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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
8 octobre 2009 (08.10.2009)

PCT

(10) Numéro de publication internationale
WO 2009/122095 A2

(51) Classification internationale des brevets :
H04L 9/28 (2006.01) *G06F 21/00* (2006.01)
G06F 7/72 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2009/050450

(22) Date de dépôt international :
18 mars 2009 (18.03.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0851884 21 mars 2008 (21.03.2008) 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)* : **BILLET, Olivier** [FR/FR]; 1211, route des Vallettes Sud, F-06140 Tourrettes sur Loup (FR). **FRANCFORT, Stanislas** [FR/FR]; Résidence Bellevue, 19, rue de la Verderie, F-14210 Evrecy (FR). **BENADJILA, Ryad** [FR/FR]; 17, rue Houdart, F-75020 Paris (FR).

(74) Mandataire : **RENARD, Béatrice**; FRANCE TELECOM/R&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), eurasien (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 :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport (règle 48.2.g))*

(54) **Title** : WHITE-BOX PROTECTION FOR CRYPTOGRAPHIC ALGORITHMS INCLUDING CALCULATION OF A QUADRATIC FORM

(54) **Titre** : PROTECTION EN BOITE-BLANCHE D'ALGORITHMES CRYPTOGRAPHIQUES COMPRENANT LE CALCUL D'UNE FORME QUADRATIQUE

$$\sum_{1 \le i \le j \le n} \alpha^{(ij)} x_i x_j \qquad \text{(I)}$$

(57) **Abstract** : The invention relates to a method for implementing a cryptographic algorithm including a calculation step for a quadratic form $Y = A(x,...,x) = (I)$, where the $n > 1$ variables $x,..., x$ as well as the coefficients $\alpha()$ belong to a finite body K of q elements, and where Y is the value taken by the quadratic form $A(x1,...,xn)$ for a given value of variables $x1,...,xn$. Said calculation step is performed by means of the following sub-steps: determining, as a function of the parity of q and n, a canonical quadratic form $Y = C(X1,...,Xn)$ equivalent to said form $A(x,...,x)$, and of the change in linear variable $X = Lx$ associated with this placing in canonical form; calculating the value of transformed variables $X,...,X$ associated with the value of variables $x,...,x$; subdividing all of the terms of said canonical quadratic form $C(X,..., X)$ in sub-assemblies each including one or more of these terms; calculate, for each of said sub-assemblies, the respective total of the terms of the sub-assembly, said calculation being performed, for at least one of the sub-assemblies, by means of a table of values; and summation of said respective sums to obtain said value Y taken by the quadratic form.

(57) **Abrégé** : L'invention concerne un procédé de mise en œuvre d'un algorithme cryptographique comprenant une étape de calcul d'une forme quadratique $Y = A(x,...,x) = (I)$, où les $n > 1$ variables $x,..., x$ ainsi que les coefficients

[Suite sur la page suivante]

WO 2009/122095 A2

α() appartiennent à un corps fini K à *q* éléments, et où Y est la valeur prise par la forme quadratique *A*(x*1,...,xn*) pour une valeur donnée des variables *x1,...,xn*. Ladite étape de calcul est réalisée au moyen des sous-étapes suivantes : détermination, en fonction de la parité de *q* et de *n*, d'une forme quadratique canonique *Y = C(X1,...,Xn)* équivalente à ladite forme *A*(x,...,*x*), et du changement de variable linéaire *X = Lx* associé à cette mise sous forme canonique; calcul de la valeur des variables transformées *X,...,X* associée à ladite valeur des variables *x,...,x* ; subdivision de l'ensemble des termes de ladite forme quadratique canonique *C(X,..., X)* en sous-ensembles comprenant chacun un ou plusieurs de ces termes; calcul, pour chacun desdits sous-ensembles, de la somme respective des termes de ce sous-ensemble, ledit calcul étant effectué, pour au moins un des sous-ensembles, au moyen d'une table de valeurs; et sommation desdites sommes respectives pour obtenir ladite valeur *Y* prise par la forme quadratique.

