(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
29 décembre 2016 (29.12.2016)

WIPO | PCT

(10) Numéro de publication internationale
WO 2016/207527 A1

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

(21) Numéro de la demande internationale : PCT/FR2016/051499

(22) Date de dépôt international : 20 juin 2016 (20.06.2016)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1555726 22 juin 2015 (22.06.2015) FR

(71) Déposant : **ORANGE** [FR/FR]; 78 rue Olivier de Serres, 75015 Paris (FR).

(72) Inventeurs : **CANARD, Sébastien**; 15 rue Alexandre Bigot, 14000 Caen (FR). **SANDERS, Olivier**; 9 rue de la Châtaigneraie, 35230 Bourgbarre (FR).

(74) Mandataire : **ORANGE/IPL**; RENARD Béatrice, 38-40 rue du Général Leclerc, 92794 Issy Moulineaux Cedex 9 (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, 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,

[Suite sur la page suivante]

(54) Title : METHOD FOR CONVERTING A FIRST CIPHER INTO A SECOND CIPHER

(54) Titre : PROCÉDÉ DE CONVERSION D'UN PREMIER CHIFFRÉ EN UN DEUXIÈME CHIFFRÉ

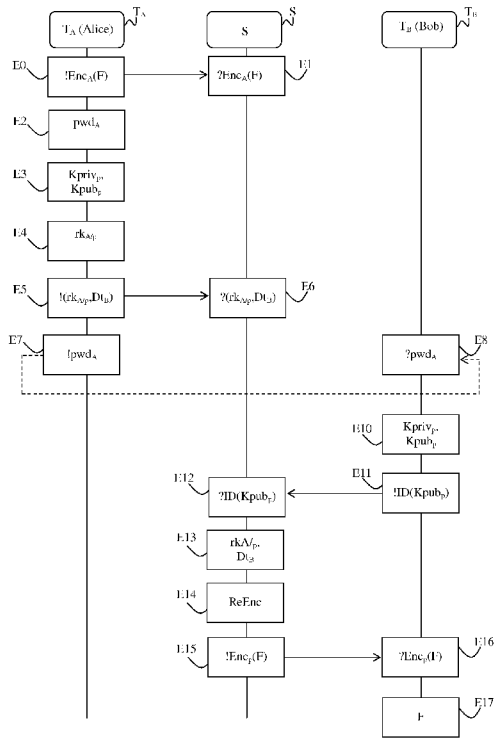


Figure 1

(57) Abstract : The invention concerns a method for converting a first cipher (F) into a second cipher, the method comprising the following steps, implemented by a secure storage server (S): - receiving (E1) the first cipher ($Enc_A(F)$), said first cipher being obtained by encrypting a piece of data by means of a public key ($Kpub_A$) of the user of a first device, - receiving (E6), from the first device, a re-encryption key ($rk_{A/p}$), said re-encryption key being calculated by applying a re-encryption key generation algorithm to the private key ($Kpriv_A$) associated with the public key of the user and to a second public key ($Kpub_p$) associated with a second private key ($Kpriv_p$), said second private key being derived from a password (pwd_A) chosen by the user of the first device, - converting (E14) the first cipher ($Enc_A(F)$) into a second cipher ($Enc_p(F)$) by applying a re-encryption algorithm to the first cipher and to the re-encryption key, said second cipher being arranged to be decrypted by a second user device by means of the second public key, said second device receiving the password from the first device on a communication channel independent of the secure server, deriving the second private key from said password and obtaining, from the server, the associated second public key.

(57) Abrégé :

[Suite sur la page suivante]

WO 2016/207527 A1

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, KM, ML, MR, NE, SN, TD, TG).

Publiée :

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

L'invention concerne un procédé de conversion d'un premier chiffré (F) en un deuxième chiffré, le procédé comprenant les étapes suivantes, mises en œuvre par un serveur de stockage sécurisé (S) : - réception (E1) du premier chiffré ($Enc_A(F)$), ledit premier chiffré étant obtenu par chiffrement d'une donnée au moyen d'une clé publique ($Kpub_A$) de l'utilisateur d'un premier dispositif, - réception (E6) en provenance du premier dispositif d'une clé de re-chiffrement ($rk_{A/p}$), ladite clé de re-chiffrement étant calculée en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée ($Kpriv_A$) associée à la clé publique de l'utilisateur et à une deuxième clé publique ($Kpub_p$) associée à une deuxième clé privée ($Kpriv_p$), ladite deuxième clé privée étant dérivée d'un mot de passe (pwd_A) choisi par l'utilisateur du premier dispositif, - conversion (E14) du premier chiffré ($Enc_A(F)$) en un deuxième chiffré ($Enc_p(F)$) par application d'un algorithme de re-chiffrement au premier chiffré et à la clé de re-chiffrement, ledit deuxième chiffré étant agencé pour être déchiffré par un deuxième dispositif utilisateur au moyen de la deuxième clé publique, ledit deuxième dispositif recevant le mot de passe du premier dispositif sur un canal de communication indépendant du serveur sécurisé, dérivant la deuxième clé privée dudit mot de passe et obtenant du serveur la deuxième clé publique associée.

Procédé de conversion d'un premier chiffré en un deuxième chiffré

La présente invention porte sur le domaine de la protection des données personnelles et/ou sensibles au moyen de cryptographie à clé publique. Plus précisément l'invention concerne un procédé adapté pour re-chiffrer, ou transchiffrer, ou convertir, un premier contenu chiffré propre à un premier utilisateur en un deuxième contenu chiffré propre à un deuxième utilisateur, et un système associé dans lequel le deuxième utilisateur n'est initialement pas inscrit au système de cryptographie à clé publique.

L'invention trouve une application particulièrement intéressante dans le cadre de l'informatique dématérialisée, ou « informatique dans le nuage » (« cloud computing » en anglais), dans lequel un fournisseur de services propose à des utilisateurs des solutions de stockage ou de transfert de données sécurisées sans que le fournisseur de services n'ait la possibilité d'accéder à ces données en clair.

On connaît des solutions de re-chiffrement ou de conversion de contenus chiffrés à base de cryptographie à clé publique qui permettent à plusieurs utilisateurs, par exemple Bob et Alice, d'échanger de façon sécurisée des documents sans qu'un fournisseur de services, intermédiaire dans l'échange, ne prenne connaissance des documents. Dans un tel système, Bob et Alice détiennent respectivement une paire de clés cryptographiques asymétriques : une clé privée et une clé publique associée. Ces paires de clés sont associées à un algorithme de chiffrement, à un algorithme de déchiffrement et à un algorithme de calcul d'une clé de re-chiffrement. L'algorithme de re-chiffrement permet de convertir un contenu chiffré propre à Alice en un contenu chiffré propre à Bob sans que l'entité qui procède au re-chiffrement n'accède au contenu en clair. Un tel exemple est décrit dans le document « Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption », de Benoît Libert et Damien Vergnaud, PKC 2008, LNCS 4939, pp.360-379, 2008. La clé de re-chiffrement associe ainsi la clé privée du déléguant, par exemple Alice, et la clé publique du délégué, Bob et permet ensuite à un équipement mandataire (le terme habituellement utilisé est le terme anglais « proxy ») de transformer un chiffré propre à Alice, obtenu au moyen de la clé publique d'Alice, en un chiffré propre à Bob, sans que la confidentialité des données manipulées ne soit à un instant donné compromise.

Habituellement, il est nécessaire que les utilisateurs impliqués soient connus du système qui met en œuvre le re-chiffrement. En ce sens, il faut que les utilisateurs soient préalablement inscrits de manière à avoir obtenus des données d'accréditation (le terme habituellement utilisés est le terme anglais « credentials »), typiquement des clés cryptographiques et plus précisément en cryptographie à clé publique, un couple clé privée/clé publique. Ainsi, pour qu'Alice puisse

partager un document avec Bob, elle doit nécessairement utiliser la clé publique de Bob. Or, si Bob n'est pas connu du système, cette clé publique n'existe pas et Alice ne peut pas procéder de manière classique au re-chiffrement d'un document pour le partager de manière sécurisée avec Bob.

Un des buts de l'invention est de remédier à des insuffisances/inconvénients de l'état de la technique et/ou d'y apporter des améliorations.

A cette fin, l'invention propose un procédé de conversion d'un premier chiffré en un deuxième chiffré, le procédé comprenant les étapes suivantes, mises en œuvre par un serveur de stockage sécurisé :

- réception du premier chiffré, ledit premier chiffré étant obtenu par chiffrement d'une donnée au moyen d'une clé publique de l'utilisateur d'un premier dispositif,

- réception en provenance du premier dispositif d'une clé de re-chiffrement, ladite clé de re-chiffrement étant calculée en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée associée à la clé publique de l'utilisateur et à une deuxième clé publique associée à une deuxième clé privée, ladite deuxième clé privée étant dérivée d'un mot de passe choisi par l'utilisateur du premier dispositif,

- conversion du premier chiffré en un deuxième chiffré par application d'un algorithme de re-chiffrement au premier chiffré et à la clé de re-chiffrement, ledit deuxième chiffré étant agencé pour être déchiffré par un deuxième dispositif utilisateur au moyen de la deuxième clé publique, ledit deuxième dispositif recevant le mot de passe du premier dispositif sur un canal de communication indépendant du serveur sécurisé, dérivant la deuxième clé privée dudit mot de passe et obtenant du serveur la deuxième clé publique associée.

Le procédé de conversion permet ainsi à l'utilisateur du premier dispositif et à l'utilisateur du deuxième dispositif de partager des données de manière sécurisée par l'intermédiaire du serveur de stockage sécurisé. Ce partage se fait sans que le serveur n'accède à la donnée en clair et surtout sans qu'il soit nécessaire que l'utilisateur du deuxième dispositif s'inscrire au service de stockage sécurisé délivré par le serveur. Le service de stockage sécurisé ainsi offert est très souple d'utilisation pour les deux utilisateurs. Le premier utilisateur n'est pas contraint de vérifier préalablement au partage d'une donnée avec le deuxième utilisateur que celui-ci est abonné au même service de stockage sécurisé que lui. Le deuxième utilisateur n'est quant à lui pas obliger de s'inscrire au service pour accéder de manière sécurisée à des données du premier utilisateur. Ce service est ainsi très avantageux dans le cadre d'un partage ponctuel, et sécurisé, de données entre les deux utilisateurs.

