCH(255,37)$	7.10^{-3}	2^{26}	2^{80}

Il convient de noter que dans ce premier mode de réalisation, la longueur de l'information confidentielle à décoder a été choisie de manière qu'aucune information ne soit perdue, ce qui limite la longueur code correcteur d'erreur utilisé pour le décodage.

Toutefois, selon un deuxième mode de réalisation, il est également envisageable d'utiliser toute la longueur des premier et deuxième syndromes S_A et S_B pour le décodage, en y ajoutant un vecteur erreur e. Ainsi, une attaque implique nécessairement la résolution d'un problème classique de décodage de syndrome pour un code correcteur d'erreur doublement circulant, ce qui le rend insoluble du fait de l'addition de l'erreur e.

Dans ce cas de figure, Alice et Bob se mettent publiquement d'accord sur une permutation P, un nombre t d'erreurs aléatoires et un code correcteur d'erreur de matrice génératrice G corrigeant un nombre d'erreurs de longueur p et de dimension k, avec un algorithme de décodage capable de résoudre un canal symétrique binaire avec une probabilité de transition $(2w^2+t)/n$.

Ensuite, Bob sélectionne une information confidentielle m qui est encodée sur une donnée C composant un message bruité $M_{2B}(C)$ tel que :

$$C = m.G + P[P_B] + e, \text{ où}$$

- G représente la matrice génératrice du code correcteur d'erreur,
- e représente le vecteur de t erreurs aléatoires de longueur m et de dimension k et
- $P[P_B]$ correspond à la permutation P de la deuxième valeur intermédiaire P_B.

A partir du message bruité, Alice peut donc calculer la valeur C + P[P_B], lui appliquer l'algorithme de décodage du code correcteur d'erreur et en déduire l'information confidentielle m, ainsi que le deuxième valeur intermédiaire P_B.

Ainsi, Alice peut composer une clé de chiffrement soit à partir de l'information confidentielle m ou comme précédemment, à partir de la deuxième valeur intermédiaire P_B ou d'une combinaison de l'information confidentielle m et de la deuxième valeur intermédiaire P_B.

De la même façon que précédemment, sont décrits dans le tableau ci-dessous, plusieurs exemples de paramètres pouvant être utilisés dans le protocole selon l'invention dans lesquels :

- le paramètre n correspond au nombre de coordonnées des syndrome S_A et S_B ;
- le paramètre sb correspond au nombre de bits échangés de façon sécurisée dans le procédé ;
- le paramètre t correspond au poids du vecteur d'erreur aléatoire ;
- code est le petit code C utilisé où BCH(255,55) X 1_3 correspond à la concaténation du code binaire BCH d'une distance de 55 concaténée avec un code de répétition de taille 3 ;
- ε est une majoration de la probabilité que le décodage soit erroné, obtenu à partir du taux d'erreur induit par $2w^2/n$ et de la capacité de correction de C ;
- security correspond à la sécurité du paramètre ; et
- complexity correspond au nombre de binaire nécessaire pour faire tourner le procédé d'un coté.

Ces paramètres sont choisis de sorte que $n2^{2w-r} = 2^{80}$.

n	w	t	sb	code C	ϵ	complexity	security
4451	33	150	78	$BCH(127,51) \otimes 1_{35}$	3.10^{-5}	2^{17}	2^{78}
4877	33	150	131	$BCH(255,37) \otimes 1_{19}$	1.10^{-2}	2^{17}	2^{78}
4877	34	150	91	$BCH(255,51) \otimes 1_{19}$	2.10^{-5}	2^{17}	2^{80}
5387	34	150	131	$BCH(255,37) \otimes 1_{21}$	3.10^{-8}	2^{17}	2^{80}
5387	34	150	91	$BCH(255,51) \otimes 1_{21}$	2.10^{-10}	2^{17}	2^{80}
5809	34	150	131	$BCH(255,51) \otimes 1_{23}$	3.10^{-10}	2^{18}	2^{80}
7829	44	150	131	$BCH(255,37) \otimes 1_{31}$	4.10^{-7}	2^{19}	2^{100}
11483	58	150	131	$BCH(255,37) \otimes 1_{45}$	7.10^{-7}	2^{20}	2^{120}

Il convient de souligner que, selon un troisième mode de réalisation, l'étape de réconciliation peut faire intervenir un message bruité $M_{2B}(C)$ tel que la donnée C comporte simultanément une opération de troncature sur la deuxième valeur intermédiaire PB et un vecteur d'erreurs aléatoire.