Protection en boîte-blanche d'algorithmes cryptographiques comprenant le calcul d'une forme quadratique

L'invention se rapporte au domaine de la protection des contenus numériques ainsi que des logiciels contre l'usage non autorisé de ces contenus et logiciels. Plus précisément, l'invention concerne des procédés cryptographiques, par exemple pour le chiffrement, l'authentification ou la signature électronique, qui sont aptes à résister aux attaques dites "attaques en boîte-blanche".

Dans le contexte du déploiement des réseaux de communications et des services audiovisuels, la distribution de contenus numériques devient problématique sur le plan des droits de propriété. En effet, la recopie de données numériques en très grand nombre, ainsi que leur redistribution à grande échelle, est devenue à la fois facile et peu coûteuse pour les particuliers. Par exemple, les industries dont les bénéfices reposent sur la distribution de données numériques (comme la musique, la vidéo, les logiciels de jeux, de navigation sur Internet, ou de manipulation de flux audiovisuels) souhaitent protéger ces données numériques contre une utilisation sortant du cadre défini par un contrat commercial entre fournisseur et consommateur ; c'est l'objet de la gestion des droits numériques (en anglais, "*Digital Rights Management*" ou DRM). Pour une présentation générale des problèmes liés à la protection des logiciels, on pourra consulter l'article de P.C. van Oorschot intitulé "*Revisiting Software Protection*" (Actes de la 6ème Conférence Internationale "*Information Security*", Springer-Verlag, pages 1 à 13, 2003).

Le problème de sécurité auquel se rapporte la présente invention est celui de la protection d'un contenu numérique ou d'un logiciel, non seulement contre des pirates extérieurs à la plateforme, mais également et surtout contre l'utilisateur légitime de la plateforme informatique hébergeant ces données numériques. En effet, cet utilisateur peut être tenté de faire usage de ces données numériques en-dehors du cadre contractuel dans lequel elles lui ont été confiées. Dans ce contexte, les procédés

cryptographiques habituels (chiffrement, signature, clés de session) sont inopérants puisque les clés secrètes requises pour pouvoir utiliser les données numériques sous contrat ont été évidemment fournies à l'utilisateur. L'utilisateur indélicat peut donc, par exemple, chercher à localiser ces clés secrètes en mémoire, ou chercher à identifier les étapes principales mises en œuvre dans le logiciel, pour en faire un usage non autorisé.

Ce contexte de protection d'un contenu numérique est appelé "contexte de protection en boîte-blanche", suite à l'article de S. Chow, P. Eisen, H. Johnson et P.C. van Oorschot intitulé *"White-Box Cryptography and an AES Implementation"* (Actes du 9ème "*Annual Workshop on Selected Areas in Cryptography*", Springer, pages 250 à 270, 2003), et à l'article des mêmes auteurs intitulé "*A White-Box DES Implementation for DRM Applications*" (Actes du "*Second ACM Workshop on Digital Rights Management*", Springer, pages 1 à 15, 2003). Cette dénomination souligne la différence de ce contexte avec celui, bien connu, de la "boîte-noire", dans lequel un pirate cherchant à attaquer un logiciel ne peut observer que des couples (données d'entrée)/(données de sortie) associés à ce logiciel, sans avoir accès aux étapes de traitement intermédiaires mises en œuvre par le logiciel ; dans le contexte d'attaque en boîte-blanche, en revanche, un attaquant peut observer pas à pas l'exécution dynamique d'un logiciel, et même modifier des instructions de ce logiciel pour pouvoir étudier les conséquences de ces modifications sur le traitement effectué par le logiciel.

Notamment, un attaquant en boîte-blanche peut chercher à retrouver les valeurs de clés secrètes enregistrées dans un logiciel (on dit que ce logiciel est une "instanciation" particulière de l'algorithme général qu'il met en œuvre), afin d'utiliser ces clés secrètes dans un logiciel équivalent dont dispose l'attaquant (en effet, l'algorithme mis en œuvre par le logiciel est dans certains cas connu dans ses étapes principales), ou sur une autre plateforme. La protection de ces clés secrètes est donc essentielle, mais rendue d'autant plus difficile que les clés cryptographiques obéissent généralement à un format bien particulier qui les distingue des autres

données enregistrées sur la plateforme informatique, ce qui permet à un attaquant de les y repérer assez facilement.