L'invention concerne aussi un procédé de stockage sécurisé d'une donnée sur un serveur sécurisé, ledit procédé étant mis en œuvre par un premier dispositif utilisateur à l'attention d'un deuxième dispositif utilisateur, l'utilisateur du premier dispositif détenant une clé privée et une clé publique associée, ledit procédé comprenant :

- génération d'une deuxième clé privée, ladite deuxième clé privée étant dérivée d'un mot de passe choisi par l'utilisateur du premier dispositif, et obtention de la deuxième clé publique associée,
- envoi dudit mot de passe à un utilisateur du deuxième dispositif sur un canal de communication indépendant du serveur sécurisé,
- calcul d'une clé de re-chiffrement en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée associée à la clé publique de l'utilisateur et à la deuxième clé publique associée,
- envoi de ladite clé de re-chiffrement au serveur sécurisé.

Le procédé est mis en œuvre ici le premier dispositif utilisateur.

Le mot de passe est envoyé par l'utilisateur du premier dispositif au deuxième utilisateur sur un canal de communication indépendant du canal utilisé entre les dispositifs et le serveur sécurisé. Cela garantit un niveau de sécurité élevé pour les deuxièmes clés qui sont générées et utilisées pour le calcul de la clé de re-chiffrement et pour le déchiffrement par le deuxième utilisateur.

L'invention concerne aussi un procédé d'obtention d'un premier chiffré généré par un premier dispositif et converti en un deuxième chiffré pour un deuxième dispositif utilisateur, ledit premier chiffré étant stocké sur un serveur, le procédé comprenant les étapes suivantes, mises en œuvre par le deuxième dispositif :

- réception en provenance du premier dispositif d'un mot de passe, ledit mot de passe étant reçu sur un canal de communication indépendant du serveur sécurisé,
- génération d'une clé privée, ladite clé privée étant dérivée du mot de passe, et obtention de la deuxième clé publique associée,
- envoi au serveur d'une requête d'obtention de la donnée chiffrée,
- réception en provenance du serveur de la donnée chiffrée,
- déchiffrement de la donnée chiffrée au moyen de la deuxième clé publique associée.

Le procédé est mis en œuvre ici par le deuxième dispositif utilisateur.

Le deuxième utilisateur déchiffre ainsi la donnée chiffrée stockée sur le serveur par le premier utilisateur à son attention sans prérequis par rapport au serveur en termes d'inscription éventuelle au service.

Avantageusement, le procédé d'obtention d'un premier chiffré comprend, dans une phase d'inscription définitive, les étapes suivantes mise en œuvre par le deuxième dispositif :

- génération d'une troisième clé privée et d'une troisième clé publique associée,
- envoi au serveur sécurisé d'une requête d'obtention de la clé de re-chiffrement,
- obtention de ladite clé de re-chiffrement,
- calcul d'une deuxième clé de re-chiffrement destinée à convertir un chiffré obtenu par application de l'algorithme de chiffrement à la clé publique en un deuxième chiffré destiné à être déchiffré au moyen de la troisième clé privée, ladite deuxième clé de re-chiffrement étant calculée à partir de la clé de re-chiffrement, de la deuxième clé privée et de la troisième clé privée.

Le procédé permet à l'utilisateur du deuxième dispositif, qui a échangé une ou plusieurs données chiffrées obtenues au moyen de la clé publique de l'utilisateur du premier dispositif, conformément aux étapes du procédé de conversion, de s'inscrire définitivement au service. L'utilisateur du deuxième dispositif génère ainsi un matériel cryptographique, en l'espèce la troisième clé privée et la troisième clé publique et calcule la deuxième clé de re-chiffrement qui lui permet d'échanger de façon pérenne, sécurisée et unidirectionnelle des données avec l'utilisateur du premier dispositif. Les étapes de ce procédé s'effectuent sans que l'utilisateur du deuxième dispositif ne fasse intervenir l'utilisateur du premier dispositif. Ce procédé est donc très souple. Par ailleurs, l'utilisateur du deuxième dispositif ne perd pas l'accès aux données qu'il a préalablement partagées avec l'utilisateur du premier dispositif.

Dans un exemple de réalisation, au moins un droit d'accès est associé au premier chiffré par le premier dispositif, un desdits droits définissant une période de validité du premier chiffré au terme de laquelle le serveur efface la clé de re-chiffrement.

Un droit d'accès associé au chiffré de la donnée que l'utilisateur du premier dispositif souhaite partager avec l'utilisateur du deuxième dispositif permet de définir de manière fine la façon dont l'utilisateur du deuxième dispositif accède à la donnée. Dans cet exemple, le partage entre les deux utilisateurs est limité dans le temps.

L'invention concerne aussi un serveur de stockage sécurisé, destiné à convertir un premier chiffré en un deuxième chiffré, le serveur comprenant :

- des premiers moyens de réception, agencés pour recevoir le premier chiffré, ledit premier chiffré étant obtenu par chiffrement d'une donnée au moyen d'une clé publique de l'utilisateur du premier dispositif,
- des deuxièmes moyens de réception, agencés pour recevoir en provenance du premier dispositif une clé de re-chiffrement, ladite clé de re-chiffrement étant calculée en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée associée à la clé publique de

l'utilisateur et à une deuxième clé publique associée à une deuxième clé privée, ladite deuxième clé privée étant dérivée d'un mot de passe choisi par l'utilisateur du premier dispositif,

- des moyens de conversion, agencés pour convertir le premier chiffré en un deuxième chiffré par application d'un algorithme de re-chiffrement au premier chiffré et à la clé de re-chiffrement, ledit deuxième chiffré étant agencé pour être déchiffré par un deuxième dispositif utilisateur au moyen de la deuxième clé publique, ledit deuxième dispositif recevant le mot de passe du premier dispositif sur un canal de communication indépendant du serveur sécurisé, dérivant la deuxième clé privée dudit mot de passe et obtenant du serveur la deuxième clé publique associée.

L'invention porte également sur un terminal de stockage sécurisé d'une donnée sur un serveur sécurisé, un utilisateur du premier dispositif détenant une clé privée et une clé publique associée, ledit terminal de stockage comprenant :

- des moyens de génération et d'obtention, agencés pour générer une deuxième clé privée, ladite deuxième clé privée étant dérivée d'un mot de passe choisi par l'utilisateur du terminal de stockage, et pour obtenir la deuxième clé publique associée,

- des premiers moyens d'envoi, agencés pour envoyer ledit mot de passe à un utilisateur d'un deuxième dispositif sur un canal de communication indépendant du serveur sécurisé,

- des moyens de calcul, agencés pour calculer une clé de re-chiffrement en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée associée à la clé publique de l'utilisateur et à la deuxième clé publique associée, et

- des deuxièmes moyens d'envoi, agencés pour envoyer ladite clé de re-chiffrement au serveur sécurisé.

L'invention porte également sur un terminal d'obtention d'un contenu, destiné à obtenir un premier chiffré généré par un premier dispositif et converti en un deuxième chiffré pour le terminal d'obtention, ledit premier chiffré étant stocké sur un serveur sécurisé, le terminal d'obtention comprenant :

- des premiers moyens de réception, agencés pour recevoir en provenance du premier dispositif un mot de passe, ledit mot de passe étant reçu sur un canal de communication indépendant du serveur sécurisé,

- des moyens de génération et d'obtention, agencés pour générer une clé privée, ladite clé privée étant dérivée du mot de passe, et pour obtenir la deuxième clé publique associée,

- des moyens d'envoi, agencés pour envoyer au serveur sécurisé une requête d'obtention de la donnée chiffrée,

- des deuxièmes moyens de réception, agencés pour recevoir en provenance du serveur la donnée chiffrée,

- des moyens de déchiffrement, agencés pour déchiffrer la donnée chiffrée au moyen de la deuxième clé publique associée.

L'invention concerne aussi un système de stockage sécurisé comprenant :

- un serveur de stockage sécurisé tel que décrit précédemment,
- au moins un terminal d'envoi d'une donnée tel que décrit précédemment, et
- au moins un terminal d'accès à une donnée stockée de manière sécurisée tel que décrit précédemment.

L'invention concerne aussi un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un serveur, le programme comprenant des instructions de code pour l'exécution des étapes du procédé de conversion d'un premier chiffré en un deuxième chiffré mises en œuvre par le serveur, lorsque le programme est exécuté sur ledit serveur.

L'invention concerne aussi un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal de stockage, le programme comprenant des instructions de code pour l'exécution des étapes du procédé de stockage sécurisé d'une donnée sur un serveur sécurisé, mises en œuvre par le terminal de stockage, lorsque le programme est exécuté sur ledit terminal.

L'invention concerne aussi un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un deuxième terminal d'obtention d'un contenu, le programme comprenant des instructions de code pour l'exécution des étapes du procédé d'obtention d'un premier chiffré mises en œuvre par le terminal d'obtention d'un contenu, lorsque le programme est exécuté sur ledit terminal.

D'autres caractéristiques et avantages de la présente invention seront mieux compris de la description et des dessins annexés parmi lesquels :

- la figure 1 présente les étapes d'un procédé de conversion d'un premier chiffré en un deuxième chiffré, selon un premier exemple de réalisation ;
- la figure 2 présente les étapes d'un procédé d'inscription définitive à un service de stockage sécurisé pour une personne initialement non abonnée, selon un exemple de réalisation ;
- la figure 3 est une représentation schématique d'un serveur de stockage sécurisé, selon un exemple de réalisation ;
- la figure 4 est une représentation schématique d'un terminal de stockage sécurisé, selon un exemple de réalisation ;
- la figure 5 est une représentation schématique d'un terminal d'obtention d'un contenu, selon un exemple de réalisation.