Une telle donnée C pourrait alors présenter la forme suivante C = m.G + v[P_B] + e.

La figure 2 représente un deuxième mode de réalisation de l'invention.

Selon ce deuxième mode de réalisation, le procédé de communication est utilisé pour permettre à Bob d'envoyer un message chiffré à l'attention de Alice selon un protocole de type El Gamal.

De même que précédemment, Alice comporte un processeur 2A, un espace mémoire 4A et une unité de communication 6A et Bob comporte un processeur 2B, un espace mémoire 4B et une unité de communication 6B.

La première étape du procédé correspond à l'étape de distribution.

Comme précédemment, Alice et Bob s'échangent préalablement des données afin de se mettre d'accord sur un anneau R, un entier n et un élément h de l'anneau R.

L'anneau R sélectionné correspond selon cet exemple à $F_2[x]/(X^n-1)$, c'est-à-dire l'ensemble des polynômes à coefficients dans le corps F_2 à deux éléments pour lesquels on considère le reste par la division du polynôme (X^n-1). On utilise alors comme fonction norme la distance de hamming.

De façon alternative, il serait également possible de sélectionner d'autres couples d'anneau R et de norme, parmi lesquels :

- l'anneau Z/pZ et la norme euclidienne ;
- l'anneau $(Z/pZ)[x]/(x^n-1)$ et la norme euclidienne également ; et
- l'anneau $(Z/p^rZ)[X]/(x^n-1)$ et pour norme le rang métrique.

Dans ce mode de réalisation, il est possible d'utiliser un code binaire doublement circulant C [2n, n] comprenant une matrice de vérification de parité de la forme $[I_n|H]$ où I_n est la matrice identité de taille n x n et h est telle que :

$$\mathbf{H} = \begin{bmatrix} h_0 & h_{n-1} & \dots & h_1 \\ h_1 & h_0 & \dots & h_2 \\ h_2 & h_1 & \dots & h_3 \\ \dots & \dots & \dots & \dots \\ h_{n-1} & h_{n-2} & \dots & h_0 \end{bmatrix}$$

Après avoir sélectionnés l'anneau R, le générateur h et l'entier n, Alice et Bob sélectionnent séparément et de façon secrète un couple d'éléments primaires X_A, Y_A pour Alice et X_B, Y_B pour Bob de sorte que ces éléments primaires X_A, Y_A, X_B et Y_B sont de petite norme, et présente donc une petite distance de Hamming, par rapport à un nombre réel positif w. Comme précédemment, pour un anneau R : F2[x]/(x^n-1) une telle petite distance de Hamming peut être de l'ordre de racine_carré(n)/10.

Alternativement, pour un mode de réalisation où l'anneau R sélectionné serait Z/pZ, un exemple de petite norme correspondant à la distance min(x,p-x) petit serait racine_carrée (p) / 100.

Alice et bob calculent ensuite respectivement les syndromes S_A et S_B à partir d'une fonction f telle que : $S_A = f(X_A,Y_A) = X_A.h + Y_A$ et $S_B = f(X_B,Y_B) = X_B.h + Y_B$, où f est une loi de composition interne associant à tout élément X_I de l'anneau R un autre élément $f(X_I)$ de l'anneau R et possédant la propriété que pour toute paire d'éléments X_I et Y_I de R, tels que X_I et Y_I ont une petite norme vis-à-vis des éléments $f(X_I)$ et $f(Y_I)$, alors $X_I.f(Y_I) - Y_I.f(X_I)$ est de petite norme.

Cet exemple de réalisation se distingue de celui de la figure 1 en ce que Alice ne transmet pas directement à Bob le premier message $M_{1A}(S_A)$ composé à partir du premier syndrome S_A. Au contraire, dans ce deuxième mode de réalisation, Alice émet le premier message $M_{1A}(S_A)$ et le met à disposition de Bob et d'autres entités électroniques dans un espace publique 10.

Ainsi, Bob peut récupérer le premier message $M_{1A}(S_A)$ et en déduire le premier syndrome S_A en interrogeant, par requête 12a, l'espace publique 10.