Prenons par exemple le cas de l'algorithme de chiffrement/déchiffrement bien connu appelé "AES" (initiales des mots anglais "*Advanced Encryption Standard*", Standard FIPS 197 publié par le *National Institute of Standards and Technology* américain). Cet algorithme comprend une succession de "tours" (au nombre de dix) utilisant chacun une clé secrète respective, ces clés de tour étant dérivées d'une clé secrète maîtresse de 128, 192 ou 256 bits. Il s'agit donc de dissimuler la valeur de ces clés de tour. Par ailleurs, l'algorithme AES comprend des étapes (du type : addition de la clé de tour/substitution/permutation circulaire/transformation linéaire) que, pour des raisons d'efficacité de calcul dans les mises en œuvre logicielles, il est préférable de calculer au moyen de tables de valeurs. Notamment, la consultation de tables représentant une transformation linéaire ne requiert pas beaucoup de ressources, même pour un grand nombre de variables, dans la mesure où l'on peut construire une table pour chaque colonne (ou groupe de colonnes) de la matrice de transformation linéaire, puis rassembler les valeurs obtenues. Prenons par exemple le cas où l'on applique une transformation linéaire L, soit $y = Lx$, où x et y sont des multiplets de 128 bits ; dans ce cas, on associe à chaque valeur de i allant de 1 à 128 une table n° i qui contient la série des valeurs du terme $L_{ji}x_i$ pour $x_i = 0$ et j allant de 1 à 128, ainsi que la série des 128 valeurs des composantes du terme $L_{ji}x_i$ pour $x_i = 1$ et j allant de 1 à 128, ce qui requiert une capacité de stockage de $2 \times 128 = 256$ bits par table ; ainsi, à l'exécution, la valeur de la composante y_j de y est obtenue dynamiquement en lisant dans chaque table (resp. n° i) la contribution due à la composante de x correspondante (resp. selon que $x_i = 0$ ou $x_i = 1$), et en ajoutant ces 128 contributions.

Malheureusement, si l'on met en œuvre naïvement l'AES sous forme de tables, les clés de tour peuvent être très facilement calculées à partir des

tables par un attaquant en boîte-blanche, puisque l'opération réalisée par chaque table, correspondant à une étape respective de l'AES, est connue. L'objet de l'article *"White-Box Cryptography and an AES Implementation"* mentionné ci-dessus est précisément de résoudre ce problème. La solution comprend l'utilisation, à la fin de chaque étape de l'AES, d'une "transformation parasite" secrète des données sortantes, suivie d'une "transformation parasite inverse" en entrée de l'étape suivante de l'AES, de façon à ce qu'un attaquant en boîte-blanche ne puisse pas en déduire le flot de données d'origine.

Cette technique s'avère être efficace pour l'AES, et plus généralement, pour tout algorithme de cryptographie faisant appel à des transformations linéaires. Or il a été proposé récemment (cf. par exemple l'algorithme de signature décrit dans l'article de A. Kipnis, J. Patarin, et L. Goubin intitulé "*Unbalanced Oil and Vinegar Signature Schemes*", EUROCRYPT 1999, pages 206 à 222, ou bien l'algorithme de chiffrement à flot décrit dans la demande WO2007/116171 au nom de France Télécom) des procédés cryptographiques faisant appel à des formes *quadratiques* ; autrement dit, un tel procédé utilise un système de m polynômes quadratiques à n variables x_1 à x_n, avec $n>1$, sur un corps fini K, ces polynômes étant donc de la forme

$$y_k = \sum_{1\le i\le j\le n} \alpha_k^{(ij)} x_i x_j + \sum_{1\le j\le n} \beta_k^{(j)} x_j + \gamma_k \qquad (1\le k\le m) \ ,$$

où les coefficients $\alpha_k^{(ij)}$, $\beta_k^{(j)}$ et γ_k appartiennent à K, et où les quantités y_k appartiennent également à K.