Les étapes d'un procédé de conversion d'un premier chiffré en un deuxième chiffré, selon un premier exemple de réalisation, vont maintenant être décrites en relation avec la figure 1.

On considère que des utilisateurs, Alice et Bob, détenteurs respectivement des terminaux T_A, T_B, souhaitent partager des données de manière sécurisée en passant par l'intermédiaire d'un serveur de stockage sécurisé S. Le serveur de stockage S est agencé pour stocker des données ; il définit également des primitives cryptographiques qui permettent la mise en œuvre d'un stockage sécurisé. Les données sont par exemple des fichiers tels que des photos, des films, etc. Les primitives cryptographiques définissent de manière classique un algorithme de génération de clés, un algorithme de génération d'une clé de re-chiffrement, des algorithmes de chiffrement, de re-chiffrement, de déchiffrement, etc. Partager des données de façon sécurisée via un serveur de stockage est particulièrement avantageux dans le cas de fichiers volumineux. Les terminaux T_A et T_B sont des équipements informatiques, tels que des PC, des terminaux mobiles intelligents (on parle de « smartphone » en anglais), etc. agencés pour mettre en œuvre celles des étapes du procédé propres à chacun des terminaux d'utilisateur.

On suppose qu'Alice est connue du serveur de stockage sécurisé S. En ce sens elle s'est préalablement enregistrée auprès du serveur S afin d'accéder à un service de stockage sécurisé et a généré une première paire de clés asymétriques : une première clé privée $Kpriv_A$ et une première clé publique associée $Kpub_A$ générées au moyen de l'algorithme de génération de clés défini pour le serveur S. Alice a transmis la première clé publique $Kpub_A$ au serveur S. Par exemple, les primitives cryptographiques associées au serveur S sont conformes aux primitives décrites dans le document « Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption », de Benoît Libert and Damien Vergnaud, PKC 2008, LNCS 4939, pp.360-379, 2008 qui définit un schéma cryptographique appelé par la suite « schéma de Libert-Vergnaud ». Dans cet exemple, la clé secrète d'Alice, $KprivA = x_A$, où x_A est un aléa dans l'ensemble $\mathbb{Z}_p^*$ des entiers relatifs inférieurs à p et supérieurs à 0, et la clé publique associée est définie par : $KpubA = g^{x_A}$, où g est un élément d'un groupe bilinéaire G.

On suppose également que dans une phase initiale E0, Alice a transmis au serveur de stockage S une ou plusieurs données chiffrées pour stockage sécurisé. Par exemple, Alice a transmis sous forme chiffrée le fichier F, noté dans sa forme chiffrée $Enc_A(F)$. Alice a chiffré le fichier F au moyen de sa propre clé publique $Kpub_A$. A ce stade, seule Alice, qui détient la clé privée $Kpriv_A$ associée, est capable de déchiffrer le fichier chiffré $Enc_A(F)$. Le fichier chiffré est reçu et stocké par le serveur S dans une étape E1 de réception. On suppose qu'Alice souhaite partager cette donnée chiffrée avec Bob alors que Bob n'est pas connu du serveur S de stockage sécurisé. En particulier Bob n'a pas suivi la procédure standard de génération de clés telle que

décrite précédemment. Il a cependant reçu au moins une description des algorithmes de déchiffrement utilisés dans le cadre du stockage sécurisé sur le serveur S.

Dans un autre exemple de réalisation, c'est un autre utilisateur qui envoie les données chiffrées qu'il générées au moyen de la clé publique d'Alice.

Dans une étape suivante E2 de choix d'un mot de passe, Alice choisit un mot de passe pwd_A. Le mot de passe pwd_A comprend par exemple quelques caractères, ou correspond à une phrase complète (dans ce cas, on parle de « passphrase » en anglais). Ce mot de passe est destiné à être transmis à Bob afin qu'Alice et Bob partagent la connaissance d'un même mot de passe, et à générer un deuxième couple de clés privée/publique destiné à être utilisé pour calculer une clé de re-chiffrement.

Dans une étape suivante E3 de génération de clés, Alice commande la dérivation d'une deuxième clé privée $Kpriv_p$ à partir du mot de passe pwd_A, puis la génération d'une deuxième clé publique associée $Kpub_p$. La deuxième clé privée $Kpriv_p$ est ainsi générée au moyen d'un algorithme éprouvé de dérivation de clés à partir d'un mot de passe. Dans un exemple de réalisation, l'algorithme de dérivation de clés utilisé est conforme aux spécifications décrites dans le NIST Special Publication 800-132 : http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf. La deuxième clé privée $Kpriv_p$ a la même structure qu'une clé secrète générée dans le cadre du système de stockage S ; elle est de la forme x_p. La deuxième clé publique $Kpub_p$ associée est calculée au moyen de l'algorithme de génération de clés utilisé par le serveur de stockage S, en l'espèce l'algorithme de génération de clés du schéma de Libert-Vergnaud. Ainsi, la deuxième clé publique associée $Kpub_p$ est de la forme g^{x_p}. Au terme de l'étape E3 de génération de clés, Alice dispose du couple de clés $Kpriv_A = x_A$, $Kpub_A = g^{x_A}$ et du deuxième couple de clés $Kpriv_p = x_p$, $Kpub_p = g^{x_p}$, obtenu à partir du mot de passe pwd_A choisi par Alice.

Dans une étape suivante E4 de calcul d'une clé de re-chiffrement, Alice commande la génération d'une clé de re-chiffrement $rk_{A/p}$. A cette fin Alice applique au moyen de son terminal T_A l'algorithme de génération d'une clé de re-chiffrement du serveur de stockage S à la clé privée $Kpriv_A$ d'Alice et à la clé deuxième publique $Kpub_p$ nouvellement générée. Cette clé de re-chiffrement $rk_{A/p}$ est destinée à permettre le re-chiffrement de données chiffrées pour Alice en données chiffrées pour le détenteur de la deuxième clé privée $Kpriv_p$. Dans l'exemple de réalisation décrit ici, et conformément au schéma de Libert-Vergnaud, la clé de re-chiffrement $rk_{A/p}$ est calculée comme suit :

$$rk_{A/p} = (g^{x_p})^{1/x_a} = g^{x_p/x_a}$$

La clé de re-chiffrement d'une clé initiale, ici la clé publique d'Alice, vers une clé finale, ainsi calculée, ici la deuxième clé publique $Kpub_p$, a la forme d'un élément dont l'exposant est un quotient dans lequel le numérateur correspond à la clé privée finale et le dénominateur à la clé privée initiale.

Dans une étape E5 d'envoi d'un message, Alice envoie au serveur de stockage S un message M qui comprend la clé de re-chiffrement $rk_{A/p}$ nouvellement calculée, ainsi que des droits associés Dt_p destinés à préciser le cadre d'utilisation de cette clé de re-chiffrement. Plus précisément, les droits associés Dt_p comprennent un identifiant de la donnée chiffrée destinée à être partagée avec Bob et un identifiant de Bob. Dans cet exemple, les droits associés Dt_B comprennent le nom du fichier chiffré $Enc_A(F)$ qu'Alice a préalablement stocké sur le serveur de stockage S et la deuxième clé publique $Kpub_p$ associée à la deuxième clé privée $Kpriv_p$, dérivée du mot de passe pwd_A dans le cadre du partage de données avec Bob. Dans un exemple de réalisation, les droits associés Dt_p comprennent également une durée maximale d'utilisation de la clé ou/et un nombre maximal d'utilisation de la clé. La clé de re-chiffrement $rk_{A/p}$ et les droits associés Dt_p sont reçus et stockés par le serveur S dans une étape E6 de réception.

Dans une étape E7 d'envoi du mot de passe, Alice envoie à Bob le mot de passe pwd_A qu'elle a choisi au cours de l'étape initiale E2 de choix d'un mot de passe par un canal de communication indépendant du serveur de stockage S. Par exemple Alice envoie le mot de passe à Bob par e-mail, ou par SMS (de l'anglais « Short Message Service »). L'utilisation d'un canal indépendant est destinée à garantir un niveau de sécurité élevé. En effet, un attaquant qui intercepterait des données destinées au serveur S n'accèderait pas pour autant au mot de passe pwd_A. Le mot de passe pwd_A est reçu par Bob, plus précisément part le terminal T_B de Bob dans une étape E8 de réception.

On remarque que l'étape E7 d'envoi du mot de passe est indépendante des étapes précédentes E3 de génération de clés, E4 de calcul d'une clé de re-chiffrement et 53 d'envoi d'un message. Elle peut ainsi être mise en œuvre à n'importe quel moment après l'étape E2 de génération d'un mot de passe.

Les étapes E0 à E7 sont mises en œuvre par Alice au moyen de son terminal T_A et par le serveur S, et concernent la configuration du partage de données avec Bob.

Dans une deuxième phase, consécutive aux étapes décrites précédemment, Bob qui a été informé par Alice qu'elle avait mis à sa disposition sur le serveur de stockage S une donnée sensible chiffrée $Enc_A(F)$ met en œuvre les étapes suivantes afin d'accéder à la donnée sensible F. Typiquement, Bob est informé par Alice en même temps que celle-ci lui envoie le mot de passe au cours de l'étape E7 d'envoi du mot de passe.

Dans une étape E10 de génération de clés, Bob commande la génération de la deuxième clé privée $Kpriv_p = x_p$ à partir du mot de passe pwd_A reçu d'Alice au cours de l'étape E8, puis le calcul de la deuxième clé publique associée $Kpub_p = g^{x_p}$ en appliquant l'algorithme de génération de clés du serveur S. La génération de la deuxième clé privée $Kpriv_p$ à partir du mot de passe pwd_A et de la deuxième clé publique associée $Kpub_p$ utilise les mêmes algorithmes de génération que ceux utilisés par Alice, ici l'algorithme de dérivation de clés spécifié dans le NIST Special Publication 800-132 pour la deuxième clé privée et l'algorithme de génération de clés du schéma de Libert-Vergnaud pour la deuxième clé publique. Au terme de l'étape E10 de génération de clés, Bob dispose du deuxième couple de clés $Kpriv_p = x_p$ et $Kpub_p = g^{x_p}$, détenu également par Alice.