Bob calcule ensuite une deuxième valeur intermédiaire P_B, telle que :

- $P_B = Y_B.S_A = Y_B.X_A + Y_B.h.Y_A$.

Ainsi, Bob est en mesure de transmettre à Alice un message comprenant :

- un deuxième message $M_{1B}(S_B)$ de longueur k composé à partir du deuxième syndrome S_B, et
- un message bruité $M_{2B}(C)$ de longueur k composé à partir d'une donnée C obtenue à partir de la deuxième valeur intermédiaire P_B et de l'information confidentielle m.

Selon un premier mode de réalisation, la donnée C est telle que

$C = m.G + v[P_B]$, où

- m représente alors une information confidentielle de longueur k,
- G représente la matrice génératrice d'un code correcteur d'erreur sur lesquels Alice et Bob se sont préalablement publiquement accordés ; et
- v[] représente une opération de troncature consistant à extraire p bits parmi les n bits d'un vecteur, Alice et Bob s'étant préalablement accordées sur la valeur de p.

De même que précédemment, Alice peut alors décoder C à partir du deuxième message $M_{1B}(S_B)$ et du message bruité $M_{2B}(C)$ après avoir calculé P_A et $C + v[P_A]$. Alice en déduit alors m.G et l'information confidentielle m.

Sont décrits dans le tableau ci-dessous, plusieurs exemples de paramètres pouvant être utilisés dans le protocole selon l'invention, dans lesquels :

- le paramètre n correspond au nombre de coordonnées des syndrome S_A et S_B ;
- le paramètre sb correspond au nombre de bits échangés de façon sécurisée dans le procédé ;
- code est le petit code C utilisé où BCH(255,55) X 1_3 correspond à la concaténation du code binaire BCH d'une distance de 55 concaténée avec un code de répétition de taille 3 ;
- ε est une majoration de la probabilité que le décodage soit erroné, obtenu à partir du taux d'erreur induit par $2w^2/n$ et de la capacité de correction de C ;
- security correspond à la sécurité du paramètre ; et
- complexity correspond au nombre de binaire nécessaire pour faire tourner le procédé d'un coté.

Ces paramètres sont choisis de sorte que $n2^{2w-r} = 2^{80}$.

n	w	sb	code C	ε	complexity	security
5000009	56	78	$BCH(127,15)$	3.10^{-3}	2^{23}	2^{80}
313603	100	131	$BCH(255,37)$	7.10^{-3}	2^{26}	2^{80}

Selon un deuxième mode de réalisation, la donnée C est telle que

$C = m.G + P[P_B]$, où

- m représente alors une information confidentielle de longueur k
- G représente la matrice génératrice du code correcteur d'erreur ; et
- $P[P_A]$ correspond à la permutation P de la deuxième valeur intermédiaire P_A.

De façon similaire, Alice peut alors décoder C à partir du deuxième message $M_{1B}(S_B)$ et du message bruité $M_{2B}(C)$ après avoir calculé P_A et de $C + v[P_A]$ pour déterminer m.G et en déduire l'information confidentielle m.

De la même façon que précédemment, sont décrits dans le tableau ci-dessous, plusieurs exemples de paramètres pouvant être utilisés dans le protocole selon l'invention dans lesquels :

- le paramètre n correspond au nombre de coordonnées des syndrome S_A et S_B ;
- le paramètre sb correspond au nombre de bits échangés de façon sécurisée dans le procédé ;
- le paramètre t correspond au poids du vecteur d'erreur aléatoire ;
- code est le petit code C utilisé où BCH(255,55) X 1_3 correspond à la concaténation du code binaire BCH d'une distance de 55 concaténée avec un code de répétition de taille 3 ;
- ε est une majoration de la probabilité que le décodage soit erroné, obtenu à partir du taux d'erreur induit par $2w^2/n$ et de la capacité de correction de C ;

- security correspond à la sécurité du paramètre ; et
- complexity correspond au nombre de binaire nécessaire pour faire tourner le procédé d'un coté.