Vu l'intérêt croissant manifesté par les hommes du métier pour ces procédés cryptographiques utilisant des formes quadratiques, les auteurs de la présente invention se sont posé la question de savoir s'il était possible de mettre en œuvre de tels procédés en mettant sous forme de table au moins certaines des étapes de calcul, et notamment le calcul de la valeur prise par une forme quadratique pour un multiplet $(x_1,...,x_n)$ donné, mais de manière

à ce que les clés secrètes mises en jeu dans le procédé soient protégées contre des attaques en boîte-blanche.

Or, lorsque l'on tente de mettre en table une forme quadratique, une difficulté apparaît immédiatement : il s'agit de la capacité en mémoire requise pour stocker une telle table. Prenons par exemple à nouveau le cas où $n = 128$ et $K = \mathrm{GF}(2)$, c'est-à-dire le cas où l'on traite des multiplets de 128 bits. Dans ce cas, la table doit contenir 2^{128} entrées possibles, et associer à chacune de ces entrées un multiplet de 128 bits ; par conséquent, la table requiert une capacité de stockage de $2^{128} \times 1$ bits, soit 2^{95} Gigaoctets!

La présente invention concerne donc un procédé de mise en œuvre d'un algorithme cryptographique comprenant une étape de calcul d'une forme quadratique

$$Y = A(x_1,...,x_n) = \sum_{1 \le i \le j \le n} \alpha^{(ij)} x_i x_j ,$$

où les $n > 1$ variables $x_1,...,x_n$ ainsi que les coefficients $\alpha^{(ij)}$ appartiennent à un corps fini K à q éléments, et où Y est la valeur prise par la forme quadratique $A(x_1,...,x_n)$ pour une valeur donnée des variables $x_1,...,x_n$. Ledit procédé est remarquable en ce que ladite étape de calcul est réalisée au moyen des sous-étapes suivantes :

- détermination, en fonction de la parité de q et de n, d'une forme quadratique canonique

$$Y = C(X_1,...,X_n) = \sum_{\substack{0 \le i \le (n-2)/2 \\ \text{ou} \\ 0 \le i \le (n-3)/2}} \gamma_i X_{2i+1} X_{2i+2} + \sum_{1 \le i \le n} \delta_i X_i^2 ,$$

où les variables $X_1,...,X_n$ ainsi que les coefficients γ_i et δ_i appartiennent audit corps K, équivalente à ladite forme $A(x_1,...,x_n)$, et du changement de variable linéaire $X = Lx$ associé à cette mise sous forme canonique,

- calcul de la valeur des variables transformées $X_1,...,X_n$ associée à ladite valeur des variables $x_1,...,x_n$,

- subdivision de l'ensemble des termes de ladite forme quadratique canonique $C(X_1,...,X_n)$ en sous-ensembles comprenant chacun un ou plusieurs de ces termes,

- calcul, pour chacun desdits sous-ensembles, de la somme respective des termes de ce sous-ensemble, ledit calcul étant effectué, pour au moins un des sous-ensembles, au moyen d'une table de valeurs, et

- sommation desdites sommes respectives pour obtenir ladite valeur Y prise par la forme quadratique.

En effet, comme expliqué en détail ci-dessous, on peut montrer que toute forme quadratique à n variables sur un corps fini K peut, au moyen d'un changement de variable linéaire adéquat, être transformée en une somme de termes telle que chaque composante X_i n'apparaisse que dans un seul terme au plus, sauf dans certains cas les composantes X_{n-1} et X_n qui apparaissent alors ensemble dans une somme de trois termes $(X_{n-1}X_n + {X_{n-1}}^2 + \delta {X_n}^2)$, où δ est une constante appartenant à K.