Dans une étape suivante E11 d'envoi d'une requête, Bob envoie au serveur de stockage S une requête d'obtention d'une donnée sensible qu'Alice ou un autre utilisateur a stockée chiffrée à son attention sur le serveur de stockage S. La requête comprend un identifiant de Bob, dans cet exemple la deuxième clé publique $Kpub_p = pk_p$. La requête est reçue par le serveur S dans une étape E12 de réception.

Dans une étape E13 d'obtention de données, le serveur de stockage S récupère, à partir de l'identifiant de Bob, la clé de re-chiffrement $rk_{A/p}$ associée par Alice à Bob et les droits Dt_p associés à la donnée sensible qu'Alice souhaite partager avec Bob.

Dans une étape E14 de conversion, le serveur de stockage S procède au re-chiffrement de la donnée chiffrée $Enc_A(F)$ associée à Bob par Alice, au moyen de la clé de re-chiffrement $rk_{A/p}$. A cette fin, le serveur S applique l'algorithme de re-chiffrement du schéma de Libert-Vergnaud à la clé de re-chiffrement $rk_{A/p}$ et à la donnée chiffrée EncA(F). Au terme de cette étape de conversion, la donnée chiffrée initialement chiffrée avec la clé publique d'Alice $Kpub_A = g^{x_A}$ est chiffrée au moyen de la deuxième clé publique $Kpub_p = g^{x_p}$ associée à la deuxième clé privée $Kpriv_p = x_p$ générée à partir du mot de passe pwd_A qu'Alice a transmis à Bob. Bob est ainsi capable d'accéder à la donnée F en clair en déchiffrant la donnée chiffrée au moyen de la deuxième clé privée $Kpriv_p$ qu'il a dérivée du mot de passe. Le donnée re-chiffrée est notée $Enc_p(F)$.

Dans une étape E15 d'envoi, le système de stockage envoie la donnée re-chiffrée $Enc_p(F)$ à Bob. Elle est reçue par Bob, plus précisément par le terminal T_B de Bob dans une étape E16 de réception.

Dans une étape E17 de déchiffrement, Bob déchiffre la donnée $Enc_p(F)$ re-chiffrée à son attention au cours de l'étape 14 de conversion. Il applique à cette fin l'algorithme de déchiffrement du serveur S à la donnée re-chiffrée $Enc_p(F)$ et à la deuxième clé privée

$Kpriv_p = x_p$ qu'il a générée à partir du mot de passe pwd_A. Il peut ainsi accéder à la donnée sensible F en clair.

Dans un exemple de réalisation où les droits Dt_B associés à la donnée sensible définissent une période de validité de la donnée sensible, le serveur de stockage S efface la clé de re-chiffrement $rk_{A/p}$ au terme de la période de validité. Il n'est alors plus possible pour Bob d'obtenir la donnée re-chiffrée à son attention. Dans un autre exemple de réalisation, le serveur de stockage S ne procède pas au re-chiffrement lors de la réception de la requête de Bob dès lors que la période de validité a expiré. Dans un exemple de réalisation où les droits associés définissent un nombre d'utilisation de la clé de re-chiffrement, le serveur comptabilise le nombre d'accès par Bob à la donnée re-chiffrée qui n'est plus accessible par Bob dès lors que le nombre d'utilisation de la clé a été atteint.

Dans un exemple de réalisation où le mot de passe choisi par Alice au cours de l'étape E2 est très court, de l'ordre de quelques caractères, il est possible, avant le calcul de la deuxième clé privée $Kpriv_P$ de diversifier ce mot de passe en appliquant un algorithme de diversification au mot de passe et à, par exemple, l'identité de Bob ou d'Alice, ou une date, etc. Cela permet à Alice de garder un même mot de passe pour un partage sécurisé avec différentes personnes, ou à différents moments.

La clé de re-chiffrement $rk_{A/p}$ calculée par le serveur S est une clé que l'on peut qualifier d'éphémère dans le sens où elle n'est destinée qu'à une utilisation ponctuelle. En effet, hormis la période de validité qui peut lui être associée, elle est également explicitement associée par Alice à une donnée F et à Bob, et n'est valable que pour le mot de passe qu'Alice a transmis à Bob. Il n'est par ailleurs pas souhaitable que Bob utilise à son tour cette clé pour stocker des données de manière sécurisée. En effet, de telles données seraient alors accessibles par Alice, indépendamment de droits que Bob associerait à ces données, puisqu'Alice connaît également le mot de passe pwd_A.

Dans un exemple de réalisation, décrit en relation avec la figure 2, on suppose que Bob, après avoir obtenu d'Alice l'accès à quelques données sensibles, conformément aux étapes du procédé de conversion d'un chiffré décrit en relation avec la figure 1, souhaite s'inscrire au service offert par le serveur de stockage S de façon définitive. En d'autres termes, Bob souhaite suivre la procédure standard de génération de clés afin de détenir des données cryptographiques qui lui permettent de partager avec Alice des données sensibles de façon classique, c'est-à-dire au moyen d'une clé de re-chiffrement pérenne qui permet de re-chiffrer directement des données chiffrées pour Alice à l'attention de Bob, indépendamment de l'utilisation d'un mot de passe associé à un contenu. On suppose qu'Alice et Bob ont mis en œuvre au moins une fois les étapes du procédé de conversion décrit précédemment et que Bob connaît au moins un mot de

passe qu'il a utilisé pour dériver la deuxième clé privée $Kpriv_p$ et la deuxième clé publique associée $Kpub_p$.

Dans une étape initiale E20 d'inscription au service, Bob génère son propre couple de clés privée/publique, conformément au schéma cryptographique utilisé par le serveur S. Bob génère ainsi aléatoirement sa propre clé privée $Kpriv_B = x_B$ et calcule au moyen de l'algorithme de génération de clés du schéma de Libert-Vergnaud la clé publique associée KpubB = g^{x_B}. Il conserve sa clé privée $Kpriv_B$ et envoie au serveur de stockage S, dans une étape E21 d'envoi, sa clé publique $Kpriv_B$ ainsi que son identifiant, dans le cas où celui-ci est différent de la clé publique. La clé publique de Bob et le cas échéant son identifiant sont reçus par le serveur S dans une étape E22 de réception.

Dans une étape suivante E23 de demande d'une clé de re-chiffrement existante E22, Bob envoie au serveur de stockage S une requête d'obtention de la clé de re-chiffrement $rk_{A/p}$ préalablement générée pour des échanges sécurisés entre Bob et Alice. Le serveur S envoie la clé de re-chiffrement $rk_{A/p}$ au cours d'une étape suivante d'envoi E24. A noter que la clé de re-chiffrement $rk_{A/p}$ est une clé publique dont la transmission ne nécessite pas de précaution particulière. La clé de re-chiffrement $rk_{A/p}$ est reçue par Bob, plus précisément par le terminal T_B de Bob, dans une étape E24 de réception

Dans une étape suivante E26 de génération d'une nouvelle clé de re-chiffrement, Bob calcule une nouvelle clé de re-chiffrement $rk_{A/B}$ permettant de transformer un chiffré d'Alice, calculé par Alice au moyen de sa clé publique $Kpub_A$, en un chiffré pour Bob qu'il pourra déchiffrer au moyen de sa nouvelle clé secrète $Kpriv_B$.

Conformément au schéma de Libert-Vergnaud, la clé de re-chiffrement d'un contenu chiffré d'Alice en un contenu chiffré pour Bob est de la forme : $g^{(x_B/x_A)}$. Or, Bob ne connaît pas la clé secrète x_A d'Alice. Il connaît par contre la clé de re-chiffrement $rk_{A/p}$ précédemment reçue du serveur $rk_{A/p} = g^{x_p/x_a}$. Il calcule donc :

$$rk_{A/B} = rk_{A/p}{}^{x_B/x_p} = (g^{x_p/x_A})^{x_B/x_p} = g^{x_B/x_A}$$

Bob obtient ainsi la nouvelle clé de re-chiffrement $rk_{A/B}$ d'Alice vers Bob. On remarque que Bob n'a pas eu à solliciter Alice pour calculer cette nouvelle clé de re-chiffrement.

Bien sûr, il est laissé la possibilité de procéder de manière classique en demandant à Alice de calculer la nouvelle clé de re-chiffrement au moyen de sa clé privée x_A et de la nouvelle clé publique de Bob, $Kpub_B = g^{x_B}$.

Dans une étape E27 d'envoi, Bob envoie la nouvelle clé de re-chiffrement $rk_{A/B}$ au serveur S pour enregistrement. La nouvelle clé est reçue et enregistrée par le serveur S dans une

étape E28 de réception. Le serveur S peut alors procéder au re-chiffrement de données d'Alice pour Bob, dès lors qu'Alice souhaite partager de manière sécurisée ces données avec Bob.

Avec cette inscription définitive au service, Bob ne perd pour autant pas l'accès aux données préalablement partagées avec Alice qu'il peut déchiffrer au moyen de la nouvelle clé de re-chiffrement.

Les étapes relatives à l'inscription définitive de Bob au service de stockage sécurisé sont décrites ici dans le cadre du schéma de Libert-Vergnaud. L'invention n'est cependant pas limitée à ce schéma. Tout schéma compatible avec un algorithme de transformation de clé qui prend en entrée une première clé de re-chiffrement $rk_{A/C}$ d'une entité A vers une entité C, la clé privée de l'entité C et la clé privée d'une entité B et qui, à partir de ces données propose de calculer une deuxième clé de re-chiffrement $rk_{A/B}$ de l'entité A vers l'entité B peut être utilisé. En effet, la clé de re-chiffrement $rk_{A/B}$ ainsi obtenue est une clé de re-chiffrement valide. Ainsi par exemple, le schéma proposé par Ateniese, FU, Green et Hohenberger dans l'article « Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage », NDSS 2005 peut également être utilisé pour la mise en œuvre du procédé de conversion d'un premier chiffré en un deuxième chiffré tel que décrit précédemment.

