(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
5 janvier 2017 (05.01.2017)

WIPO | PCT

(10) Numéro de publication internationale
WO 2017/001809 A1

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

(21) Numéro de la demande internationale : PCT/FR2016/051686

(22) Date de dépôt international : 1 juillet 2016 (01.07.2016)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
15 56225 1 juillet 2015 (01.07.2015) FR

(71) Déposants : **CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE - CNRS** - [FR/FR]; 3, rue Michel Ange, 75016 Paris (FR). **INRIA - INSTITUT NATIONAL DE LA RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE** [FR/FR]; Domaine de Voluceau Rocquencourt, 78153 Le Chesnay (FR). **UNIVERSITE PIERRE ET MARIE CURIE (PARIS 6)** [FR/FR]; 4, Place Jussieu, 75005 Paris (FR).

(72) Inventeurs : **FAUGERE, Jean-charles**; 22 rue de l'Esplanade, 91360 Epinay Sur Orge (FR). **PERRET, Ludovic**; 29 rue Pasteur, 92120 Montrouge (FR).

(74) Mandataire : **CABINET PLASSERAUD**; 66, rue de la Chaussée d'Antin, 75440 Paris Cedex 09 (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, 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).

[Suite sur la page suivante]

(54) Title : OPTIMIZED IMPLEMENTATION OF THE HFE

(54) Titre : MISE EN OEUVRE OPTIMISEE DU HFE

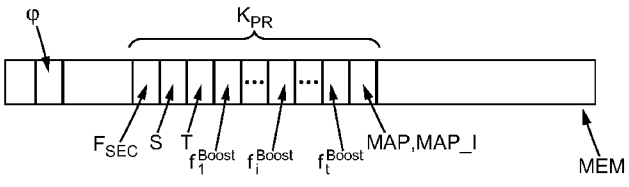


FIG. 3

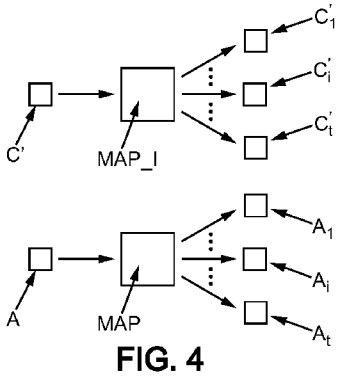


FIG. 4

(57) Abstract : The description relates in particular to methods of accelerated implementation, by an electronic circuit, of a cryptographic algorithm of HFE type. The description also relates to electronic circuits and computer programs able to implement such methods, as well as to storage media comprising such computer programs.

(57) Abrégé : La description concerne notamment des procédés de mise en œuvre accélérée, par un circuit électronique, d'un algorithme cryptographique de type HFE, La description concerne également des circuits électroniques et des programmes d'ordinateur aptes à mettre en œuvre de teis procédés, ainsi que des supports de stockage comprenant de tels programmes d'ordinateur.

WO 2017/001809 A1

Publiée :

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

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

MISE EN ŒUVRE OPTIMISEE DU HFE

La demande concerne notamment une mise en œuvre optimisée de l'algorithme HFE (acronyme de l'expression de langue anglaise Hidden Field Equations).

Pour concevoir des cryptosystèmes, une alternative au recours aux problèmes de la théorie des nombres consiste à s'appuyer sur le problème de résolution d'un système polynomial (désigné par l'acronyme PoSSo). La branche de la cryptographie s'appuyant sur PoSSo est appelée cryptographie multivariée. Le problème PoSSo étant NP-difficile, un cryptosystème multivarié résiste aux attaques quantiques. A l'inverse, on connaît des algorithmes quantiques pour factoriser un entier ou résoudre le problème du logarithme discret en un temps polynomial. Ces algorithmes mettraient à mal la sécurité des algorithmes asymétriques RSA ou encore ElGamal dans un monde où l'informatique quantique serait accessible, tandis qu'un cryptosystème basé sur un problème NP-difficile (tel que PoSSo) resterait pérenne.

L'avènement des ordinateurs quantiques n'est pas encore d'actualité, mais l'usage d'algorithmes tels que le RSA est extrêmement répandu (notamment au sein des cartes à puce). Il est donc judicieux de rechercher des cryptosystèmes s'appuyant sur des problèmes mathématiques difficiles que les ordinateurs quantiques ne pourraient pas aisément résoudre.

Les cryptosystèmes multivariés considérés comme parmi les meilleurs présentent, outre une sécurité que l'on considère accrue, une certaine efficacité en terme notamment de vitesse de chiffrement et de déchiffrement.

Certains cryptosystèmes symétriques (tels que QUAD) ou des fonctions de hachage utilisent le principe de la cryptographie multivariée.

De façon générale, en cryptographie symétrique (non nécessairement multivariée, par exemple en QUAD, DES, 3DES, AES, etc.), chaque utilisateur dispose d'une clé (secrète) qu'il doit partager avec ses correspondants. Toute personne ayant accès à une telle clé secrète peut déchiffrer tout ce qui a été

chiffré avec cette clé, et peut chiffrer ce que bon lui semble avec cette clé comme si elle en était titulaire.

Toutefois, la cryptographie multivariée est principalement utilisée en cryptographie asymétrique. La cryptographie asymétrique s'appuie sur des paires de clés. Ainsi, au lieu de disposer d'une seule clé (secrète), chaque utilisateur dispose d'une paire de clés, dont l'une est publique (elle peut être librement partagée sans mettre en péril la sécurité) et l'autre privée. On parle habituellement de clé privée en cryptographie asymétrique et de clé secrète en cryptographie symétrique, bien que les termes privée/secrète soient utilisés indistinctement par certains auteurs. En cryptographie asymétrique, la distribution des clés se trouve grandement simplifiée. La clé publique peut être échangée aisément. Il suffit par exemple de la faire certifier par une autorité de certification, qui émet un certificat contenant cette clé publique. Le certificat peut ensuite être échangé librement sans sécurité particulière (abstraction faite notamment de la vérification éventuelle de la validité temporelle du certificat et de listes de révocations). Quant à la clé privée, elle est propre à son utilisateur et n'a donc pas de raison d'être partagée. Par exception, les clés privées de chiffrement peuvent être archivées de façon sécurisée. Ceci évite que la perte de la clé privée n'entraîne l'impossibilité de déchiffrer les informations chiffrées avec la clé publique correspondante. L'application consécutive, à un message donné, de la clé privée et de la clé publique, ou inversement de la clé publique puis de la clé privée, est l'identité (on retrouve le message d'origine à l'issue des deux applications). Une paire de clé peut donc offrir plusieurs types d'utilisations. Une personne peut ainsi utiliser la clé publique d'un tiers pour chiffrer un message à son attention. Elle sait que seul ce tiers détient la clé privée correspondante et donc que seul ce tiers peut déchiffrer le message. En pratique, on utilise généralement un algorithme symétrique, plus rapide, pour opérer le chiffrement de données, et on utilise la clé publique pour ne chiffrer que la clé symétrique utilisée (après application d'une opération dite de "padding" de cette clé symétrique visant à la compléter avec des données de façon à obtenir un bloc compatible avec l'opération à clé publique). Cette clé symétrique peut ainsi être générée pour un usage unique

et être facilement partagée avec le tiers. Le problème du partage des clés en cryptographie symétrique est ainsi résolu par la cryptographie asymétrique. A l'inverse, une personne peut utiliser sa clé privée pour signer un message et communiquer le message ainsi signé à des tiers. Habituellement, on applique un algorithme de hachage ("hash") sur le message à signer, et c'est ce hash que l'on signe avec la clé privée (après "padding" approprié). Les tiers peuvent aisément se procurer la clé publique du prétendu signataire, et vérifier que le message a été signé par la bonne personne (seul la personne indiquée dans le certificat contenant la clé publique détient la clé privée correspondante, et personne d'autre qu'elle n'a donc pu signer). Des variantes sont possibles. Il est également possible d'utiliser la cryptographie asymétrique à des fins d'authentification. Par exemple, une personne souhaitant authentifier un tiers peut générer un nombre aléatoire et le lui transmettre. Le tiers est alors censé signer ce nombre aléatoire et renvoyer la signature. De nombreux autres usages de la cryptographie asymétrique sont connus et conventionnels depuis plusieurs décennies.