Grâce à cette propriété, on peut avantageusement mettre en table chaque terme de la somme séparément, plus, dans certains cas, la somme des trois termes $(X_{n-1}X_n + {X_{n-1}}^2 + \delta {X_n}^2)$. Par exemple, si $K = \mathrm{GF}(2)$, une table donnant la valeur du terme $\gamma_i X_{2i+1}X_{2i+2}$ ou de la somme de termes $(X_{n-1}X_n + {X_{n-1}}^2 + \delta {X_n}^2)$ ne doit avoir qu'une capacité de stockage en mémoire de 4 bits (correspondant à 2 valeurs possibles pour chacune des deux variables). On peut naturellement aussi mettre en une seule table la somme de deux termes du type $\gamma_i X_{2i+1}X_{2i+2}$, avec une capacité de $4 \times 4 = 16$ bits, ou un nombre plus grand de termes si l'on dispose de capacités de stockage suffisantes. Il ne reste plus ensuite qu'à sommer les valeurs ainsi obtenues pour obtenir la valeur cherchée de la forme

quadratique. Ainsi, en appliquant une transformation canonique aux formes quadratiques, la présente invention permet avantageusement la mise en table de tout procédé cryptographique comprenant au moins une forme quadratique en ne requérant que des capacités de stockage très modestes.

Ce procédé cryptographique mettant en œuvre un calcul selon l'invention pourra alors avantageusement être protégé contre les attaques en boîte-blanche au moyen de "transformations parasites" insérées entre des sous-étapes successives du procédé qui sont calculées au moyen d'une table, conformément à l'enseignement de l'article *"White-Box Cryptography and an AES Implementation"* mentionné ci-dessus.

Selon des caractéristiques particulières, ledit calcul de la valeur des variables transformées $X_1,...,X_n$ est lui aussi réalisé au moyen d'une mise en table. Grâce à ces caractéristiques, ladite mise en œuvre est avantageusement rapide et économique en termes de stockage en mémoire.

Corrélativement, l'invention concerne un dispositif pour mettre en œuvre un algorithme cryptographique comprenant une étape de calcul d'une forme quadratique

$$Y = A(x_1,...,x_n) = \sum_{1 \le i \le j \le n} \alpha^{(ij)} x_i x_j ,$$

où les $n > 1$ variables $x_1,...,x_n$ ainsi que les coefficients $\alpha^{(ij)}$ appartiennent à un corps fini K à q éléments, et où Y est la valeur prise par la forme quadratique $A(x_1,...,x_n)$ pour une valeur donnée des variables $x_1,...,x_n$. Ledit dispositif est remarquable en ce que, pour réaliser ladite étape de calcul, il comprend :

- des moyens pour déterminer, en fonction de la parité de q et de n, une forme quadratique canonique

$$Y = C(X_1,...,X_n) = \sum_{\substack{0 \le i \le (n-2)/2 \\ \text{ou} \\ 0 \le i \le (n-3)/2}} \gamma_i X_{2i+1} X_{2i+2} + \sum_{1 \le i \le n} \delta_i X_i^2 ,$$

où les variables $X_1,...,X_n$ ainsi que les coefficients γ_i et δ_i appartiennent audit corps K, équivalente à ladite forme $A(x_1,...,x_n)$, et le changement de variable linéaire $X = Lx$ associé à cette mise sous forme canonique,

- des moyens pour calculer la valeur des variables transformées $X_1,...,X_n$ associée à ladite valeur des variables $x_1,...,x_n$,

- des moyens pour subdiviser l'ensemble des termes de ladite forme quadratique canonique $C(X_1,...,X_n)$ en sous-ensembles comprenant chacun un ou plusieurs de ces termes,

- des moyens pour calculer, pour chacun desdits sous-ensembles, la somme respective des termes de ce sous-ensemble, ledit calcul étant effectué, pour au moins un des sous-ensembles, au moyen d'une table de valeurs, et

- des moyens pour sommer lesdites sommes respectives pour obtenir ladite valeur Y prise par la forme quadratique.

Les avantages offerts par ce dispositif sont essentiellement les mêmes que ceux offerts par le procédé corrélatif succinctement exposé ci-dessus.

Selon des caractéristiques particulières, ce dispositif comprend également des moyens pour réaliser ledit calcul de la valeur des variables transformées $X_1,...,X_n$ au moyen d'une mise en table. Grâce à ces caractéristiques, ladite mise en œuvre est avantageusement rapide et économique en termes de stockage en mémoire.

Le dispositif selon l'invention pourra notamment prendre la forme d'une plate-forme logicielle, ou d'un circuit électronique.