Un serveur de stockage sécurisé S, selon un exemple de réalisation, va maintenant être décrit en relation avec la figure 3. Un tel serveur est un équipement informatique qui comprend de manière classique :

- un microprocesseur 30, ou « CPU » (de l'anglais « Central Processing Unit »), destiné à charger des instructions en mémoire, à les exécuter, à effectuer des opérations,
- une ensemble de mémoires, dont une mémoire volatile 31, ou « RAM » (pour « Random Access Memory ») utilisée pour exécuter des instructions de code, stocker des variables, etc.,
- une mémoire de stockage 32 de type mémoire flash ou « EEPROM » (de l'anglais « Read-Only Memory » et « Electronically-Erasable Programmable Read-Only Memory). La mémoire de stockage 32 est agencée pour mémoriser des instructions de code destinées à mettre en œuvre les étapes du procédé de conversion tel que décrit précédemment. La mémoire de stockage 32 est également agencée pour mémoriser les primitives du schéma cryptographique à clé publique utilisé. Dans un exemple de réalisation, elle mémorise les primitives du schéma de Libert-Vergnaud ;
- des interfaces de communication 33, agencées pour communiquer avec les terminaux T_A et T_B d'Alice et de Bob.

Dans un cas où le serveur S est un environnement en cloud computing, c'est-à-dire une machine virtuelle hébergée par un serveur hôte (non représenté sur la figure 3), on comprend que le microprocesseur 30, les mémoires 31, 32, les interfaces de communication 33 sont des ressources virtualisées mises à disposition de la machine virtuelle par un hyperviseur à partir de ressources matérielles d'une couche d'exécution matérielle du serveur hôte.

Le serveur S comprend également :

- des premiers moyens de réception 34, agencés pour recevoir d'un premier dispositif utilisateur un premier chiffré $Enc_A(F)$, ledit premier chiffré étant obtenu par chiffrement d'une donnée au moyen d'une clé publique $Kpub_A$ de l'utilisateur du premier dispositif. Les premiers moyens de réception 34 sont agencés pour mettre en œuvre l'étape E1 du procédé de conversion décrit précédemment ;

- des deuxièmes moyens de réception 35, agencés pour recevoir en provenance du premier dispositif une clé de re-chiffrement $rk_{A/p}$, ladite clé de re-chiffrement étant calculée en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée $Kpriv_A$ associée à la clé publique de l'utilisateur et à une deuxième clé publique $Kpub_p$ associée à une deuxième clé privée $Kpriv_p$, ladite deuxième clé privée étant dérivée d'un mot de passe pwd_A choisi par l'utilisateur du premier dispositif. Les deuxièmes moyens de réception 35 sont agencés pour mettre en œuvre l'étape E6 du procédé de conversion décrit précédemment ;

- des moyens de conversion 36, agencés pour convertir le premier chiffré $Enc_A(F)$ en un deuxième chiffré $Enc_p(F)$ par application d'un algorithme de re-chiffrement au premier chiffré et à la clé de re-chiffrement, ledit deuxième chiffré étant agencé pour être déchiffré par un deuxième dispositif utilisateur au moyen de la deuxième clé publique, ledit deuxième dispositif recevant le mot de passe du premier dispositif sur un canal de communication indépendant du serveur sécurisé, dérivant la deuxième clé privée dudit mot de passe et obtenant du serveur la deuxième clé publique associée. Les moyens de conversion 36 sont agencés pour mettre en œuvre l'étape E14 de conversion du procédé de conversion décrit précédemment ;

Les interfaces de communication 33, les premiers moyens de réception 34, les deuxièmes moyens de réception 35, les moyens de conversion 36 sont de préférence des modules logiciels comprenant des instructions logicielles pour faire exécuter les étapes du procédé de conversion d'un premier chiffré en un deuxième chiffré tel que décrit précédemment.

L'invention concerne donc aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé de conversion d'un premier chiffré en un deuxième chiffré tel que décrit précédemment lorsque ce programme est exécuté par un processeur du serveur sécurisé S,

- un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur décrit ci-dessus.

Les modules logiciels peuvent être stockés dans, ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un CD-ROM, une disquette magnétique ou un disque dur, ou bien un support de transmission tel qu'un signal ou un réseau de télécommunication.

Un terminal de stockage sécurisé T_A, selon un exemple de réalisation de l'invention, va maintenant être décrit en relation avec la figure 4.

Le terminal de stockage sécurisé T_A est destiné à commander le stockage sécurisé d'une donnée sur un serveur à l'attention d'un autre terminal. Le terminal de stockage T_A est un équipement informatique tel qu'un PC ou un terminal mobile intelligent qui comprend :

- une unité de traitement 40, ou CPU,

- un ensemble de mémoires, dont une mémoire volatile 41, ou RAM et une mémoire de stockage 42 de type mémoire flash ou EEPROM. La mémoire volatile 41 est agencée pour exécuter des instructions de code, stocker des variables, etc. La mémoire de stockage 42 est agencée pour mémoriser des données. En particulier, la mémoire de stockage 42 mémorise une application de stockage sécurisé qui comprend des instructions de code pour mettre en œuvre celles des étapes du procédé de stockage sécurisé sur un serveur tel que décrit précédemment. La mémoire de stockage 42 est également agencée pour stocker un couple de clés privée/publique $Kpriv_A/Kpub_A$ obtenu du serveur sécurisé lors d'une phase d'inscription à un service de stockage sécurisé sur le serveur S ;

- des interfaces de communication 43, agencées pour communiquer avec le serveur de stockage S et l'autre terminal TB.

Le terminal de stockage sécurisé T_A comprend également :

- des moyens de génération 44, agencés pour générer une deuxième clé privée $Kpriv_p$, ladite deuxième clé privée étant dérivée d'un mot de passe pwd_A choisi par l'utilisateur du terminal de stockage T_A, et pour obtenir la deuxième clé publique associée $Kpub_p$. Les moyens de génération 44 sont agencés pour mettre en œuvre l'étape E3 du procédé de conversion de chiffré tel que décrit précédemment ;

- des premiers moyens d'envoi 45, agencés pour envoyer ledit mot de passe à un utilisateur de l'autre terminal sur un canal de communication indépendant du serveur sécurisé. Les premiers moyens d'envoi 45 sont agencés pour mettre en œuvre l'étape E7 du procédé de conversion de chiffré tel que décrit précédemment ;

- des moyens de calcul 46, agencés pour calculer une clé de re-chiffrement $rk_{A/p}$ en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée $Kpriv_A$ associée à la clé publique de l'utilisateur et à la deuxième clé publique associée $Kpub_p$. Les moyens de calcule 46 sont agencés pour mettre en œuvre l'étape E4 du procédé de conversion de chiffré tel que décrit précédemment ;

- des deuxièmes moyens d'envoi 47, agencés pour envoyer de ladite clé de re-chiffrement au serveur sécurisé. Les deuxièmes moyens d'envoi 47 sont agencés pour mettre en œuvre l'étape E5 du procédé de conversion de chiffré tel que décrit précédemment.

Dans un exemple de réalisation dans lequel le premier chiffré $Enc_A(F)$ est envoyé par Alice, le terminal TA comprend également :

- des troisièmes moyens d'envoi (non représentés sur la figure), agencés pour envoyer au serveur sécurisé un premier chiffré $Enc_A(F)$, ledit premier chiffré étant obtenu par chiffrement de la donnée au moyen de la clé publique $Kpub_A$ de l'utilisateur du terminal de stockage T_A. Les deuxièmes moyens d'envoi sont agencés pour mettre en œuvre l'étape E0 du procédé de conversion de chiffré tel que décrit précédemment.

Les interfaces de communication 43, les premiers moyens d'envoi 45, les moyens de génération 44, les deuxièmes moyens d'envoi 47 et les moyens de calcul 46 sont de préférence des modules logiciels comprenant des instructions logicielles pour faire exécuter les étapes du procédé de conversion d'un premier chiffré en un deuxième chiffré tel que décrit précédemment.

L'invention concerne donc aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé de conversion d'un premier chiffré en un deuxième chiffré tel que décrit précédemment lorsque ce programme est exécuté par un processeur du terminal T_A de stockage sécurisé,

- un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur décrit ci-dessus.

Les modules logiciels peuvent être stockés dans, ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un CD-ROM, une disquette magnétique ou un disque dur, ou bien un support de transmission tel qu'un signal ou un réseau de télécommunication.

Un terminal T_B d'obtention d'un contenu, selon un exemple de réalisation, va maintenant être décrit en relation avec la figure 5.

Le terminal T_B d'obtention d'un contenu est destiné à obtenir d'un serveur de stockage sécurisé S une première donnée chiffrée préalablement générée par un premier terminal T_A et

convertie en un deuxième chiffré pour le terminal d'obtention, ladite première donnée chiffrée étant stockée sur le serveur sécurisé à l'attention du terminal T_B d'obtention d'un contenu. Le terminal T_B d'obtention d'un contenu est un équipement informatique tel qu'un PC ou un terminal mobile intelligent qui comprend :

- une unité de traitement 50, ou CPU ;
- un ensemble de mémoires, dont une mémoire volatile 51, ou RAM et une mémoire de stockage 52 de type mémoire flash ou EEPROM. La mémoire volatile 51 est agencée pour exécuter des instructions de code, stocker des variables, etc. La mémoire de stockage 52 est agencée pour mémoriser des données. En particulier, la mémoire de stockage 52 mémorise une application d'obtention d'un premier chiffré généré par le premier terminal et converti en un deuxième chiffré à l'attention du terminal d'obtention, qui comprend des instructions de code pour mettre en œuvre celles des étapes du procédé de conversion d'un premier chiffré en un deuxième chiffré tel que décrit précédemment ;
- des interfaces de communication 53, agencées pour communiquer avec le serveur sécurisé S et le premier terminal T_A.