En cryptographie asymétrique multivariée, la clé publique est déterminée par un système de polynômes en plusieurs variables. Pour pouvoir être inversé, ce système dispose d'une trappe. Le premier cryptosystème utilisant ce concept, appelé C*, a été proposé par T. Matsumoto et H. Imai en 1988. Il a été cassé par J. Patarin en 1995. L'attaque de J. Patarin s'appuie notamment sur la présence, dans C*, d'un unique monôme non linéaire, soit généralement d'un unique coefficient $A_{i,j}$ non nul (les coefficients $A_{i,j}$ sont décrits dans l'équation (1) ci-dessous). J. Patarin a lui-même proposé une amélioration de C* appelée HFE en 1996, dans laquelle un polynôme C*, qui comprend un unique monôme non linéaire, est remplacé par un polynôme (dit polynôme HFE) comprenant au moins deux monômes non linéaires (donc au moins deux des coefficients $A_{i,j}$ d'un polynôme HFE sont non nuls). C'est la mise en œuvre de cet algorithme HFE que l'invention se propose d'améliorer.

L'algorithme HFE, bien connu de l'homme du métier, peut être résumé de la manière suivante.

On note par $M(D)$ le nombre d'opérations nécessaires pour multiplier deux polynômes univariés de degrés strictement inférieurs à D sur un corps $\mathbb{K}$ donné. Il est possible de calculer les racines d'un polynôme F de degré strictement inférieur à D sur ce corps $\mathbb{K}$ en $O(M(D)\log(D))$ opérations dans le corps $\mathbb{K}$. Ceci est expliqué notamment dans Joachim von zur Gathen, Jürgen Gerhard, Modern Computer Algebra (3. ed.), Cambridge University Press 2013, ISBN 978-1-107-03903-2, pages I-XIII, 1-795 dont le contenu est incorporé par référence.

Dans la suite, on note $C(D)=M(D)\log(D)$.

Soit $(q,n,m,D)\in \mathbb{N}^4$ avec q une puissance d'un nombre premier, $m \leq n$, D étant strictement positif et φ un morphisme entre le corps $\mathbb{F}_{q^n}$ et l'espace vectoriel $\mathbb{F}_q^n$. Ainsi, si $(\theta_1,\theta_2,...,\theta_n)\in(\mathbb{F}_{q^n})^n$ est une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, on a:

$$\varphi:\mathbb{F}_{q^n}\rightarrow\mathbb{F}_q^n$$

$$V=\sum_{i=1}^{n}v_i\theta_i\mapsto(v_1,...,v_n)$$

Soit $F\in\mathbb{F}_{q^n}[X]$. On construit une application $\mathfrak{F}^*$ dans l'extension de corps $\mathbb{F}_{q^n}$:

$$\mathfrak{F}^*:\mathbb{F}_{q^n}\rightarrow\mathbb{F}_{q^n}$$
$$V\mapsto F(V)$$

On choisit un polynôme F avec la structure suivante:

$$F=\sum_{\substack{0\leq i\leq j<n\\ q^i+q^j\leq D}}A_{i,j}X^{q^i+q^j}+\sum_{\substack{0\leq i<n\\ q^i\leq D}}B_iX^{q^i}+C \qquad (1)$$

avec $A_{i,j}, B_i, C \in \mathbb{F}_{q^n}, \forall i, j, 0 \leq i \leq j < n$.

Dans l'équation (1), les monômes $A_{i,j}X^{q^i+q^j}$ sont en principe non linéaires (une exception est exposée ci-après). Les autres monômes (monômes $B_iX^{q^i}$) sont linéaires car, le corps $\mathbb{F}_{q^n}$ étant de caractéristique q, pour tout $\{x, y\} \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, B_i(x+y)^{q^i} = B_i x^{q^i} + B_i y^{q^i}$.

La sécurité de HFE provient essentiellement des monômes non linéaires.

Le degré du polynôme F est strictement inférieur à D. D est strictement inférieur à q^n-1.

De plus, au moins deux coefficients parmi les coefficients $A_{i,j}$ (pour tout i,j avec $0 \leq i \leq j < n$) sont non nuls, sinon on est en présence de C* et non de HFE, qui vise précisément à combler une faille de C*. Bien entendu, lorsque q est égal à 2, si l'on veut que la présence de deux coefficients non nuls parmi les coefficients $A_{i,j}$ suffise à garantir que l'on n'est pas en présence d'un polynôme F ne comprenant qu'un seul monôme non linéaire, il faut imposer $i<j$ dans l'équation (1) ci-dessus (au lieu de $i \leq j$). En effet, dans le cas particulier q=2, les monômes de la forme $A_{i,j}X^{q^i+q^j}$ sont des monômes linéaires si i=j, et ne contribuent donc pas à la sécurité de HFE. Dans le cas q=2 et i=j, on a $q^i+q^j=q^i+q^i=2q^i=q^{i+1}$, or le corps étant de caractéristique q, pour tout $\{x, y\} \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, A_{i,i}(x+y)^{q^{i+1}} = A_{i,i}x^{q^{i+1}} + A_{i,i}y^{q^{i+1}}$.

Un polynôme HFE (ou "de structure HFE" ou "de type HFE" ou "HFE shape" en anglais) est défini comme un polynôme univarié selon l'équation (1), respectant les conditions bien connues précitées (il doit comprendre au moins deux monômes non linéaires de la forme $A_{i,j}X^{q^i+q^j}$).

On peut voir l'application $\mathfrak{F} = \varphi \circ \mathfrak{F}^* \circ \varphi^{-1}$ comme l'évaluation d'un système de polynômes quadratiques à coefficients dans $\mathbb{F}_q$:

$$\mathfrak{F} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$
$$(v_1, \ldots, v_n) \mapsto (f_1(v_1, \ldots, v_n), \ldots, f_n(v_1, \ldots, v_n))$$

avec $(f_1, \ldots, f_n) \in (\mathbb{F}_q[x_1, \ldots, x_n])^n$ où les f_i sont construits de telle façon que:

$$F(\varphi^{-1}(x_1, \ldots, x_n)) = \varphi^{-1}(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$$
$$F\left(\sum_{i=1}^{n} \theta_i x_i\right) = \sum_{i=1}^{n} \theta_i f_i(x_1, \ldots, x_n)$$

Considérons par exemple une instance de HFE avec $q=2$, $n=m=4$ et $D=6$. On considère l'extension de corps $\mathbb{F}_{2^4} = \mathbb{F}_2 / \langle \alpha^4 + \alpha + 1 \rangle$. Le vecteur $(1, \alpha, \alpha^2, \alpha^3)$ est une base de l'espace vectoriel $(\mathbb{F}_2)^4$. On choisit un polynôme univarié de degré au plus $D=6$ qui respecte la construction HFE selon l'équation (1), par exemple:

$$F = X^5 + (\alpha^3 + \alpha^2 + 1)X^4 + (\alpha^3 + \alpha^2)X^3 + (\alpha^3 + \alpha + 1)X^2 + (\alpha^2 + \alpha)$$