L'invention vise également un programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur. Ce programme d'ordinateur est remarquable en ce qu'il comprend des

instructions pour l'exécution des étapes de l'un quelconque des procédés succinctement exposés ci-dessus, lorsqu'il est exécuté sur un ordinateur.

Les avantages offerts par ce programme d'ordinateur sont essentiellement les mêmes que ceux offerts par lesdits procédés.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-dessous de modes de réalisation particuliers, donnés à titre d'exemples non limitatifs.

L'invention s'applique à des calculs effectués sur tout corps fini K. Par exemple, il peut s'agir de $GF(2^p)$, c'est-à-dire le corps de Fermi des p-uplets d'éléments binaires ("bits"), où p est un entier strictement positif ; en particulier, lorsque $p = 8$, les éléments du corps peuvent être vus comme des octets ("*bytes*" en anglais) d'éléments binaires ("*bits*" en anglais).

La mise en forme canonique des formes quadratiques sur un corps fini K de cardinal q au moyen d'une transformation linéaire des n variables est présentée par exemple dans les pages 278 à 289 du livre "*Finite Fields*" de R. Lidl et H. Niederreiter (volume 20 de "*Encyclopedia of Mathematics and its Applications*", Cambridge University Press, 2ème éd., 1997). Les divers cas possibles pour la forme canonique équivalente sont les suivants :

- si q est impair, on peut mettre la forme quadratique sous la forme d'une pure somme de carrés des variables transformées X_i,

- si q est pair et n est impair, on peut mettre la forme quadratique sous la forme

$$X_1X_2 + X_3X_4 + ... + X_{n-2}X_{n-1} + X_n{}^2, \text{ et}$$

- si q est pair et n est pair, on peut mettre la forme quadratique soit sous la forme

$$X_1X_2 + X_3X_4 + ... + X_{n-2}X_{n-1} + X_{n-1}X_n,$$

soit sous la forme

$$X_1X_2 + X_3X_4 + ... + X_{n-2}X_{n-1} + X_{n-1}X_n + {X_{n-1}}^2 + \delta {X_n}^2,$$

où δ est une constante appartenant à K.

On va maintenant présenter, uniquement à titre illustratif, un exemple numérique simple de mise en table selon l'invention. On choisit $K = GF(2)$, c'est-à-dire que $q = 2$ et les "nombres" considérés sont des bits.

Supposons donc que, dans le cadre d'un procédé cryptographique quelconque (tel que chiffrement, authentification ou signature), une étape comprenne le calcul de la fonction

$$f(x_1, x_2, x_3, x_4) = x_1x_2 + x_2x_4 + x_3x_4 + x_3 + 1$$

opérant sur $n = 4$ bits x_1, x_2, x_3, x_4. On note que cette fonction comprend :

- une partie quadratique $x_1x_2 + x_2x_4 + x_3x_4$, et

- une partie affine $x_3 + 1$.

Conformément à l'invention, on va appliquer un changement de variable linéaire afin de mettre la partie quadratique sous forme canonique. On notera pour ce faire que $\lambda^2 = \lambda$ pour tout nombre λ (c'est-à-dire $\lambda = 0$ ou $\lambda = 1$) de $GF(2)$. La fonction f ci-dessus peut donc s'écrire :

$$f(x_1, x_2, x_3, x_4) = (x_1 + x_2 + x_3)(x_2 + x_3 + x_4) + x_1(x_3 + x_4) + x_1 + 1.$$

Le changement de variable $X = Lx$ adéquat est donc le suivant :

$$X_1 = x_1 + x_2 + x_3$$

$$X_2 = x_2 + x_3 + x_4$$

$$X_3 = x_3 + x_4$$

$$X_4 = x_1$$

Avec

$$L = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

ce changement de variable pouvant, optionnellement, être mis en œuvre sous la forme de tables.

