



(51) Classification internationale des brevets :
H04L 9/20 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2009/050028

(22) Date de dépôt international :
9 janvier 2009 (09.01.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0850168 11 janvier 2008 (11.01.2008) FR

(71) Déposant (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,
F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : SEURIN,
Yannick [FR/FR]; 8, rue du lieutenant Emile Fontaine,
91160 Saulx les Chartreux (FR). GILBERT, Henri [FR/
FR]; 2, allée des Peupliers, F-91440 Bures sur Yvette
(FR).

(74) Mandataire : STEPHANN, Valérie; FRANCE
TELECOM FTR & D/PIV/Brevets, 38-40, rue du Général
Leclerc, F-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, BR, BW, BY, BZ,
CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG,
SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), européen (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, SE, SI, SK, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— relative à la qualité d'inventeur (règle 4.17.iv))

Publiée :

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

[Suite sur la page suivante]

(54) Title : METHOD AND ENTITY FOR PROBABILISTIC SYMMETRICAL ENCRYPTION

(54) Titre : PROCEDE ET ENTITE DE CHIFFREMENT SYMETRIQUE PROBABILISTE

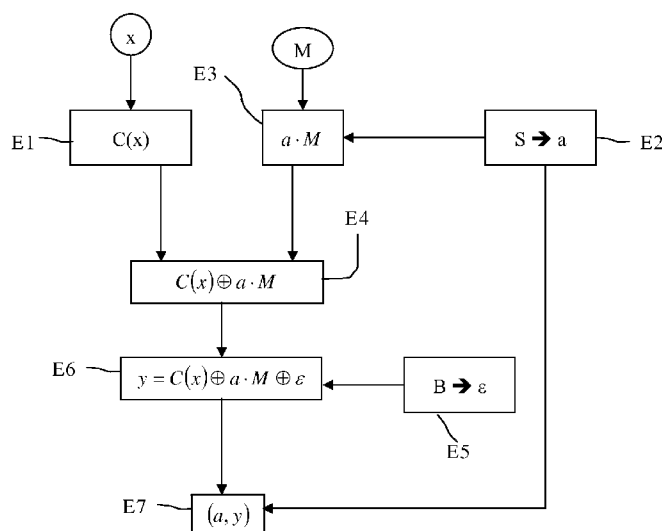


Figure 1

(57) Abstract : The invention relates to a method
for the probabilistic symmetrical encryption of an
element of a plaintext message (x) using a secret
key that can be represented in the form of a
matrix (M). The method includes an encryption
step (E4) of the plaintext message element (x)
using the matrix (M) parameterised by a random
vector (a) in order to obtain an encrypted message
element (y) coupled to the random vector (a). It
further comprises an encoding step (E1) of the
plaintext message element (x) into a code word
(C (x)) using an error correction code having a
given correction capacity (t) and an addition step
(E6) of a noise vector (ε). The error correction
code and the noise vector (ε) are adapted so that
the weight of the Hamming of the noise vector (ε)
is lower than or equal to the correction capacity
(t) of the correction code.

(57) Abrégé : L'invention concerne un procédé
de chiffrement symétrique probabiliste d'un
élément de message en clair (x) à l'aide d'une clé
secrète pouvant être représentée sous la forme
d'une matrice (M). Il comprend une opération de
chiffrement (E4) de l'élément de message en

[Suite sur la page suivante]



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

(88) Date de publication du rapport de recherche internationale :

8 octobre 2009

clair (x), à l'aide de la matrice (M) paramétrée par un vecteur aléatoire (a), afin d'obtenir un élément de message chiffré (y) couplé au vecteur aléatoire (a). En outre, il est prévu une étape d'encodage (E1) de l'élément de message en clair (x) en un mot de code (C (x)) à l'aide d'un code correcteur d'erreurs ayant une capacité de correction donnée (t) et une étape d'ajout (E6) d'un vecteur de bruit (ϵ). Le code correcteur d'erreurs et le vecteur de bruit (ϵ) sont adaptés pour que le poids de Hamming du vecteur de bruit (ϵ) soit inférieur ou égal à la capacité de correction (t) du code correcteur.

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2009/050028

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/00

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JEAN-PHILIPPE AUMASSON ET AL: "TCHo : A Hardware-Oriented Trapdoor Cipher" INFORMATION SECURITY AND PRIVACY; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, vol. 4586, 2 July 2007 (2007-07-02), pages 184-199, XP019065040 ISBN: 978-3-540-73457-4 abstract page 184, line 1 - page 188, line 21	1-11
A	US 2003/223579 A1 (KANTER ERAN [IL] ET AL) 4 December 2003 (2003-12-04) abstract paragraph [0194] - paragraph [0307] figures 1,2,8,9 ----- -/-	1-11

☒ 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

5 août 2009

Date of mailing of the international search report

12/08/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Dujardin, Corinne

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2009/050028

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RAO T R N ET AL: "PRIVATE-KEY ALGEBRAIC-CODE ENCRYPTIONS" IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE, US, vol. 35, no. 4, 1 July 1989 (1989-07-01), pages 829-833, XP000100912 ISSN: 0018-9448 abstract page 829, left-hand column, line 1 - page 831, right-hand column, line 30 -----	1-11
A	BLUM A ET AL: "Cryptographic primitives based on hard learning problems" ADVANCES IN CRYPTOLOGY - CRYPTO '93. 13TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE PROCEEDINGS SPRINGER-VERLAG BERLIN, GERMANY, 1994, pages 278-291, XP008096803 ISBN: 3-540-57766-1 page 278, line 1 - page 279, line 23 page 287, line 13 - page 288, line 17 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2009/050028

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003223579	A1	04-12-2003	NONE

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale n°

PCT/FR2009/050028

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/00

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, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	JEAN-PHILIPPE AUMASSON ET AL: "TCho : A Hardware-Oriented Trapdoor Cipher" INFORMATION SECURITY AND PRIVACY; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS]; SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, vol. 4586, 2 juillet 2007 (2007-07-02), pages 184-199, XP019065040 ISBN: 978-3-540-73457-4 abrégé page 184, ligne 1 - page 188, ligne 21	1-11
A	US 2003/223579 A1 (KANTER ERAN [IL] ET AL) 4 décembre 2003 (2003-12-04) abrégé alinéa [0194] - alinéa [0307] figures 1,2,8,9 ----- -/--	1-11

☒ 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

G document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

5 août 2009

Date d'expédition du présent rapport de recherche internationale

12/08/2009

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

Fonctionnaire autorisé

Dujardin, Corinne

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	RAO T R N ET AL: "PRIVATE-KEY ALGEBRAIC-CODE ENCRYPTIONS" IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE, US, vol. 35, no. 4, 1 juillet 1989 (1989-07-01), pages 829-833, XP000100912 ISSN: 0018-9448 abrégé page 829, colonne de gauche, ligne 1 - page 831, colonne de droite, ligne 30 -----	1-11
A	BLUM A ET AL: "Cryptographic primitives based on hard learning problems" ADVANCES IN CRYPTOLOGY - CRYPTO '93. 13TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE PROCEEDINGS SPRINGER-VERLAG BERLIN, GERMANY, 1994, pages 278-291, XP008096803 ISBN: 3-540-57766-1 page 278, ligne 1 - page 279, ligne 23 page 287, ligne 13 - page 288, ligne 17 -----	

Renseignements relatifs aux membres de familles de brevets

PCT/FR2009/050028

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)