On peut construire la représentation de F sur $\mathbb{F}_2$ en calculant:

$$F\left(\sum_{i=1}^{n} \alpha^{i-1} x_i\right) = (x_3 x_4^4 + x_3 x_4^2)\alpha^{14} + (x_1^4 + x_2 x_4^4 + x_2 x_4^2 + x_3^2 x_4 + x_4^2)\alpha^{13} +$$
$$(x_1 x_4^2 + x_1 x_4^4 + x_3^3)\alpha^{12} + (x_2^2 x_4 + x_2 x_3^2 + x_3^4 x_4 + x_3^2)\alpha^{11} +$$
$$(x_1 x_3^2 + x_2^2 x_3 + x_3^5 + x_4^4)\alpha^{10} + (x_1^2 x_4 + x_2^3 + x_2^2 + x_2 x_3^4)\alpha^9 +$$
$$(x_1^3 x_3 + x_1 x_2^2 + x_1 x_3^4)\alpha^8 + (x_1^2 x_2 + x_1^2 + x_2^4 x_4)\alpha^7 +$$
$$(x_1^3 + x_2^4 x_3 + x_3^4)\alpha^6 + (x_2^5 + 1)\alpha^5 + (x_1 x_2^4)\alpha^4 +$$
$$(x_1^4 x_4)\alpha^3 + (x_1^4 x_3 + x_2^4)\alpha^2 + (x_1^4 x_2)\alpha + (x_1^5 + x_4^5 + x_4^3)$$

Il suffit alors de réduire les puissances de α par $\alpha^4+\alpha+1$, puis de remplacer x_i^2 par x_i pour tout $i, 1 \le i \le n$. On obtient:

$$F\left(\sum_{i=1}^{n}\alpha^{i-1}x_i\right)=(x_1x_2+x_1+x_2x_3+x_3+x_4)\alpha^3$$
$$+(x_1x_2+x_2x_3+x_2x_4+1)\alpha^2$$
$$+(x_1x_2+x_1x_3+x_1x_4+x_1+x_2x_3+x_2+x_3x_4+x_3+x_4+1)\alpha$$
$$+(x_1x_2+x_1x_3+x_1+x_2x_3+x_2x_4+x_3x_4)$$

Ce qui correspond aux polynômes:

$$f_1(x_1,x_2,x_3,x_4)=x_1x_2+x_1x_3+x_1+x_2x_3+x_2x_4+x_3x_4$$

$$f_2(x_1,x_2,x_3,x_4)=x_1x_2+x_1x_3+x_1x_4+x_1+x_2x_3+x_2+x_3x_4+x_3+x_4+1$$

$$f_3(x_1,x_2,x_3,x_4)=x_1x_2+x_2x_3+x_2x_4+1$$

$$f_4(x_1,x_2,x_3,x_4)=x_1x_2+x_1+x_2x_3+x_3+x_4$$

Une paire de clé HFE peut alors être calculée de la façon suivante.

On définit la clé privée d'une paire de clé HFE comme comprenant un polynôme F de type HFE ainsi que deux transformations affines inversibles, notées S et T. On peut représenter chacune des transformations S et T sous forme d'une matrice n^*n et d'un vecteur de taille n. Ces trois éléments F, S et T sont évidemment conservés de manière confidentielle (ils ne sont pas partagés avec les tiers). Dans la suite, on considère pour simplifier que les transformations S et T sont linéaires (les vecteurs associés sont nuls, et les transformations S et T sont alors représentées simplement par des matrices).

La clé publique correspondante de la paire de clé HFE considérée peut être déterminée de la façon suivante.

On commence par calculer les polynômes $f_1,\ldots,f_n$ correspondant au

polynôme F de la façon indiquée dans l'exemple ci-dessus.

On calcule alors:

$$(g_1(x_1,...,x_n),...,g_n(x_1,...,x_n)) =$$
$$(f_1((x_1,...,x_n)\cdot S),...,f_n((x_1,...,x_n)\cdot S))\cdot T$$

La clé publique HFE est alors $(g_1,\ldots,g_m)$, avec $m \leq n$.

Un chiffrement et un déchiffrement HFE peuvent s'opérer de la manière suivante, avec $m=n$.

Pour chiffrer un message clair $\underline{M} = (M_1,...,M_n) \in \mathbb{F}_q^n$, on calcule le message chiffré:

$$\underline{c} \in \mathbb{F}_q^n = (c_1,...,c_n) = (g_1(M_1,...,M_n),...,g_n(M_1,...,M_n)) .$$

Le possesseur de la clé secrète peut déchiffrer le message chiffré $\underline{c} \in \mathbb{F}_q^n$ en calculant une solution $\underline{z} \in \mathbb{F}_q^n$ du système:

$f_1(\underline{z})-c'_1=0,\ldots,f_n(\underline{z})-c'_n=0$, avec $\underline{c'}=(c'_1,\ldots,c'_n)=\underline{c}\ T^{-1}$.

Dans le cadre du HFE, ceci est équivalent à trouver les $\underline{z} \in \mathbb{F}_q^n$ tels que:

$$F(\varphi^{-1}(\underline{z})) = \varphi^{-1}(\underline{c'}) \qquad (2)$$

On détermine ainsi le message clair $\underline{M} = \underline{z}\ S^{-1}$, pour un $\underline{z}$ solution de l'équation (2).

Une signature HFE peut s'opérer de la manière suivante (avec $m \leq n$). Une signature HFE peut consister à appliquer le procédé de déchiffrement HFE décrit précédemment sur un message auquel on ajoute des valeurs tirées aléatoirement.

Soit Hash $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ une fonction de hachage cryptographique. Pour signer un message $\underline{M} \in \mathbb{F}_q^n$,on calcule $\underline{a}=(a_1,\ldots,a_m)=\mathrm{Hash}(\underline{M})$, où $\underline{a} \in \mathbb{F}_q^m$ est l'empreinte (également appelée hash ou condensat) d'un message $\underline{M}$ à signer. On tire aléatoirement $(n-m)$ valeurs $(r_1,\ldots,r_{n-m})$

dans $\mathbb{F}_q^{n-m}$. On détermine alors $\underline{z} \in \mathbb{F}_q^n$ tel que:

$$F(\varphi^{-1}(\underline{z})) = \varphi^{-1}((\underline{a}, r_1, ..., r_{n-m}) \cdot T^{-1}) \quad (3)$$

Le vecteur $\underline{sig} = \underline{z} \cdot S^{-1} \in \mathbb{F}_q^n$ est une signature du message $\underline{M}$.

Pour un n-uplet $(a_1,\ldots,a_m,r_1,\ldots,r_{n-m})$ donné, il est possible que l'équation (3) n'ait aucune solution. Si c'est le cas, il suffit de répéter l'opération avec d'autres valeurs pour $r_1,\ldots,r_{n-m}$.

Pour vérifier que la signature $\underline{sig}$ est valide pour $\underline{M}$, il suffit de comparer $\underline{a}=\mathrm{Hash}(\underline{M})$ avec le résultat de l'application de la clé publique à la signature $\underline{sig}$. Autrement dit, on teste si $(g_1(\underline{sig}),\ldots,g_m(\underline{sig}))=\underline{a}$. Si cette égalité n'est pas vérifiée, alors $\underline{sig}$ n'est pas une signature valide du message $\underline{M}$.

Dans son article Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms, *Advances in Cryptology* – EUROCRYPT'96, volume 1070 des Lecture Notes in Computer Science, pages 33–48, Springer, 1996, J. Patarin, propose par exemple d'utiliser q=2, n=80 et D=96 pour avoir un chiffré (ou une signature) de 80 bits.

On recense principalement deux attaques contre HFE.

L'attaque directe en recouvrement de message contre HFE (proposée dans: Algebraic cryptanalysis of HFE using Gröbner bases, Jean-Charles Faugère, Reasearch report RR-4738, INRIA, 2003) a une complexité $O(n^{2*dreg-1})$ avec $dreg < \log_2(D)$.Par exemple, $dreg$ est égal à 4 si D est compris entre 17 et 128, $dreg$ est égal à 5 si D est compris entre 129 et 512, et $dreg$ est égal à 6 si D est compris entre 513 et 1280. Les valeurs de $dreg$ en fonction de D sont données dans l'article précité de Jean-Charles

Faugère.

La complexité de l'attaque en recouvrement de clé proposée dans Luk Bettale, Jean-Charles Faugère, and Ludovic Perret, Cryptanalysis of multivariate and odd-characteristic HFE variants, *Public Key Cryptography – PKC 2011*, volume 6571 des Lecture Notes in Computer Science, pages 441–458. Springer, 2011, est $O(n^{2\lfloor \log_2(D) \rfloor + D})$.