Ces paramètres sont choisis de sorte que $n2^{2w-r} = 2^{80}$.

n	w	t	sb	code C	ϵ	complexity	security
4451	33	150	78	$BCH(127,51) \otimes \mathbf{1}_{35}$	3.10^{-3}	2^{17}	2^{78}
4877	33	150	131	$BCH(255,37) \otimes \mathbf{1}_{19}$	1.10^{-2}	2^{17}	2^{78}
4877	34	150	91	$BCH(255,51) \otimes \mathbf{1}_{19}$	2.10^{-3}	2^{17}	2^{80}
5387	34	150	131	$BCH(255,37) \otimes \mathbf{1}_{21}$	3.10^{-8}	2^{17}	2^{80}
5387	34	150	91	$BCH(255,51) \otimes \mathbf{1}_{21}$	2.10^{-10}	2^{17}	2^{80}
5869	34	150	131	$BCH(255,51) \otimes \mathbf{1}_{23}$	3.10^{-10}	2^{18}	2^{80}
7829	44	150	131	$BCH(255,37) \otimes \mathbf{1}_{31}$	4.10^{-7}	2^{19}	2^{180}
11483	58	150	131	$BCH(255,37) \otimes \mathbf{1}_{43}$	7.10^{-7}	2^{20}	2^{130}

Il convient de souligner que, selon un troisième mode de réalisation, l'étape de réconciliation peut faire intervenir un message bruité $M_{2B}(C)$ tel que la donnée C comporte simultanément une opération de troncature sur la deuxième valeur intermédiaire PB et un vecteur d'erreurs aléatoire.

La figure 3 illustre à un troisième exemple de réalisation dans lequel le procédé selon l'invention est utilisé pour réaliser un protocole d'authentification.

Ce troisième exemple de réalisation fonctionne de la même façon que le deuxième exemple de réalisation. A l'issue du procédé tel que décrit précédemment, Alice renvoie l'information confidentielle m à Bob afin de garantir que Alice possède bien la clé privée correspondant aux deux éléments primaires X_A, Y_A associés à la clé publique correspondant au syndrome S_A.

REVENDICATIONS

1. Procédé cryptographique de communication d'une information confidentielle m entre une première entité (A) électronique et une deuxième entité (B) électronique comportant une étape de distribution et une étape de réconciliation, l'étape de distribution comportant plusieurs étapes consistant en ce que :

- d'une part, la première entité (A) :
  - calcule un premier syndrome $S_A = X_A + f(Y_A)$ à partir d'une première information secrète composée de deux éléments primaires X_A et Y_A appartenant à un anneau R et présentant une norme sensiblement petite vis-à-vis d'un élément $f(X_A)$ ou $f(Y_A)$,
    - l'anneau R possédant l'addition et la multiplication, et
    - f étant une loi de composition interne associant à tout élément X_I de l'anneau R un autre élément $f(X_I)$ de l'anneau R, et possédant la propriété que pour toute paire d'éléments X_I et Y_I de R, tels que X_I et Y_I ont une petite norme vis-à-vis des éléments $f(X_I)$ et $f(Y_I)$, alors $X_I.f(Y_I) - Y_I.f(X_I)$ est de petite norme, et
  - émet un premier message composé à partir de ce premier syndrome S_A de sorte que ledit premier syndrome S_A soit accessible par la deuxième entité (B),
- d'autre part, la deuxième entité (B) :
  - calcule un deuxième syndrome $S_B = X_B + f(Y_B)$ à partir d'une deuxième information secrète composée de deux éléments secondaires X_B et Y_B appartenant à l'anneau R et présentant une norme sensiblement petite vis-à-vis d'un élément $f(X_B)$ ou $f(Y_B)$,
  - transmet à la première entité (A) un deuxième message composé à partir du deuxième syndrome S_B de sorte que ledit deuxième syndrome S_B soit accessible par la première entité (A),
- caractérisé en ce que, lors de cette première étape de distribution, la première entité (A) et la deuxième entité (B) calculent respectivement une première valeur intermédiaire P_A et une deuxième valeur intermédiaire P_B, telles que :
  - $P_A = Y_A.S_B = Y_A.X_B + Y_A.f(Y_B)$, et
  - $P_B = Y_B.S_A = Y_B.X_A + Y_B\, f(Y_A)$,
  - de sorte que, lors de l'étape de réconciliation, la première entité (A) soit capable de retrouver l'information confidentielle par une opération de déchiffrement d'un message bruité composé par la deuxième entité (B) à partir, notamment, de la deuxième valeur intermédiaire PB.