Le terminal T_B d'obtention d'un contenu comprend également :

- des premiers moyens de réception 54, agencés pour recevoir en provenance du premier terminal un mot de passe pwd_A, ledit mot de passe étant reçu sur un canal de communication indépendant du serveur sécurisé. Les premiers moyens de réception 54 sont agencés pour mettre en œuvre l'étape E8 du procédé de conversion décrit précédemment ;
- des moyens 55 de génération et d'obtention, agencés pour générer une clé privée $Kpriv_p$, ladite clé privée étant dérivée du mot de passe pwd_A, et pour obtenir la deuxième clé publique associée $Kpub_p$. Les moyens 55 de génération et d'obtention sont agencés pour mettre en œuvre l'étape E10 du procédé de conversion décrit précédemment ;
- des moyens d'envoi 56, agencés pour envoyer au serveur sécurisé S une requête d'obtention de la donnée chiffrée. Les moyens d'envoi 56 sont agencés pour mettre en œuvre l'étape E11 du procédé de conversion décrit précédemment ;
- des deuxièmes moyens de réception 57, agencés pour recevoir en provenance du serveur S la donnée chiffrée. Les deuxièmes moyens de réception 57 sont agencés pour mettre en œuvre l'étape E16 du procédé de conversion décrit précédemment ;
- des moyens de déchiffrement 58, agencés pour déchiffrer la donnée chiffrée au moyen de la deuxième clé publique associée. Les moyens de déchiffrement 58 sont agencés pour mettre en œuvre l'étape E17 du procédé de conversion tel que décrit précédemment.

Les interfaces de communication 53, les premiers moyens de réception 54, les moyens 55 de génération et d'obtention, les moyens d'envoi 56, les deuxièmes moyens de réception 57,

les moyens de déchiffrement 58 sont de préférence des modules logiciels comprenant des instructions logicielles pour faire exécuter celles des étapes du procédé de conversion d'un premier chiffré en un deuxième chiffré précédemment décrit et qui sont mises en œuvre par le terminal T_B d'obtention d'un contenu.

Dans un exemple de réalisation, comprenant une phase d'inscription définitive au service de stockage sécurisé, le terminal T_B d'obtention d'un contenu comprend également les moyens suivants (non représentés sur la figure 5) :

- des deuxièmes moyens de génération et d'obtention, agencés pour générer une troisième clé privée $Kpriv_B$ et pour obtenir une troisième clé publique associée $Kpub_B$;
- des deuxièmes moyens d'envoi, agencés pour envoyer au serveur sécurisé une requête d'obtention de la clé de re-chiffrement $rk_{A/p}$;
- des moyens d'obtention, agencés pour obtenir ladite clé de re-chiffrement ;
- des moyens de calcul, agencés pour calculer une deuxième clé de re-chiffrement $rk_{A/B}$ destinée à convertir un chiffré obtenu par application de l'algorithme de chiffrement à la clé publique $Kpub_A$ en un deuxième chiffré destiné à être déchiffré au moyen de la troisième clé privée, ladite deuxième clé de re-chiffrement étant calculée à partir de la clé de re-chiffrement, de la deuxième clé privée $Kpriv_p$ et de la troisième clé privée $Kpriv_B$.

Ces moyens sont de préférence des moyens logiciels comprenant des instructions logicielles pour faire exécuter celles des étapes du procédé de conversion d'un premier chiffré en un deuxième chiffré précédemment décrit et qui sont mises en œuvre par le terminal T_B d'obtention d'un contenu lors de la phase d'inscription définitive au service de stockage sécurisé.

L'invention concerne aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé de conversion d'un premier chiffré en un deuxième chiffré tel que décrit précédemment lorsque ce programme est exécuté par un processeur du terminal T_B d'obtention d'un contenu,
- un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur décrit ci-dessus.

Les modules logiciels peuvent être stockés dans, ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un CD-ROM, une disquette magnétique ou un disque dur, ou bien un support de transmission tel qu'un signal ou un réseau de télécommunication.

REVENDICATIONS

1. Procédé de conversion d'un premier chiffré (F) en un deuxième chiffré, le procédé comprenant les étapes suivantes, mises en œuvre par un serveur de stockage sécurisé (S) :

- réception (E1) du premier chiffré ($Enc_A(F)$), ledit premier chiffré étant obtenu par chiffrement d'une donnée au moyen d'une clé publique ($Kpub_A$) de l'utilisateur d'un premier dispositif,

- réception (E6) en provenance du premier dispositif d'une clé de re-chiffrement ($rk_{A/p}$), ladite clé de re-chiffrement étant calculée en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée ($Kpriv_A$) associée à la clé publique de l'utilisateur et à une deuxième clé publique ($Kpub_p$) associée à une deuxième clé privée ($Kpriv_p$), ladite deuxième clé privée étant dérivée d'un mot de passe (pwd_A) choisi par l'utilisateur du premier dispositif,

- conversion (E14) du premier chiffré ($Enc_A(F)$) en un deuxième chiffré ($Enc_p(F)$) par application d'un algorithme de re-chiffrement au premier chiffré et à la clé de re-chiffrement, ledit deuxième chiffré étant agencé pour être déchiffré par un deuxième dispositif utilisateur au moyen de la deuxième clé publique, ledit deuxième dispositif recevant le mot de passe du premier dispositif sur un canal de communication indépendant du serveur sécurisé, dérivant la deuxième clé privée dudit mot de passe et obtenant du serveur la deuxième clé publique associée.

2. Procédé de stockage sécurisé d'une donnée sur un serveur sécurisé, ledit procédé étant mis en œuvre par un premier dispositif utilisateur à l'attention d'un deuxième dispositif utilisateur, l'utilisateur du premier dispositif détenant une clé privée ($Kpriv_A$) et une clé publique associée ($Kpub_A$), ledit procédé comprenant :

- génération (E3) d'une deuxième clé privée ($Kpriv_p$), ladite deuxième clé privée étant dérivée d'un mot de passe (pwd_A) choisi par l'utilisateur du premier dispositif, et obtention de la deuxième clé publique associée ($Kpub_p$),

- envoi (E7) dudit mot de passe à un utilisateur du deuxième dispositif sur un canal de communication indépendant du serveur sécurisé,

- calcul (E4) d'une clé de re-chiffrement ($rk_{A/p}$) en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée ($Kpriv_A$) associée à la clé publique de l'utilisateur et à la deuxième clé publique associée ($Kpub_p$),

- envoi (E5) de ladite clé de re-chiffrement au serveur sécurisé.

3. Procédé d'obtention d'un premier chiffré généré par un premier dispositif (T_A) et converti en un deuxième chiffré ($Enc_B(F)$) pour un deuxième dispositif utilisateur (T_B), ledit premier chiffré étant stocké sur un serveur S, le procédé comprenant les étapes suivantes, mises en œuvre par le deuxième dispositif :

- réception (E8) en provenance du premier dispositif d'un mot de passe (pwd_A), ledit mot de passe étant reçu sur un canal de communication indépendant du serveur sécurisé,
- génération (E10) d'une clé privée ($Kpriv_p$), ladite clé privée étant dérivée du mot de passe (pwd_A), et obtention de la deuxième clé publique associée ($Kpub_p$),
- envoi (E11) au serveur d'une requête d'obtention de la donnée chiffrée,
- réception (E16) en provenance du serveur de la donnée chiffrée,
- déchiffrement (E17) de la donnée chiffrée au moyen de la deuxième clé publique associée.

4. Procédé d'obtention d'un premier chiffré selon la revendication 3 comprenant, dans une phase d'inscription définitive, les étapes suivantes mise en œuvre par le deuxième dispositif :

- génération (E20) d'une troisième clé privée ($Kpriv_B$) et d'une troisième clé publique associée ($Kpriv_B$),
- envoi (E23) au serveur sécurisé d'une requête d'obtention de la clé de re-chiffrement ($rk_{A/p}$),
- obtention (E25) de ladite clé de re-chiffrement,
- calcul (E26) d'une deuxième clé de re-chiffrement ($rk_{A/B}$) destinée à convertir un chiffré obtenu par application de l'algorithme de chiffrement à la clé publique ($Kpub_A$) en un deuxième chiffré destiné à être déchiffré au moyen de la troisième clé privée, ladite deuxième clé de re-chiffrement étant calculée à partir de la clé de re-chiffrement, de la deuxième clé privée ($Kpriv_p$) et de la troisième clé privée ($Kpriv_B$).

5. Procédé de conversion selon la revendication 1, dans lequel au moins un droit d'accès est associé au premier chiffré par le premier dispositif, un desdits droits définissant une période de validité du premier chiffré au terme de laquelle le serveur efface la clé de re-chiffrement.

6. Serveur de stockage sécurisé (S), destiné à convertir un premier chiffré ($Enc_A(F)$) en un deuxième chiffré, le serveur comprenant :

- des premiers moyens de réception (34), agencés pour recevoir le premier chiffré ($Enc_A(F)$), ledit premier chiffré étant obtenu par chiffrement d'une donnée au moyen d'une clé publique ($Kpub_A$) de l'utilisateur du premier dispositif,

- des deuxièmes moyens de réception (35), agencés pour recevoir en provenance du premier dispositif une clé de re-chiffrement ($rk_{A/p}$), ladite clé de re-chiffrement étant calculée en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée ($Kpriv_A$) associée à la clé publique de l'utilisateur et à une deuxième clé publique ($Kpub_p$) associée à une deuxième clé privée ($Kpriv_p$), ladite deuxième clé privée étant dérivée d'un mot de passe (pwd_A) choisi par l'utilisateur du premier dispositif,

- des moyens de conversion (36), agencés pour convertir le premier chiffré ($Enc_A(F)$) en un deuxième chiffré ($Enc_p(F)$) par application d'un algorithme de re-chiffrement au premier chiffré et à la clé de re-chiffrement, ledit deuxième chiffré étant agencé pour être déchiffré par un deuxième dispositif utilisateur au moyen de la deuxième clé publique, ledit deuxième dispositif recevant le mot de passe du premier dispositif sur un canal de communication indépendant du serveur sécurisé, dérivant la deuxième clé privée dudit mot de passe et obtenant du serveur la deuxième clé publique associée.