Une clé privée utilisée dans l'algorithme HFE conventionnel comprend un polynôme de type HFE (univarié), qui fait la sécurité et l'efficacité du chiffrement. Le degré de ce polynôme est fixé selon un compromis entre la sécurité et l'efficacité, qui sont deux contraintes opposées. Une difficulté qui se pose dans l'algorithme HFE conventionnel est trouver un degré assurant à la fois sécurité et efficacité à la mise en œuvre concrète de l'algorithme.

L'invention vise à améliorer la situation.

Un aspect de l'invention concerne un procédé de mise en œuvre accélérée, par un circuit électronique, d'un algorithme cryptographique HFE exploitant une clé privée HFE basée sur un polynôme de type HFE, sur un morphisme, et sur une première et une deuxième transformations affines, le procédé comprenant:

/E1/ une utilisation, par le circuit électronique, d'au moins un polynôme supplémentaire compris dans la clé privée HFE, et

/E2/ une utilisation, par le circuit électronique, d'une première et d'une deuxième fonctions de mappage comprises dans la clé privée HFE, et associant chacune, à un paramètre d'entrée donné, autant de paramètres de sortie qu'il y a de polynômes supplémentaires dans la clé privée HFE,

l'au moins un polynôme supplémentaire et les fonctions de mappage étant tels que, pour un paramètre donné, et pour toute racine du polynôme de type HFE moins ledit paramètre donné, le résultat de la première fonction de mappage appliquée à ladite racine est une racine de chaque polynôme

supplémentaire moins un paramètre de sortie, correspondant audit chaque polynôme supplémentaire, de la deuxième fonction de mappage appliquée audit paramètre donné.

Le procédé est avantageux notamment en ce qu'il permet une mise en œuvre plus rapide de l'algorithme HFE que la mise en œuvre conventionnelle de cet algorithme. Ceci est particulièrement avantageux lorsqu'il est envisagé d'utiliser l'algorithme HFE sur des dispositifs mobiles tels que des smartphones (parfois appelés "téléphones intelligents" en français) dont la puissance de calcul est limitée par rapport à celle d'un ordinateur de bureau conventionnel. Le procédé est a fortiori avantageux lorsque l'algorithme est mis en œuvre sur un circuit électronique tel qu'une carte à puce, dont la puissance de calcul est très limitée. Le procédé permet une représentation transformée du polynôme de type HFE utilisé dans l'algorithme HFE conventionnel, grâce au(x) polynôme(s) supplémentaire(s) et à la fonction de mappage. Un attaquant éventuel n'a pas d'accès à la structure du polynôme de type HFE (qui nécessite la connaissance de la clé privée), il peut savoir tout au plus qu'il est confronté à un polynôme de haut degré. Mais grâce aux polynômes supplémentaires, le polynôme de type HFE peut être représenté de façon à ce que les opérations à clé privée (déchiffrement ou signature notamment) soient néanmoins exécutées plus rapidement, sans abaisser la sécurité.

Un autre aspect de l'invention concerne un circuit électronique agencé pour mettre en œuvre de façon accélérée un algorithme cryptographique HFE exploitant une clé privée HFE basée sur un polynôme de type HFE, sur un morphisme, et sur une première et une deuxième transformations affines, le circuit électronique comprenant:

un sous circuit électronique d'utilisation d'au moins un polynôme supplémentaire compris dans la clé privée HFE, et

un sous circuit électronique d'utilisation d'une première et d'une deuxième fonctions de mappage comprises dans la clé privée HFE, et associant chacune, à un paramètre d'entrée donné, autant de paramètres de

sortie qu'il y a de polynômes supplémentaires dans la clé privée HFE,

l'au moins un polynôme supplémentaire et les fonctions de mappage étant tels que, pour un paramètre donné, et pour toute racine du polynôme de type HFE moins ledit paramètre donné, le résultat de la première fonction de mappage appliquée à ladite racine est une racine de chaque polynôme supplémentaire moins un paramètre de sortie, correspondant audit chaque polynôme supplémentaire, de la deuxième fonction de mappage appliquée audit paramètre donné.

Un tel circuit électronique est avantageux notamment en ce qu'il permet une mise en œuvre plus rapide de l'algorithme HFE que la mise en œuvre conventionnelle de cet algorithme.

D'autres aspects, buts et avantages de l'invention apparaîtront de manière non limitative à la lecture de la description de quelques uns de ses modes de réalisation.

L'invention sera également mieux comprise à l'aide des dessins, sur lesquels :

- la figure 1 illustre un circuit électronique selon un mode de réalisation de l'invention ;
- la figure 2 illustre l'architecture d'un circuit électronique selon un mode de réalisation de l'invention ;
- la figure 3 illustre la mémoire d'un circuit électronique selon un mode de réalisation de l'invention;
- la figure 4 illustre le fonctionnement d'une fonction de mappage selon un mode de réalisation de l'invention.

La figure 1 montre une circuit électronique selon un mode de réalisation de l'invention, prenant la forme d'une carte à puce SC. Cette carte à puce comprend une puce électronique ICC.

La figure 2 montre l'architecture d'une puce électronique ICC de la carte à puce SC selon la figure 1. La puce ICC comprend notamment un processeur

MP, une mémoire MEM, et un dispositif d'entrées sorties IO. Ces différents composants sont représentés schématiquement sous la forme de composants discrets fixés sur un PCB (non représenté), et reliés entre eux par un bus non représenté. Mais ces différents composants peuvent être (et sont en pratique, dans le cas des cartes à puce) intégrés sur une même puce découpée à partir d'un même wafer et fixée dans un module de carte à puce.

La figure 3 montre le contenu d'une mémoire non volatile MEM d'un circuit électronique selon un mode de réalisation possible de l'invention. On trouve, dans une première partie de la mémoire, une zone de stockage d'un morphisme φ. On trouve, dans une autre partie de la mémoire, une clé privée K_{PR} selon un mode de réalisation de l'invention, comprenant notamment un polynôme F_{SEC}, des transformations affines S et T, des polynômes supplémentaires $f_1^{Boost},\ldots,f_i^{Boost},\ldots,f_t^{Boost}$, et deux fonctions de mappage MAP et MAP_I.

La figure 4 montre une première fonction de mappage MAP, qui à un paramètre d'entrée A associe un paramètre de sortie $(A_1,\ldots,A_i,\ldots,A_t)$, et une deuxième fonction de mappage MAP_I, qui à un paramètre d'entrée C' associe un paramètre de sortie $(C'_1,\ldots,C'_i,\ldots,C'_t)$.

Un premier mode de réalisation se rapporte à un procédé de mise en œuvre accélérée, par un circuit électronique SC, d'un algorithme cryptographique HFE. Le circuit électronique est par exemple une carte à puce SC, mais il peut également s'agir de tout autre circuit électronique approprié, par exemple un circuit électronique dédié, un FPGA, un ASIC, un microcontrôleur, un DSP, ou encore un circuit comprenant un processeur et une mémoire, la mémoire stockant un programme d'ordinateur approprié.

L'algorithme cryptographique HFE selon le premier mode de réalisation est modifié de manière à exploiter une clé privée HFE basée non seulement sur un polynôme F_{SEC} de type HFE, sur un morphisme φ, et sur une première et une deuxième transformations affines S et T, mais en plus sur d'autres éléments. L'exploitation de la clé peut consister à l'utiliser afin d'effectuer des

opérations de déchiffrement, de signature, ou encore d'authentification. L'exploitation peut consister également à manipuler la clé privée (par exemple en effectuant un enregistrement de sauvegarde de cette clé privée au sein d'un serveur sécurisé, au cas où elle serait perdue), cette exploitation pouvant comprendre la génération préalable de ladite clé privée.

Selon une mise en œuvre possible, le polynôme F_{SEC} de type HFE correspond à un polynôme de type HFE conventionnel, noté F dans la description supra.