2. Procédé cryptographique selon la revendication 1, dans lequel le premier message émis par la première entité (A) est transmis directement à destination de la deuxième entité (B).

3. Procédé selon la revendication 2, dans lequel le message bruité composé par la deuxième entité (B) lors de la phase de réconciliation comprend une donnée C obtenue à partir notamment de la deuxième valeur intermédiaire P_B et de l'information confidentielle m.

4. Procédé selon la revendication 3, dans lequel la première entité (A) décode l'information confidentielle m à partir notamment du message bruité et de la première valeur intermédiaire PA.

5. Procédé cryptographique selon la revendication 4, dans lequel l'information confidentielle m est encodée dans la donnée C du message bruité, par un code correcteur d'erreur.

6. Procédé cryptographique selon la revendication 5, dans lequel la donnée C du message bruité est telle que $C = m.G + P_B + e$, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

7. Procédé cryptographique selon la revendication 5, dans lequel la donnée C du message bruité est telle que $C = m.G + v[PB]$, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p.

8. Procédé cryptographique selon la revendication 5, dans lequel la donnée C du message bruité est telle que $C = m.G + v[PB] + e$, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées,
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p,
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

9. Procédé cryptographique selon l'une quelconque des revendications 1 à 8, dans lequel la première entité (A) compose une clé de chiffrement soit à partir de l'information confidentielle m, soit à partir de la deuxième valeur intermédiaire P_B, soit à partir d'une combinaison de l'information confidentielle et de la deuxième valeur intermédiaire P_B.

10. Procédé cryptographique selon la revendication 1, dans lequel, après avoir émis le premier message composé à partir du premier syndrome S_A, la première entité (A) met ce premier message à

disposition de la deuxième entité (B) dans un espace publique accessible au moins à une autre entité électronique.

11. Procédé cryptographique selon la revendication 10, dans lequel, après avoir calculé le deuxième syndrome S_B, la deuxième entité (B) transmet, à la première entité (A) :

- le deuxième message composé à partir du deuxième syndrome S_B, et
- le message bruité composé à partir d'une donnée C obtenue à partir de la deuxième valeur intermédiaire P_B et de l'information confidentielle m.

12. Procédé cryptographique selon la revendication 11, dans lequel la première entité A décode l'information confidentielle à partir du deuxième message et du message bruité.

13. Procédé cryptographique selon la revendication 11, dans lequel la première entité A décode l'information confidentielle m à partir du deuxième syndrome SB composant le deuxième message, de la deuxième valeur intermédiaire PB composant le message bruité et de la première valeur intermédiaire PA.

14. Procédé cryptographique selon l'une quelconque des revendications 11 à 13, dans lequel l'information confidentielle m est encodée dans la donnée C du message bruité, par un code correcteur d'erreur.

15. Procédé cryptographique selon la revendication 14, dans lequel la donnée C du message bruité est telle que C = m.G + PB + e, avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

16. Procédé cryptographique selon la revendication 14, dans lequel la donnée C du message bruité est telle que C = m.G + v[PB], avec :

- m qui représente l'information confidentielle,
- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées, et
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p.

17. Procédé cryptographique selon la revendication 14, dans lequel la donnée C du message bruité est telle que C = m.G + v[PB] + e, avec :

- m qui représente l'information confidentielle,

- G qui représente la matrice génératrice d'un code correcteur d'erreur sur lesquels la première entité A et la deuxième entité B se sont préalablement publiquement accordées,
- v[] qui représente une opération consistant à extraire p coordonnées parmi les n coordonnées d'un vecteur, la première entité A et la deuxième entité B s'étant préalablement accordées sur la valeur du p,
- e qui représente un vecteur d'erreurs aléatoires de longueur n et de norme petite, la première entité A et la deuxième entité B s'étant préalablement publiquement accordées sur la longueur n.

18. Procédé cryptographique selon l'une quelconque des revendications 9 à 17, dans lequel la première entité (A) compose message d'authentification soit à partir de l'information confidentielle m, soit à partir de la deuxième valeur intermédiaire PB, soit à partir d'une combinaison de l'information confidentielle m et de la deuxième valeur intermédiaire PB.