7. Terminal (T_A) de stockage sécurisé d'une donnée sur un serveur sécurisé (S), un utilisateur du premier dispositif détenant une clé privée ($Kpriv_A$) et une clé publique associée ($Kpub_A$), ledit terminal de stockage comprenant :

- des moyens (44) de génération et d'obtention, agencés pour générer une deuxième clé privée ($Kpriv_p$), ladite deuxième clé privée étant dérivée d'un mot de passe (pwd_A) choisi par l'utilisateur du terminal de stockage, et pour obtenir la deuxième clé publique associée ($Kpub_p$),

- des premiers moyens d'envoi (45), agencés pour envoyer ledit mot de passe à un utilisateur d'un deuxième dispositif (T_B) sur un canal de communication indépendant du serveur sécurisé,

- des moyens de calcul (46), agencés pour calculer une clé de re-chiffrement ($rk_{A/p}$) en appliquant un algorithme de génération de clés de re-chiffrement à la clé privée ($Kpriv_A$) associée à la clé publique de l'utilisateur et à la deuxième clé publique associée ($Kpub_p$), et

- des deuxièmes moyens d'envoi (47), agencés pour envoyer ladite clé de re-chiffrement au serveur sécurisé.

8. Terminal (T_B) d'obtention d'un contenu, destiné à obtenir un premier chiffré généré par un premier dispositif (T_A) et converti en un deuxième chiffré ($Enc_B(F)$) pour le terminal

d'obtention, ledit premier chiffré étant stocké sur un serveur sécurisé (S), le terminal d'obtention comprenant :

- des premiers moyens de réception (54), agencés pour recevoir en provenance du premier dispositif un mot de passe (pwd_A), ledit mot de passe étant reçu sur un canal de communication indépendant du serveur sécurisé,
- des moyens de génération et d'obtention (55), agencés pour générer une clé privée ($Kpriv_p$), ladite clé privée étant dérivée du mot de passe (pwd_A), et pour obtenir la deuxième clé publique associée ($Kpub_p$),
- des moyens d'envoi (56), agencés pour envoyer au serveur sécurisé une requête d'obtention de la donnée chiffrée,
- des deuxièmes moyens de réception (57), agencés pour recevoir en provenance du serveur la donnée chiffrée,
- des moyens de déchiffrement (58), agencés pour déchiffrer la donnée chiffrée au moyen de la deuxième clé publique associée.

9. Système de stockage sécurisé comprenant :

- un serveur de stockage sécurisé selon la revendication 6,
- au moins un terminal d'envoi d'une donnée selon la revendication 7, et
- au moins un terminal d'accès à une donnée stockée de manière sécurisée selon la revendication 8.

10. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un ordinateur, le programme comprenant des instructions de code pour l'exécution des étapes du procédé de conversion d'un premier chiffré en un deuxième chiffré selon la revendication 1, lorsque le programme est exécuté sur ledit ordinateur.

11. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal utilisateur, le programme comprenant des instructions de code pour l'exécution des étapes du procédé de stockage sécurisé d'une donnée sur un serveur sécurisé, selon la revendication 2, lorsque le programme est exécuté sur ledit terminal.

12. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal utilisateur, le programme comprenant des instructions de code pour l'exécution des étapes du procédé d'obtention d'un premier chiffré selon l'une des revendications 3 à 4, lorsque le programme est exécuté sur ledit terminal.

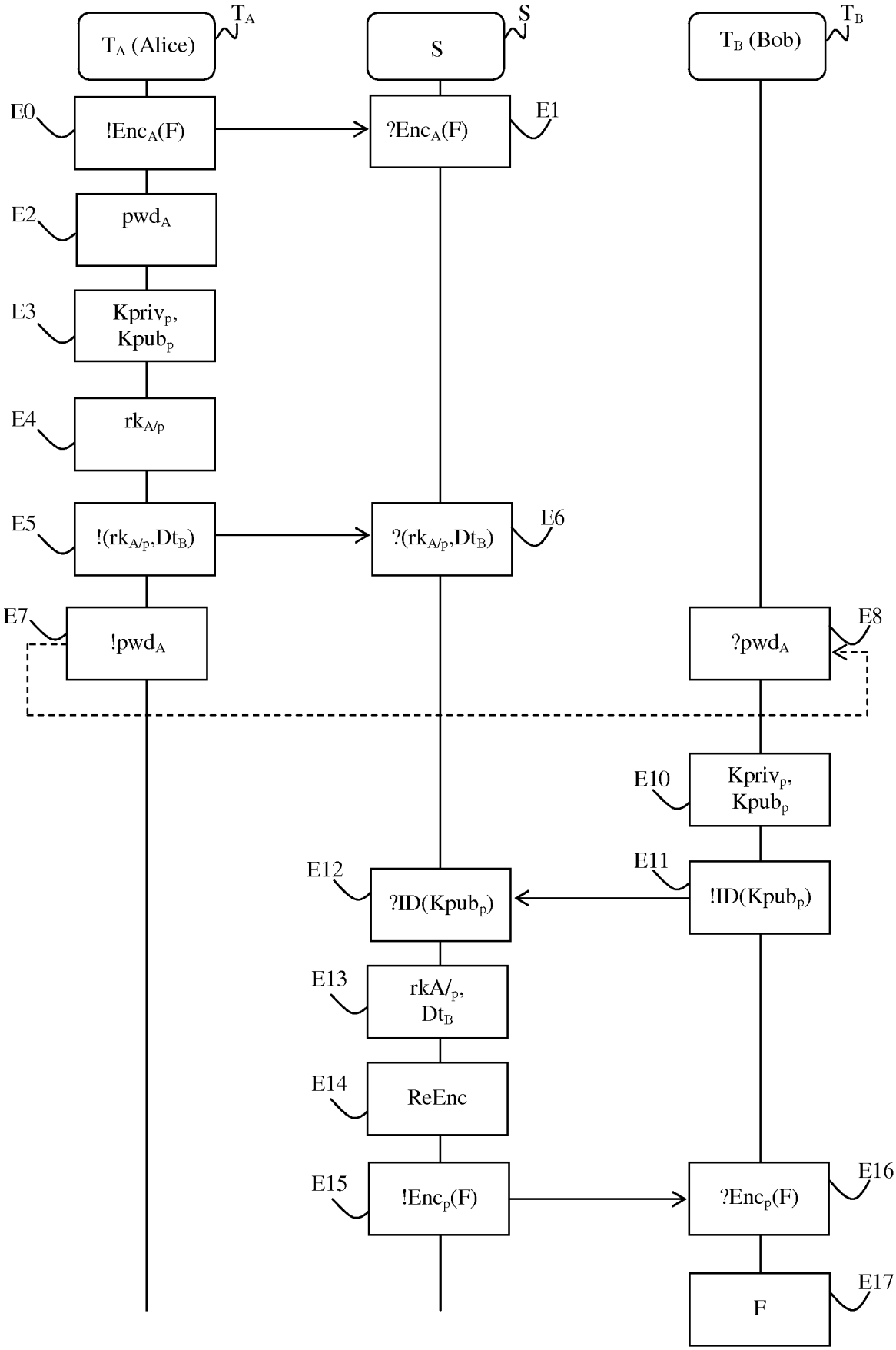

T_A (Alice)
T_A
S
S
T_B (Bob)
T_B
E0
!Enc_A(F)
?Enc_A(F)
E1
E2
pwd_A
E3
Kpriv_p, Kpub_p
E4
rk_A/p
E5
!(rk_A/p,Dt_B)
?(rk_A/p,Dt_B)
E6
E7
!pwd_A
?pwd_A
E8
E10
Kpriv_p, Kpub_p
E12
?ID(Kpub_p)
E11
!ID(Kpub_p)
E13
rkA/_p, Dt_B
E14
ReEnc
E15
!Enc_p(F)
?Enc_p(F)
E16
F
E17