Par l'expression "clé privée basée sur" on entend que la clé privée peut être construite à partir des éléments énumérés mais qu'elle ne les comprend pas nécessairement. Par exemple, il n'est pas nécessaire de stocker une représentation du morphisme au sein de chaque clé privée, le morphisme pouvant être propre à l'algorithme HFE considéré et étant alors commun à toutes les clés privées générées pour cet algorithme. De même, la clé privée ne contient pas nécessairement le polynôme F_{SEC} de type HFE. En effet, il est possible que la clé privée contienne d'autres éléments permettant de recalculer facilement le polynôme F_{SEC}. Selon une mise en œuvre possible, la clé privée contient les deux transformations affines S et T. Selon une autre mise en œuvre, elle contient de surcroît le polynôme F_{SEC}.

Le procédé selon le premier mode de réalisation comprend une utilisation, par le circuit électronique, d'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s) compris dans la clé privée HFE. Selon une mise en œuvre possible, chacun des polynômes supplémentaires est différent du polynôme F_{SEC}. Par différent, on entend que le polynôme égal à la différence entre le polynôme F_{SEC} et l'un quelconque des polynômes f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaires n'est pas un polynôme nul (c'est-à-dire qu'au moins l'un de ses coefficients est non nul). Selon une mise en œuvre possible, au moins l'un des polynômes f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaires est de degré strictement supérieur à 1. Selon une mise en œuvre possible, la clé privée HFE comprend un seul polynôme supplémentaire. Selon une autre mise en œuvre, la clé privée HFE comprend plusieurs polynômes f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost}

supplémentaires. L'utilisation doit être entendue au sens large. Selon une mise en œuvre possible, l'utilisation d'au moins un polynôme supplémentaire comprend la mise en œuvre d'une opération cryptographique (par exemple une signature électronique, une authentification ou un déchiffrement) avec la clé privée comprenant l'au moins un polynôme supplémentaire, ce qui implique un calcul à l'aide du au moins un polynôme supplémentaire. Selon une autre mise en œuvre possible, l'utilisation comprend le stockage, après génération d'une clé privée selon un mode de réalisation de l'invention, du au moins un polynôme supplémentaire dans une mémoire d'enregistrement de clé privée. Selon une autre mise en œuvre possible, l'utilisation comprend la transmission, après génération d'une clé privée selon un mode de réalisation de l'invention, du au moins un polynôme supplémentaire à un autre circuit électronique.

Le procédé selon le premier mode de réalisation comprend une utilisation, par le circuit électronique, d'une première et d'une deuxième fonctions de mappage (MAP et MAP_I respectivement) comprises dans la clé privée HFE, et associant chacune, à un paramètre d'entrée (noté respectivement A et C') donné, autant de paramètres de sortie (respectivement $A_1,A_2,...,A_t$ et C'_1, C'_2, ... C'_t) qu'il y a de polynômes f_1^{Boost}, f_2^{Boost}, ... f_i^{Boost} supplémentaires dans la clé privée HFE. Comme au paragraphe précédent, l'utilisation doit être entendue au sens large. Selon une mise en œuvre possible, l'utilisation des fonctions de mappage consiste à effectuer une opération cryptographique (par exemple une signature électronique, une authentification ou un déchiffrement) avec la clé privée comprenant lesdites fonctions de mappage, ce qui implique un calcul à l'aide desdites fonctions de mappage. Selon une autre mise en œuvre possible, l'utilisation comprend le stockage, après génération d'une clé privée selon un mode de réalisation de l'invention, desdites fonctions de mappage dans une mémoire d'enregistrement de clé privée. Selon une autre mise en œuvre possible, l'utilisation comprend la transmission, après génération d'une clé privée selon un mode de réalisation de l'invention, desdites fonctions de mappage à un autre circuit électronique.

La première fonction de mappage MAP est une fonction qui transporte les racines entre le polynôme de type HFE et le(s) polynôme(s) supplémentaire(s). La fonction dite fonction inverse de la première fonction de mappage (notée MAP^{-1}) désigne la fonction qui à un élément de l'ensemble d'arrivée de la première fonction de mappage MAP associe la préimage de cet élément dans l'ensemble de départ de la fonction de mappage MAP. Selon le premier mode de réalisation, l'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s) et la première fonction de mappage MAP sont tels que, pour un paramètre C' donné, et pour toute racine A du polynôme F_{SEC} de type HFE moins ledit paramètre C' donné, le résultat $(A_1,A_2,...,A_t)$ de la première fonction de mappage MAP appliquée à ladite racine A est une racine de chaque polynôme f_i^{Boost} supplémentaire moins un paramètre de sortie C'_i, correspondant audit chaque polynôme f_i^{Boost} supplémentaire (au sens par exemple où le paramètre C'_i et ce polynôme f_i^{Boost} ont le même indice, noté i en l'espèce), de la deuxième fonction de mappage MAP_I appliquée audit paramètre C' donné. La deuxième fonction de mappage MAP_I peut être une fonction identité (si son ensemble de départ et son ensemble d'arrivée sont les mêmes). Le fait que les ensembles de départ et d'arrivée soient les mêmes n'implique pas d'utiliser une fonction de mappage identité. De façon plus générale, la deuxième fonction de mappage MAP_I est adaptée pour que la première fonction MAP transporte les racines comme indiqué ci-dessus. Un résultat $(X_1, X_2, ... X_t)=MAP(X)$ (respectivement $(X_1, X_2, ... X_t)=MAP_I(X)$) d'une fonction de mappage se décompose en t paramètres de sortie $X_1, X_2, ... X_t$ qui (réciproquement) forment ensemble ledit résultat $(X_1, X_2, ... X_t)$.

Ainsi, si l'on note $(C'_1, C'_2, ... C'_t)=MAP_I(C')$ et $(A_1, A_2, ... A_t)=MAP(A)$, et si $F_{SEC}(A)=C'$, alors $f_i^{Boost}(A_1,...,A_t)=C'_i$ pour tout i entre 1 et t, t désignant le nombre de polynômes supplémentaires f_i^{Boost}.

Ce procédé de mise en œuvre accélérée d'un algorithme cryptographique HFE peut être intégré de manière conventionnelle dans des architectures de PKI (infrastructures à clés publiques).

Par exemple, il est possible de réaliser une authentification et un chiffrement TLS (Transport Layer Security, le remplaçant du SSL, acronyme

de Secure Socket Layer) grâce à l'algorithme HFE selon l'invention. Il convient cependant de changer la spécification TLS afin d'y autoriser l'emploi de l'algorithme HFE selon l'invention, ou d'utiliser une version propriétaire de TLS permettant un tel support.

De façon analogue, il est possible d'intégrer ce procédé de mise en œuvre accélérée d'un algorithme cryptographique HFE dans la suite de protocoles IPSEC spécifiée par l'IETF. Il convient par exemple d'ajouter aux protocoles pertinents de l'IPSEC (notamment les protocoles ISAKMP et IKE) le support d'un procédé HFE selon l'invention (en plus des algorithmes traditionnels tels que RSA ou Diffie-Hellman).

Ce procédé accéléré peut également être mis en œuvre dans le cadre d'une base de donnée distribuée en un ensemble de nœuds de stockage, la base de données gérant une liste d'enregistrements protégés cryptographiquement (à l'aide de HFE) contre la falsification ou la modification par ses nœuds de stockage. Ce procédé accéléré peut plus particulièrement être mis en œuvre dans le cadre du procédé Blockchain utilisé notamment pour gérer la monnaie cryptographique bitcoin.

Selon un deuxième mode de réalisation, un procédé selon le premier mode de réalisation comprend une génération, par le circuit électronique, de ladite clé privée HFE.

Ladite génération comprend une génération, par le circuit électronique SC, dudit au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_l^{Boost} supplémentaire(s).

Ladite génération comprend une génération, par le circuit électronique SC, desdites fonctions de mappage MAP et MAP_I.