19. Procédé cryptographique selon l'une quelconque des revendications 1 à 18, dans lequel l'anneau R est l'anneau $F_q[x] / (X^n - 1)$, c'est-à-dire l'ensemble des polynômes à coefficients dans le corps F_q à q éléments pour lesquels on considère le reste par la division du polynôme $(X^n - 1)$.

20. Procédé cryptographique selon la revendication 19 dans lequel la norme correspond à la distance de hamming.

21. Procédé cryptographique selon la revendication 19 ou 20, dans lequel :
- n est sensiblement égale à 6000, et
- X_A, X_B, Y_A, Y_B présentent une norme égale à 35
- de sorte que la norme de $P_A - P_B$ est sensiblement égale à 2400.

22. Procédé cryptographique selon l'une quelconque des revendications 1 à 18, dans lequel l'anneau R est l'anneau Z/pZ, c'est-à-dire l'ensemble des entiers modulo p moins le reste de la division par p.

23. Procédé cryptographique selon la revendication 22, dans lequel la norme est une norme euclidienne.

24. Procédé selon la revendication 22 ou 23, dans lequel :
- p est sensiblement égale à 2500,
- f(x)=h.x modulo p avec h un nombre aléatoire plus petit que p, et/ou
- X_A, X_B, Y_A, Y_B sont des éléments de R de norme plus petite que racine (p).

25. Programme d'ordinateur comprenant une pluralité d'instructions pour la mise en œuvre, à l'exécution, du procédé selon l'une quelconque des revendications 1 à 24.

26. Dispositif cryptographique comprenant des moyens de calculs agencés pour mettre en œuvre le procédé selon l'une des revendications 1 à 24.

27. Support de données comprenant un dispositif cryptographique selon la revendication 26.

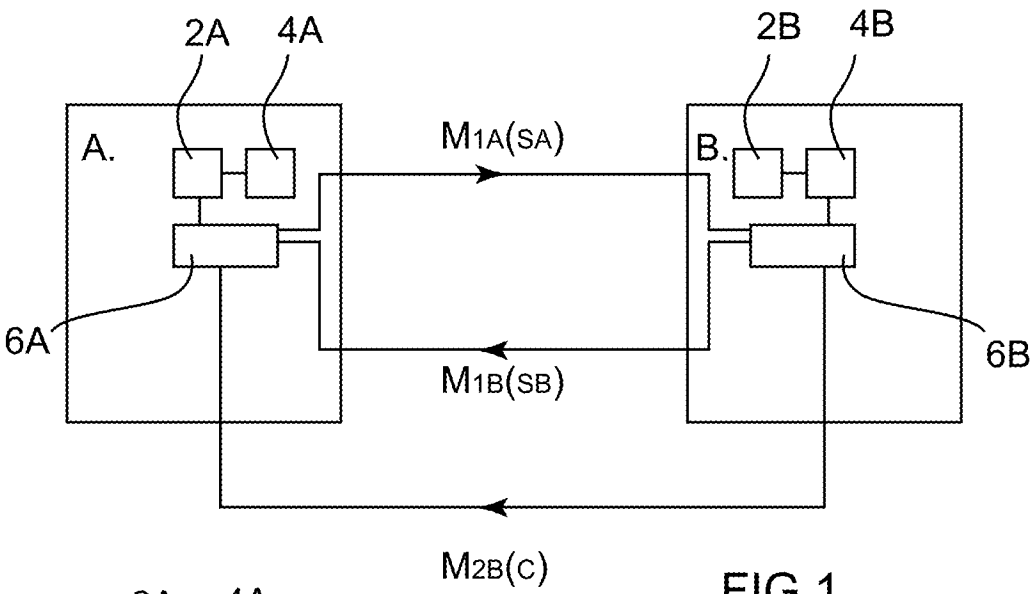
2A
4A
2B
4B
A.
B.
M1A(SA)
6A
6B
M1B(SB)
M2B(C)