La forme canonique équivalente à la fonction f est donc la suivante :

$$g(X_1,X_2,X_3,X_4)=X_1X_2+X_3X_4+X_4+1.$$

Procédons à présent à la mise en table de cette fonction $g(X_1,X_2,X_3,X_4)$. On peut écrire :

$$L=\left(C_1|C_2|C_3|C_4\right)$$

$$X = \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix}$$

$$L\times X=C_1\times X_1+C_2\times X_2+C_3\times X_3+C_4$$

Cela permet de mettre en table séparément les quatre opérations $C_i \times X_i$ au moyen de quatre tables de 8 bits (un octet) chacune, correspondant aux deux valeurs possibles pour X_i. On notera que l'on peut en outre, optionnellement, mettre en table la somme des résultats ainsi obtenus.

On pourrait aussi, si on le souhaite, procéder par paire de colonnes de la matrice L, telle que

$$C_1|C_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}$$

ce qui donne des tables de 2 octets chacune, telle que

$$C_1|C_2(Entrée='00') ='0000'$$

$$C_1|C_2(Entrée='01') ='1100'$$

$$C_1|C_2(Entrée='10') ='1001'$$

$$C_1|C_2(Entrée ='11') ='0101'$$

que l'on peut mémoriser simplement sous la forme

$$'0000\ |1100\ |1001\ |0101'$$

On procède alors de manière analogue pour mettre en table les termes de la fonction g. On rappelle que, grâce à l'invention, les termes de la forme quadratique peuvent être mis en table séparément, car la transformation canonique a eu pour effet que chaque variable n'apparaît que dans un seul terme quadratique de la forme obtenue. Par exemple, la mise en table du produit X_1X_2 donne la suite '0|0|0|1', ce qui requiert une capacité de mémoire de 4 bits. De même, la somme $(X_3X_4 + X_4)$ ne requiert que 4 bits de mémoire. Si on le souhaite, on peut même mettre en une seule table la fonction

$$g(X_1, X_2, X_3, X_4) = X_1X_2 + X_3X_4 + X_4 + 1$$

toute entière, en réservant pour ce calcul une capacité en mémoire de 16 bits.

Tout procédé cryptographique mettant en œuvre un calcul selon l'invention pourra alors avantageusement être protégé contre les attaques en

boîte-blanche au moyen de "transformations parasites" insérées entre des sous-étapes successives du procédé qui sont calculées au moyen d'une table, conformément à l'enseignement de l'article *"White-Box Cryptography and an AES Implementation"* mentionné ci-dessus.

Comme indiqué ci-dessus, la présente invention concerne également un système informatique mettant en œuvre le procédé selon l'invention. Ce système informatique comporte de manière classique une unité centrale de traitement commandant par des signaux une mémoire, ainsi qu'une unité d'entrée et une unité de sortie.

De plus, ce système informatique peut être utilisé pour exécuter un programme d'ordinateur comportant des instructions pour la mise en œuvre de l'un quelconque des procédés selon l'invention.

En effet, l'invention vise aussi un programme d'ordinateur téléchargeable depuis un réseau de communication comprenant des instructions pour l'exécution des étapes d'un procédé selon l'invention lorsqu'il est exécuté sur un ordinateur. Ce programme d'ordinateur peut être stocké sur un support lisible par ordinateur et peut être exécutable par un microprocesseur.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette ("*floppy disc*" en anglais) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé

via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

En variante, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé selon l'invention.

La présente invention trouve son application dans le cadre de nombreuses applications mettant en jeu des contenus numériques.

REVENDICATIONS

1. Procédé de protection par un dispositif d'un algorithme cryptographique contre des attaques, l'algorithme étant apte à mettre en œuvre une étape de calcul d'une forme quadratique

$$Y = A(x_1,...,x_n) = \sum_{1 \le i \le j \le n} \alpha^{(ij)} x_i x_j ,$$

où les $n > 1$ variables $x_1,...,x_n$ ainsi que les coefficients $\alpha^{(ij)}$ appartiennent à un corps fini K à q éléments, et où Y est la valeur prise par la forme quadratique $A(x_1,...,x_n)$ pour une valeur donnée des variables $x_1,...,x_n$,

caractérisé en ce que, pour protéger ledit algorithme le dispositif met en œuvre les sous-étapes suivantes :