Selon une mise en œuvre possible, les générations des deux paragraphes précédents sont des étapes préalables. Autrement dit, l'utilisation de l'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_l^{Boost} supplémentaire(s) et celle des fonctions de mappage sont postérieurs à leur génération par le circuit électronique, et peuvent comprendre le stockage de l'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_l^{Boost} supplémentaire(s) et celui des fonctions de mappage

dans une mémoire d'enregistrement de clés privées à l'intérieur du circuit électronique. Selon d'autres modes de réalisation, la génération des clés privées n'est pas réalisée par le circuit électronique mais par exemple par un serveur (qui génère alors le au moins un polynôme supplémentaire et les fonctions de mappage pour chaque clé privée générée). Ce serveur transmet chaque clé privée qu'il a générée au circuit électronique pertinent, de manière sécurisée. Selon un mode de réalisation, les clés privées ayant vocation à être utilisées pour des opérations de signature ou d'authentification sont générées par le circuit électronique lui-même, qui peut interdire leur extraction par des mécanismes de sécurité (il n'y a donc pas d'archivage possible, mais en contrepartie une garantie accrue qu'aucun tiers mal intentionné ne peut accéder à ces clés privées). Le défaut d'archivage ne pose pas de problème significatif. En effet, alors que la perte d'une clé privée est concevable (par exemple par perte, destruction ou vol du circuit électronique stockant une telle clé privée), la perte d'une clé publique est beaucoup moins courante, car la clé publique est souvent partagée largement (sous forme de certificat) en plus d'être enregistrée sur un serveur sécurisé (typiquement un serveur d'autorité de certification). La perte d'une telle clé privée empêche donc d'effectuer de nouvelles signatures ou authentifications avec la clé perdue (mais il est très simple de révoquer l'ancienne clé et d'en générer une nouvelle pour assurer à l'avenir les mêmes fonctions de signature et/ou d'authentification). Mais une telle perte n'empêche pas de vérifier les signatures ou authentifications passées (ce qui reste possible grâce à la clé publique, qui est généralement conservée). Selon un mode de réalisation possible, les clés privées ayant vocation à être utilisées pour des opérations de déchiffrement sont générées par un serveur sécurisé, qui en conserve une copie de sauvegarde de manière sécurisée, et les transmet aux circuits électroniques pertinents (à savoir les circuits électroniques qui ont vocation à effectuer des opération de déchiffrement avec ces clés). Ceci permet de pouvoir déchiffrer des messages chiffrés dans le passé alors que la clé privée permettant ce déchiffrement a depuis été perdue (par exemple par perte, destruction ou vol, comme envisagé précédemment pour d'autres types de clés).

Selon un troisième mode de réalisation, un procédé selon le premier ou le second mode de réalisation comprend une opération de déchiffrement.

Cette opération de déchiffrement comprend une réception (à une étape D1), par le circuit électronique SC, d'un message sous forme chiffrée c (qui peut être tronqué) et d'un hash h calculé sur le message sous forme non chiffrée. Le hash h est susceptible de présenter plusieurs intérêts. En particulier, le polynôme HFE possède éventuellement plusieurs racines. La fonction de déchiffrement peut donc conduire à plusieurs messages déchiffrés possibles parmi lesquels il convient alors de déterminer lequel est le bon. Le hash h fournit dans un tel contexte une redondance compensant l'ambiguïté du déchiffrement (qui peut conduire à plusieurs messages clairs possibles alors qu'un seul est pertinent). Le hash h permet également d'introduire une redondance pouvant compenser le fait que le message sous forme chiffrée est tronqué.

L'opération de déchiffrement comprend une application, par le circuit électronique SC, de l'inverse de la deuxième transformation affine T au message sous forme chiffrée c afin d'obtenir un message chiffré intermédiaire c'. On a ainsi $c'=c*T^{-1}$, T^{-1} désignant la transformation inverse de la transformation affine T.

L'opération de déchiffrement comprend une application, par le circuit électronique SC, de l'inverse du morphisme φ au message chiffré intermédiaire c'.

L'opération de déchiffrement comprend une obtention d'au moins un (par exemple de t) paramètre(s) de sortie C'_1, C'_2, ... C'_t, par application, par le circuit électronique SC, de la deuxième fonction de mappage MAP_I au résultat de ladite application de l'inverse du morphisme φ.

L'opération de déchiffrement comprend une résolution, par le circuit électronique SC, d'un système d'équation(s) tel que chaque polynôme f_i^{Boost} supplémentaire soit égal au paramètre de sortie C'_i respectif obtenu à l'étape précédente.

L'opération de déchiffrement comprend une application, par le circuit électronique SC, de l'inverse de la première fonction de mappage MAP à une solution du système d'équation(s).

L'opération de déchiffrement comprend une application, par le circuit électronique SC, du morphisme φ au(x) résultat(s) de l'inverse de la fonction de mappage MAP obtenu à l'étape précédente (la préimage peut contenir plusieurs résultats, qui peuvent alors être traités un par un, indépendamment les uns des autres, par application du morphisme à chacun d'eux).

L'opération de déchiffrement comprend une obtention d'une estimation du message sous forme non chiffrée, par application, par le circuit électronique SC, de l'inverse de la première transformation affine S au résultat (ou à chacun des résultats, s'il y en a plusieurs) du morphisme obtenu à l'étape précédente.

L'opération de déchiffrement comprend un calcul, par le circuit électronique SC, d'un hash de l'estimation du message sous forme non chiffrée. Le hash est issu d'une fonction de hachage cryptographique publique (par exemple SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256, etc.) qui a été utilisée lors de l'opération de chiffrement ayant conduit au message chiffré que le circuit électronique tente de déchiffrer.

L'opération de déchiffrement comprend, si le hash de l'estimation du message sous forme non chiffrée est différent du hash h reçu à l'étape D1, l'obtention d'une autre estimation du message sous forme non chiffrée selon les étapes précédentes, jusqu'à ce que les deux hash soient égaux.

Selon un quatrième mode de réalisation, un procédé selon l'un des premier au troisième modes de réalisation comprend une opération de signature.

Cette opération de signature comprend un calcul, par le circuit électronique SC, d'un hash d'un message à signer.

L'opération de signature comprend une génération, par le circuit électronique, d'un nombre aléatoire de taille égale à la taille d'un élément de l'ensemble d'arrivée du morphisme φ moins la taille du hash du message à signer. Par taille, on entend taille au sens informatique du terme. Par exemple, si un élément de l'ensemble d'arrivée du morphisme φ est codé sur 256 bits, et si le hash d'un message est codé sur 224 bits, alors le nombre aléatoire généré est un nombre aléatoire de 32 bits.

L'opération de signature comprend une application, par le circuit électronique, de l'inverse de la deuxième transformation affine T à une concaténation du nombre aléatoire et du hash du message à signer.

L'opération de signature comprend une application, par le circuit électronique, de l'inverse du morphisme φ au résultat de l'application de l'inverse de la deuxième transformation affine T.

L'opération de signature comprend une obtention d'au moins un paramètre de sortie (par exemple une obtention de t paramètres de sortie C'_1, C'_2, ... C'_t), par application, par le circuit électronique, de la deuxième fonction de mappage MAP_I au résultat de ladite application de l'inverse du morphisme.

L'opération de signature comprend une résolution, par le circuit électronique, d'un système d'équation(s) tel que chaque polynôme f_i^{Boost} supplémentaire soit égal au paramètre de sortie C'_i respectif obtenu à l'étape précédente.

L'opération de signature comprend, si le système d'équation(s) n'admet pas de solution, une répétition des étapes précédentes avec un autre nombre aléatoire. Selon une mise en œuvre possible, l'autre nombre aléatoire est un nombre aléatoire généré à nouveau par le circuit électronique. Selon une autre mise en œuvre, l'autre nombre aléatoire résulte de l'incrémentation, par le circuit électronique, du précédent nombre aléatoire.