FIG.1

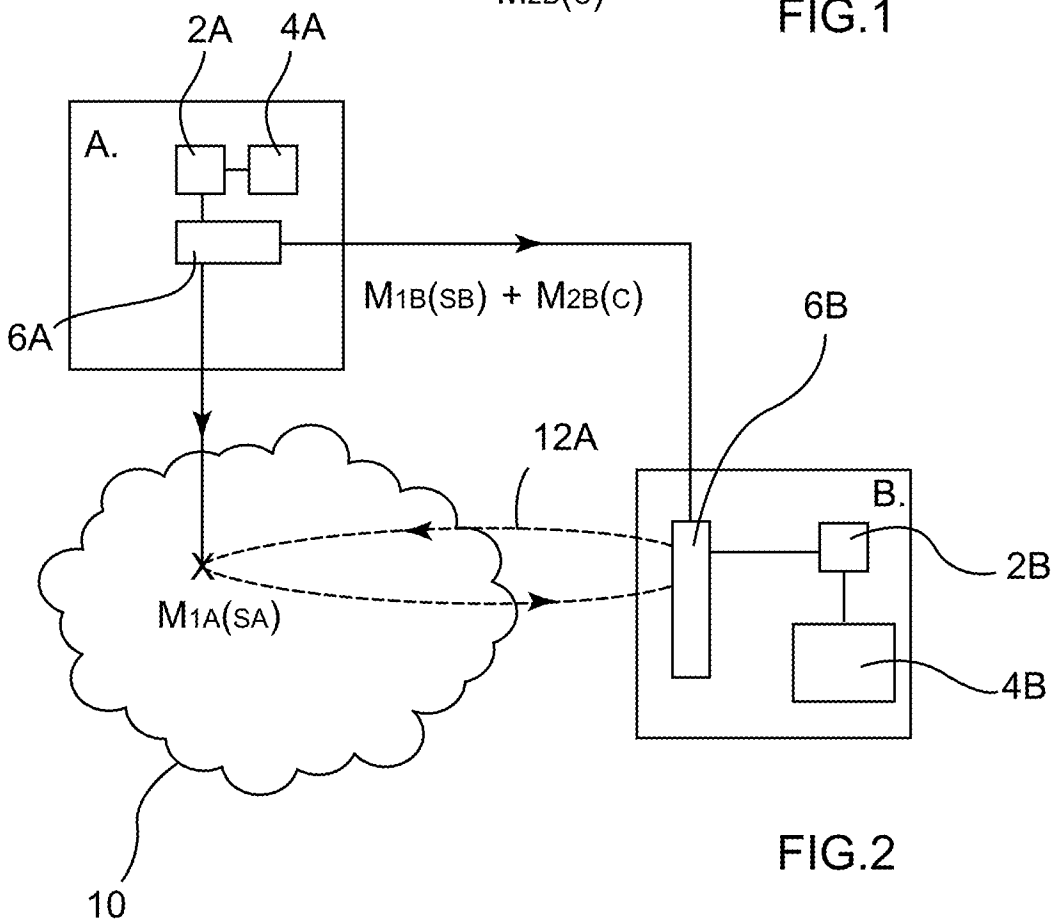
2A
4A
A.
6A
M1B(SB) + M2B(C)
6B
12A
B.
2B
M1A(SA)
4B
10