- détermination, en fonction de la parité de q et de n, d'une forme quadratique canonique

$$Y = C(X_1,...,X_n) = \sum_{\substack{0 \le i \le (n-2)/2 \\ \text{ou} \\ 0 \le i \le (n-3)/2}} \gamma_i X_{2i+1} X_{2i+2} + \sum_{1 \le i \le n} \delta_i X_i^2 ,$$

où les variables $X_1,...,X_n$ ainsi que les coefficients γ_i et δ_i appartiennent audit corps K, équivalente à ladite forme $A(x_1,...,x_n)$, et du changement de variable linéaire $X = Lx$ associé à cette mise sous forme canonique,

- calcul de la valeur des variables transformées $X_1,...,X_n$ associée à ladite valeur des variables $x_1,...,x_n$,

- subdivision de l'ensemble des termes de ladite forme quadratique canonique $C(X_1,...,X_n)$ en sous-ensembles comprenant chacun un ou plusieurs de ces termes,

- calcul, pour chacun desdits sous-ensembles, de la somme respective des termes de ce sous-ensemble, ledit calcul étant effectué, pour au moins un des sous-ensembles, au moyen d'une table de valeurs, et

- sommation desdites sommes respectives pour obtenir ladite valeur Y prise par la forme quadratique.

2. Procédé selon la revendication 1, caractérisé en ce que ledit calcul de la valeur des variables transformées $X_1,...,X_n$ est lui aussi réalisé au moyen d'une mise en table.

3. Procédé selon la revendication 1 ou la revendication 2, caractérisé en ce que l'on insère des transformations parasites entre des sous-étapes successives du procédé qui sont calculées au moyen d'une table,

4. Dispositif pour protéger un algorithme cryptographique contre des attaques, ledit algorithme étant apte à mettre en œuvre une étape de calcul d'une forme quadratique

$$Y = A(x_1,...,x_n) = \sum_{1 \le i \le j \le n} \alpha^{(ij)} x_i x_j ,$$

où les $n > 1$ variables $x_1,...,x_n$ ainsi que les coefficients $\alpha^{(ij)}$ appartiennent à un corps fini K à q éléments, et où Y est la valeur prise par la forme quadratique $A(x_1,...,x_n)$ pour une valeur donnée des variables $x_1,...,x_n$,

caractérisé en ce que, pour réaliser ladite étape de calcul, ledit dispositif comprend :

- des moyens pour déterminer, en fonction de la parité de q et de n, une forme quadratique canonique

$$Y = C(X_1,...,X_n) = \sum_{\substack{0 \le i \le (n-2)/2 \\ \text{ou} \\ 0 \le i \le (n-3)/2}} \gamma_i X_{2i+1} X_{2i+2} + \sum_{1 \le i \le n} \delta_i X_i^2 ,$$

où les variables $X_1,...,X_n$ ainsi que les coefficients γ_i et δ_i appartiennent audit corps K, équivalente à ladite forme $A(x_1,...,x_n)$, et le changement de variable linéaire $X = Lx$ associé à cette mise sous forme canonique,

- des moyens pour calculer la valeur des variables transformées $X_1,...,X_n$ associée à ladite valeur des variables $x_1,...,x_n$,

- des moyens pour subdiviser l'ensemble des termes de ladite forme quadratique canonique $C(X_1,...,X_n)$ en sous-ensembles comprenant chacun un ou plusieurs de ces termes,

- des moyens pour calculer, pour chacun desdits sous-ensembles, la somme respective des termes de ce sous-ensemble, ledit calcul étant effectué, pour au moins un des sous-ensembles, au moyen d'une table de valeurs, et

- des moyens pour sommer lesdites sommes respectives pour obtenir ladite valeur Y prise par la forme quadratique.

5. Dispositif selon la revendication 4, caractérisé en ce qu'il comprend également des moyens pour réaliser ledit calcul de la valeur des variables transformées $X_1,...,X_n$ au moyen d'une mise en table.

6. Circuit électronique, caractérisé en ce qu'il comprend un dispositif selon la revendication 4 ou la revendication 5.

7. Programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions pour l'exécution des étapes du procédé de mise en œuvre d'un algorithme cryptographique selon l'une quelconque des revendications 1 à 3, lorsqu'il est exécuté sur un ordinateur.

8. Support d'informations lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur selon la revendication 7.