L'opération de signature comprend une application, par le circuit électronique, de l'inverse de la première fonction de mappage MAP à une solution du système d'équation(s). Si la préimage renvoyée par l'inverse de la

première fonction de mappage comprend plusieurs résultats, le circuit électronique recherche parmi eux un résultat qui convient (le résultat doit aboutir à une racine de $F_{SEC} - \varphi^{-1}$).

L'opération de signature comprend une application, par le circuit électronique, du morphisme φ au résultat de l'inverse de la première fonction de mappage MAP obtenu à l'étape précédente.

L'opération de signature comprend une obtention d'une signature du message à signer, par application, par le circuit électronique, de l'inverse de la première transformation affine S au résultat du morphisme φ obtenu à l'étape précédente.

Selon un cinquième mode de réalisation, la clé privée HFE d'un procédé selon l'une des premier au quatrième modes de réalisation précédents comprend un unique polynôme f^{Boost} supplémentaire, la première fonction de mappage MAP est un monôme, et le polynôme de type HFE F_{SEC} est égal à la composition du polynôme f^{Boost} supplémentaire avec la première fonction de mappage MAP.

Selon un sixième mode de réalisation, un programme d'ordinateur comprend une suite d'instructions mettant en œuvre les étapes du procédé selon l'un des premier au cinquième modes de réalisation lorsqu'elles sont exécutées par un processeur. Ce programme est par exemple rédigé en langage assembleur, ou encore en langage C. De tels langages, de bas niveau, sont avantageux dans la mesure où ils permettent des optimisations fines et autorisent la mise en place de contremesures de façon plus efficace. Des langages de plus haut niveau sont possibles mais dégradent généralement les performances et ne permettent pas nécessairement de mettre en place des contremesures efficaces.

Selon un septième mode de réalisation, un support de stockage non transitoire lisible par ordinateur comprend un programme d'ordinateur selon le sixième mode de réalisation. Ce support de stockage est par exemple une mémoire permettant un stockage permanent. La mémoire peut être réinscriptible (Flash, EEPROM, RAM protégée par batterie, voire support magnétique ou optique) ou non réinscriptible (ROM, etc.). Un tel support de stockage peut être intégré à une carte à puce ou à un ordinateur quelconque, en particulier un smartphone.

Selon un huitième mode de réalisation, un circuit électronique (par exemple une carte à puce SC) est agencé pour mettre en œuvre de façon accélérée un algorithme cryptographique HFE exploitant une clé privée HFE basée sur un polynôme F_{SEC} de type HFE, sur un morphisme, et sur une première S et une deuxième T transformations affines.

Le circuit électronique comprend un sous circuit électronique d'utilisation d'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s) compris dans la clé privée HFE. Selon une mise en œuvre possible, Le sous circuit électronique d'utilisation d'au moins un polynôme est par exemple un circuit électronique dédié, un FPGA, un ASIC, un microcontrôleur, un DSP, ou encore un circuit comprenant un processeur et une mémoire, la mémoire stockant un programme d'ordinateur approprié. Selon une mise en œuvre possible, le sous circuit électronique d'utilisation d'au moins un polynôme partage un processeur avec le circuit électronique.

Le circuit électronique comprend un sous circuit électronique d'utilisation des fonctions de mappage MAP et MAP_I comprises dans la clé privée HFE, et associant, à un paramètre d'entrée donné, autant de paramètre(s) de sortie qu'il y a de polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s) dans la clé privée HFE. Selon une mise en œuvre possible, Le sous circuit électronique d'utilisation des fonctions de mappage est par exemple un circuit électronique dédié, un FPGA, un ASIC, un microcontrôleur, un DSP, ou encore un circuit comprenant un processeur et une mémoire, la mémoire stockant un programme d'ordinateur approprié. Selon une mise en œuvre possible, le sous

circuit électronique d'utilisation des fonctions de mappage partage un processeur avec le circuit électronique.

Par exemple, le circuit électronique comprend un processeur, une mémoire contenant un programme d'ordinateur agencé pour mettre en œuvre l'utilisation de l'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s), et une mémoire contenant un programme d'ordinateur agencé pour mettre en œuvre l'utilisation des fonctions de mappage. Le sous circuit électronique d'utilisation d'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s) peut comprendre le processeur et la mémoire contenant le programme d'ordinateur agencé pour mettre en œuvre l'utilisation de l'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s), et le sous circuit électronique d'utilisation des fonctions de mappage peut comprendre le même processeur (partagé) et la mémoire contenant le programme d'ordinateur agencé pour mettre en œuvre l'utilisation des fonctions de mappage. Selon une autre mise en œuvre possible, le sous circuit électronique d'utilisation d'au moins un polynôme(s) f_1^{Boost}, f_2^{Boost}, ... f_t^{Boost} supplémentaire(s) et le sous circuit électronique d'utilisation des fonctions de mappage sont deux sous circuits entièrement distincts, pouvant néanmoins coopérer l'un avec l'autre.

L'au moins un polynôme supplémentaire et les fonctions de mappage sont tels que, pour un paramètre C' donné, et pour toute racine A du polynôme F_{SEC} de type HFE moins ledit paramètre C' donné, le résultat $(A_1,...,A_l)$ de la première fonction de mappage MAP appliquée à ladite racine A est une racine de chaque polynôme f_i^{Boost} supplémentaire moins un paramètre de sortie C'_i, correspondant audit chaque polynôme f_i^{Boost} supplémentaire, de la deuxième fonction de mappage MAP appliquée audit paramètre C' donné.

Selon un neuvième mode de réalisation, un circuit électronique selon le huitième mode de réalisation comprend, afin de mettre en œuvre une opération de déchiffrement, un sous circuit électronique de réception d'un message sous forme chiffrée c et d'un hash h calculé sur le message sous forme non chiffrée.

Le circuit électronique comprend un sous circuit électronique d'application de l'inverse de la deuxième transformation affine T au message sous forme chiffrée c afin d'obtenir un message chiffré intermédiaire c'.

Le circuit électronique comprend un sous circuit électronique d'application de l'inverse du morphisme au message chiffré intermédiaire c'.

Le circuit électronique comprend un sous circuit électronique d'obtention d'au moins un paramètre de sortie C'_1, C'_2, ... C'_t, par application de la deuxième fonction de mappage MAP_I au résultat de ladite application de l'inverse du morphisme.

Le circuit électronique comprend un sous circuit électronique de résolution d'un système d'équation(s) tel que chaque polynôme f_i^{Boost} supplémentaire soit égal au paramètre de sortie C'_i respectif.

Le circuit électronique comprend un sous circuit électronique d'application de l'inverse de la première fonction de mappage MAP à une solution du système d'équation(s).

Le circuit électronique comprend un sous circuit électronique d'application du morphisme au résultat de l'inverse de la première fonction de mappage MAP.

Le circuit électronique comprend un sous circuit électronique d'obtention d'une estimation du message sous forme non chiffrée, par application de l'inverse de la première transformation affine S au résultat de l'application du morphisme.

Le circuit électronique comprend un sous circuit électronique de calcul d'un hash de l'estimation du message sous forme non chiffrée.

Le circuit électronique comprend un sous circuit électronique de vérification agencé pour vérifier si le hash de l'estimation du message sous forme non chiffrée est différent du hash h reçu, et dans l'affirmative pour déclencher l'obtention d'une autre estimation du message sous forme non chiffrée, jusqu'à ce que les deux hash soient égaux.

Selon un dixième mode de réalisation, la clé privée HFE d'un circuit électronique selon le huitième ou neuvième mode de réalisation comprend un unique polynôme f^{Boost} supplémentaire, la première fonction de mappage MAP est un monôme, et le polynôme F_{SEC} de type HFE est égal à la composition du polynôme f^{Boost} supplémentaire avec la première fonction de mappage MAP.

D'autres modes de réalisation sont décrits plus précisément ci-dessous.