FIG.2

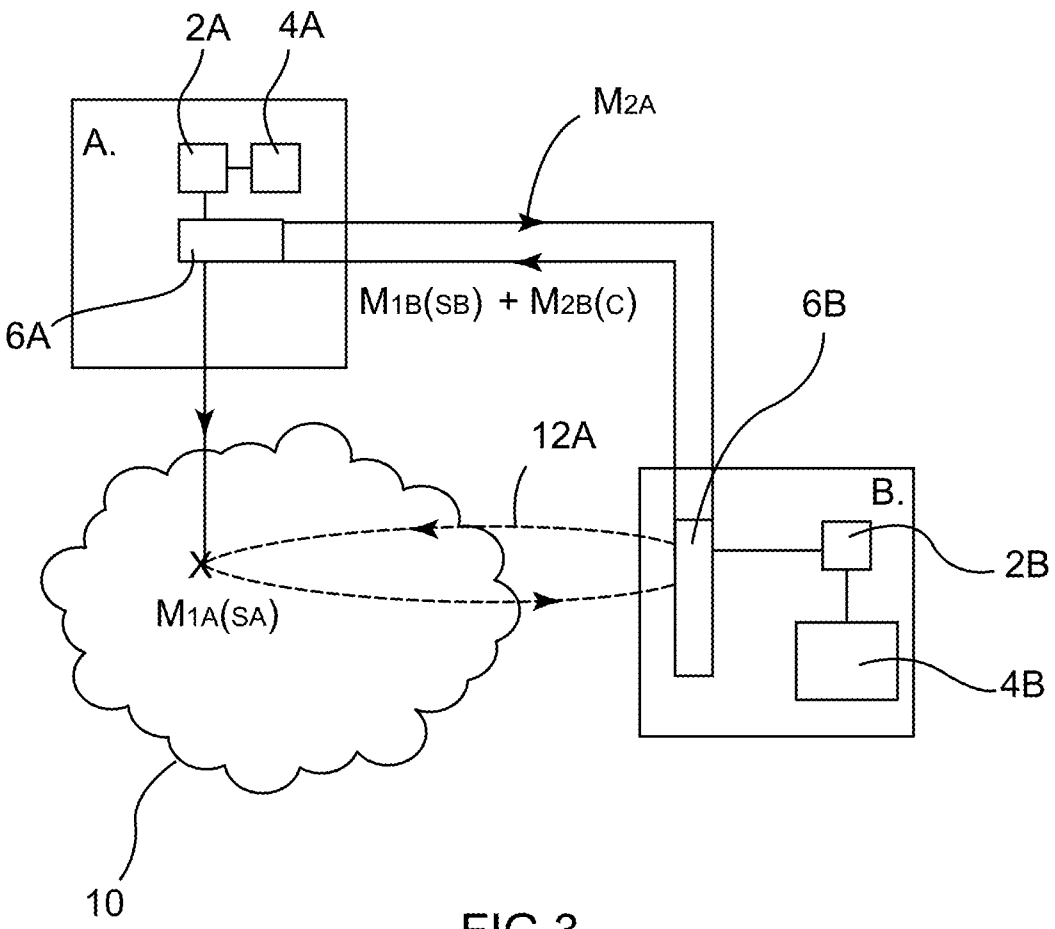

FIG.3

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2011/050336

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	REGEV O: "On lattices, Learning with Errors, Random Linear Codes, and Cryptography", INTERNET CITATION, 24 May 2005 (2005-05-24), pages 84-93, XP002497024, [retrieved on 2005-01-01] section 4 ----- -/--	1-27

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 June 2011	22/06/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Manet, Pascal

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2011/050336

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DIFFIE W ET AL: "NEW DIRECTIONS IN CRYPTOGRAPHY", IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE, US LNKD-DOI:10.1109/TIT.1976.1055638, vol. 22, no. 6, 1 November 1976 (1976-11-01), pages 644-654, XP000565260, ISSN: 0018-9448 the whole document	1-27
A	KASAHARA M: "A CONSTRUCTION OF PUBLIC-KEY CRYPTOSYSTEM USING ALGEBRAIC CODING ON THE BASIS OF SUPERIMPOSITION AND RANDOMNES", IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS,COMMUNICATIONS AND COMPUTER SCIENCES, ENGINEERING SCIENCES SOCIETY, TOKYO, JP, vol. E89A, no. 1, 1 January 2006 (2006-01-01), pages 47-54, XP001241425, ISSN: 0916-8508 the whole document	1-27

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2011/050336

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/08 H04L9/30
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	REGEV O: "On lattices, Learning with Errors, Random Linear Codes, and Cryptography", INTERNET CITATION, 24 mai 2005 (2005-05-24), pages 84-93, XP002497024, [extrait le 2005-01-01] section 4	1-27

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 juin 2011	22/06/2011

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Manet, Pascal

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2011/050336

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	DIFFIE W ET AL: "NEW DIRECTIONS IN CRYPTOGRAPHY", IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE, US LNKD-DOI:10.1109/TIT.1976.1055638, vol. 22, no. 6, 1 novembre 1976 (1976-11-01), pages 644-654, XP000565260, ISSN: 0018-9448 le document en entier	1-27
A	KASAHARA M: "A CONSTRUCTION OF PUBLIC-KEY CRYPTOSYSTEM USING ALGEBRAIC CODING ON THE BASIS OF SUPERIMPOSITION AND RANDOMNES", IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS,COMMUNICATIONS AND COMPUTER SCIENCES, ENGINEERING SCIENCES SOCIETY, TOKYO, JP, vol. E89A, no. 1, 1 janvier 2006 (2006-01-01), pages 47-54, XP001241425, ISSN: 0916-8508 le document en entier	1-27