Figure 1

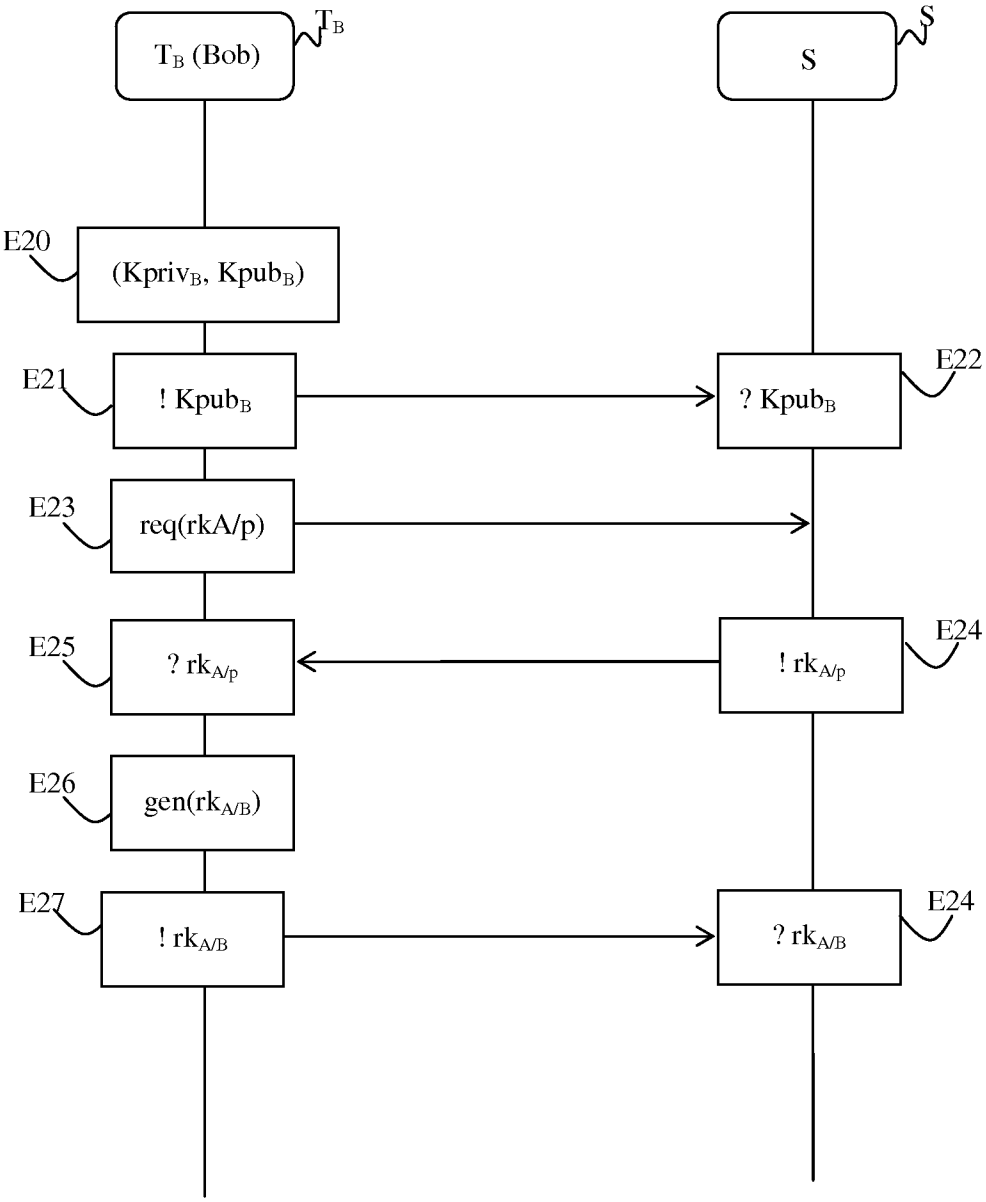

T_B (Bob)
T_B
S
S
E20
($Kpriv_B$, $Kpub_B$)
E21
! $Kpub_B$
? $Kpub_B$
E22
E23
req(rkA/p)
E25
? $rk_{A/p}$
! $rk_{A/p}$
E24
E26
gen($rk_{A/B}$)
E27
! $rk_{A/B}$
? $rk_{A/B}$
E24

Figure 2

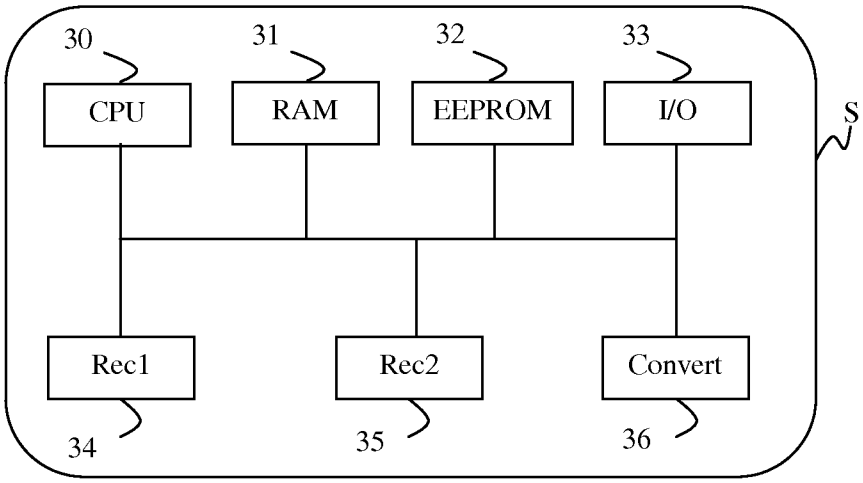


Figure 3

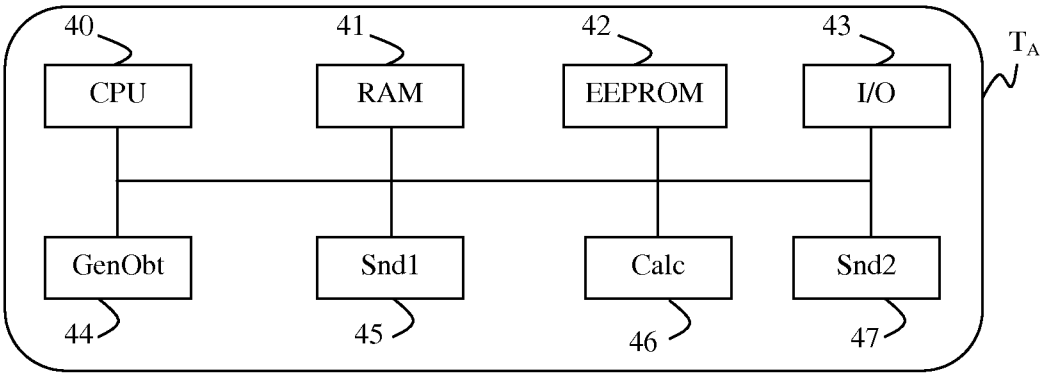


Figure 4

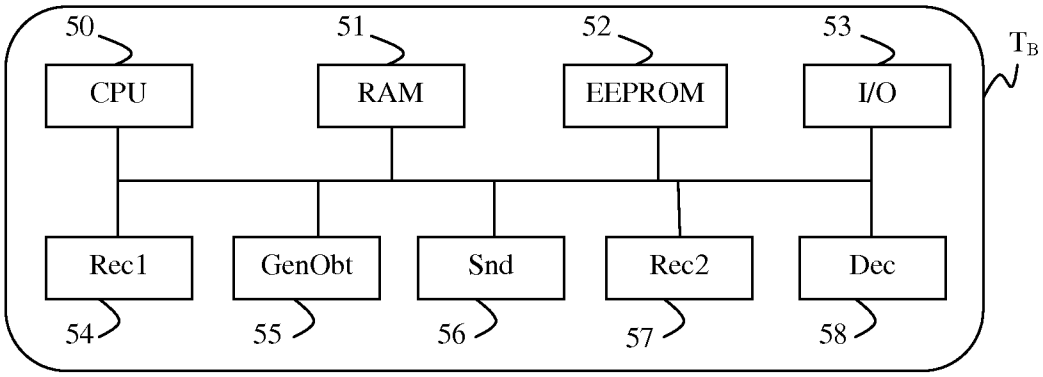


Figure 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/051499

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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 practicable, 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.
X	BENOÎT LIBERT ET AL: "Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption", 9 March 2008 (2008-03-09), PUBLIC KEY CRYPTOGRAPHY - PKC 2008; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 360 - 379, XP047030395, ISBN: 978-3-540-78439-5	1,5,6,10
Y	sections 3 et 4	2,3,7-9, 11,12
A		4

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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 application or patent 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
26 September 2016	10/10/2016

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	Billet, Olivier

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/051499

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GOICHIRO HANAOKA ET AL: "Methodology for designing cryptographic systems with advanced functionality based on a modular approach", SYNTHESIOLOGY, vol. 7, no. 2, 1 September 2014 (2014-09-01), pages 92-104, XP055266053,	1,5,6,10
Y	section 2	2,3,7-9, 11,12
A		4

Y	BILLY LAU ET AL: "Mimesis Aegis: A Mimicry Privacy Shield- A System's Approach to Data Privacy on Public Cloud", 23RD USENIX SECURITY SYMPOSIUM, 1 January 2014 (2014-01-01), pages 33-48, XP055267498, section 4.1	2,3,7-9, 11,12

T	Meltem Sönmez Turan ET AL: "NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Applications National Institute of Standards and Technology", , 1 December 2010 (2010-12-01), XP055267552, Retrieved from the Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.7177&rep=rep1&type=pdf [retrieved on 2016-04-21]	1-12

A	US 2014/140508 A1 (KAMATH DEEPAK [US] ET AL) 22 May 2014 (2014-05-22) the whole document	1-12

A	MARC RENNHARD ET AL: "SecureSafe", PROCEEDINGS OF THE FIRST WORKSHOP ON MEASUREMENT, PRIVACY, AND MOBILITY, MPM '12, 1 January 2012 (2012-01-01), pages 1-6, XP055267495, New York, New York, USA DOI: 10.1145/2181196.2181197 ISBN: 978-1-4503-1163-2 the whole document	1-12

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2016/051499

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014140508 A1	22-05-2014	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2016/051499

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. 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
X	BENOÎT LIBERT ET AL: "Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption", 9 mars 2008 (2008-03-09), PUBLIC KEY CRYPTOGRAPHY - PKC 2008; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 360 - 379, XP047030395, ISBN: 978-3-540-78439-5	1,5,6,10
Y	sections 3 et 4	2,3,7-9, 11,12
A		4

-/--

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

[X] 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
26 septembre 2016	10/10/2016

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	Billet, Olivier

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	GOICHIRO HANAOKA ET AL: "Methodology for designing cryptographic systems with advanced functionality based on a modular approach", SYNTHESIOLOGY, vol. 7, no. 2, 1 septembre 2014 (2014-09-01), pages 92-104, XP055266053,	1,5,6,10
Y	section 2	2,3,7-9, 11,12
A		4

Y	BILLY LAU ET AL: "Mimesis Aegis: A Mimicry Privacy Shield- A System's Approach to Data Privacy on Public Cloud", 23RD USENIX SECURITY SYMPOSIUM, 1 janvier 2014 (2014-01-01), pages 33-48, XP055267498, section 4.1	2,3,7-9, 11,12

T	Meltem Sönmez Turan ET AL: "NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Applications National Institute of Standards and Technology", , 1 décembre 2010 (2010-12-01), XP055267552, Extrait de l'Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.7177&rep=rep1&type=pdf [extrait le 2016-04-21]	1-12

A	US 2014/140508 A1 (KAMATH DEEPAK [US] ET AL) 22 mai 2014 (2014-05-22) le document en entier	1-12

A	MARC RENNHARD ET AL: "SecureSafe", PROCEEDINGS OF THE FIRST WORKSHOP ON MEASUREMENT, PRIVACY, AND MOBILITY, MPM '12, 1 janvier 2012 (2012-01-01), pages 1-6, XP055267495, New York, New York, USA DOI: 10.1145/2181196.2181197 ISBN: 978-1-4503-1163-2 le document en entier	1-12

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2016/051499

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2014140508 A1	22-05-2014	AUCUN	