Une manière de générer une paire de clés publique et privée selon un mode de réalisation possible est la suivante. Soit $(q, n, m, t, D) \in \mathbb{N}^5$ avec q une puissance d'un nombre premier et $m \leq n$. Un circuit électronique définit $\mathrm{Aff}_n(\mathbb{F}_q) = \mathrm{GL}_n(\mathbb{F}_q) \times \mathbb{F}_q^n$ comme l'ensemble des transformations affines inversibles de $\mathbb{F}_q^n$.

La clé secrète dans HFEBoost comprend:

1. un polynôme univarié $F_{SEC} \in \mathbb{F}_{q^n}[X]$ de type HFE (équation (1) précitée) de degré D_{SEC}.

2. des polynômes $f_1^{Boost}, \ldots, f_t^{Boost} \in \mathbb{K}[Y_1, \ldots, Y_t]$, avec $\mathbb{K}$ un corps quelconque (par exemple des polynômes $f_1^{Boost}, \ldots, f_t^{Boost} \in \mathbb{F}_{q^n}[Y_1, \ldots, Y_t]$ si l'on prend comme corps $\mathbb{K}$ le corps $\mathbb{F}_{q^n}$).

3. une première fonction de mappage $\mathrm{MAP}: \mathbb{F}_{q^n} \rightarrow \mathbb{K}^t$. La fonction MAP transporte toute racine $Z \in \mathbb{F}_{q^n}$ du polynôme F_{SEC} en une solution dans $\mathbb{K}^t$ du système $f_1^{Boost}=0, \ldots, f_t^{Boost}=0, \ldots, f_t^{Boost}$. Une deuxième fonction de mappage $\mathrm{MAP_I}: \mathbb{F}_{q^n} \rightarrow \mathbb{K}^t$.

4. deux transformations affines

$\left((\mathbf{S},\underline{s}),(\mathbf{T},\underline{t})\right)\in \mathrm{Aff}_n(\mathbb{F}_q)\times \mathrm{Aff}_n(\mathbb{F}_q)$. On adopte ici une notation plus précise (différente des notations utilisées précédemment) afin de faire apparaître expressément dans la notation la partie affine ($\underline{s}$ et $\underline{t}$, respectivement) des transformations, les notations S et T désignant des transformations linéaires. En pratique, utiliser une transformation linéaire en lieu et place d'une transformation affine (en posant $\underline{s}=0$ et $\underline{t}=0$) ne présente pas d'inconvénient (cela ne diminue pas la sécurité de manière notable, et cela simplifie légèrement les calculs).

Soit $\underline{c}'\in \mathbb{F}_q^n=\left(c'_1,...,c'_n\right)$.

Les polynômes $f_1^{\mathrm{Boost}},...,f_t^{\mathrm{Boost}}\in\mathbb{K}\left[Y_1,...,Y_t\right]$ sont tels que:

— si $A\in\mathbb{F}_{q^n}$ est une racine de $F_{\mathrm{SEC}}-\varphi^{-1}\left(\underline{c}'\right)$, alors $\mathrm{MAP}(A)$ est une solution de $f_1^{\mathrm{Boost}}(\mathrm{MAP}(A))=C'_1,...,f_t^{\mathrm{Boost}}(\mathrm{MAP}(A))=C'_t$,

avec $(C'_1,...,C'_t)=\mathrm{MAP_I}\left(\varphi^{-1}\left(\underline{c}'\right)\right)$,

— il est possible de calculer les solutions de $f_1^{\mathrm{Boost}}(\mathrm{MAP}(A))=C'_1,...,f_t^{\mathrm{Boost}}(\mathrm{MAP}(A))=C'_t$ en un temps inférieur à $O\left(C\left(D_{\mathrm{SEC}}\right)\right)$. On entend par là que l'on trouve les racines de l'ensemble des polynômes f_i^{Boost} plus vite que les racines du polynôme F_{SEC}, ce qui permet d'accélérer le traitement par rapport au HFE conventionnel.

Un circuit électronique construit les polynômes $f_1,...,f_n\in\left(\mathbb{F}_q\left[x_1,...,x_n\right]\right)^n$ tels que:

$$F_{\mathrm{SEC}}\left(\varphi^{-1}\left(x_1,...,x_n\right)\right)=\varphi^{-1}\left(f_1\left(x_1,...,x_n\right),...,f_n\left(x_1,...,x_n\right)\right)$$

et

$$F_{SEC}\left(\sum_{i=1}^{n}\theta_i x_i\right)=\sum_{i=1}^{n}\theta_i f_i\left(x_1,...,x_n\right).$$

Le circuit électronique construit également la clé publique en masquant les composantes $f_1,...,f_n$ de F_{SEC}.

Plus précisément, pour construire une clé publique, le circuit électronique calcule, selon un mode de réalisation:

$$\left(g_1\left(x_1,...,x_n\right),...,g_n\left(x_1,...,x_n\right)\right)=\left(f_1\left(\ell_1,...,\ell_n\right),...f_n\left(\ell_1,...,\ell_n\right)\right)\mathbf{T}+\underline{t},$$

avec $\left(\ell_1,...,\ell_n\right)=\left(x_1,...,x_n\right)\mathbf{S}+\underline{s}$.

La clé publique est alors l'ensemble des polynômes quadratiques:

$$\left(g_1,...,g_m\right).$$

Selon un mode de réalisation, le circuit électronique utilise les fonctions de mappage MAP et MAP_I et les polynômes $f_1^{Boost},...,f_t^{Boost}\in\mathbb{K}\left[Y_1,...,Y_t\right]$ pour les opérations impliquant la clé privée, telles que le déchiffrement ou la signature.

Le circuit électronique peut mettre en œuvre le chiffrement et le déchiffrement de la façon suivante. Soient $\mathbb{L}$ un corps et $Hash:\mathbb{F}_q^n\rightarrow\mathbb{L}$ une fonction de hachage cryptographique publique. Une fonction de hachage cryptographique est une fonction de hachage qui est notamment résistante aux collisions (il est en pratique impossible de trouver un message qui donne le même hash que celui d'un message aléatoire donné). De plus, il est en pratique impossible de retrouver le contenu d'un message à partir de son hash (calculé par une fonction de hachage cryptographique).

Pour chiffrer un message clair $\underline{M}=\left(M_1,...,M_n\right)\in\mathbb{F}_q^n$, le circuit

électronique calcule, selon une mise en œuvre possible, un hash $\underline{h}=\mathrm{Hash}(\underline{M})\in\mathbb{L}$ et un message chiffré tronqué c:

$$c\in\mathbb{F}_q^m=(c_1,...,c_m)=\left(g_1\left(M_1,...,M_n\right),...g_m\left(M_1,...,M_n\right)\right).$$

Le message chiffré correspondant au message clair $\underline{M}$ est défini comme étant le couple $(\underline{c},\underline{h})$.

Le déchiffrement peut alors s'opérer de la manière suivante.

Soit $\underline{r}=(r_1,...,r_{n-m})\in\mathbb{F}_q^{n-m}$ et $\underline{c}'=((\underline{c},\underline{r})-\underline{t}).\mathbf{T}^{-1}$. Le possesseur de la clé privée peut déchiffrer le message chiffré $(\underline{c},\underline{h})$ en recherchant, pour chaque $\underline{r}=(r_1,...,r_{n-m})\in\mathbb{F}_q^{n-m}$, les solutions $\underline{Z}\in\mathbb{K}^t$ du système:

$$f_1^{Boost}(\underline{Z})=C'_1,...,f_t^{Boost}(\underline{Z})=C'_t,$$

avec $(C'_1,...,C'_t)=\mathrm{MAP_I}\left(\varphi^{-1}(\underline{c}')\right)$.

Le circuit électronique calcule alors $\underline{M}\in\varphi((\mathrm{MAP}^{-1}(\underline{Z})-\underline{s})\cdot\mathbf{S}^{-1})$ pour un $\underline{Z}$ solution de l'équation (2), telle que $\mathrm{Hash}(\varphi((\mathrm{MAP}^{-1}(\underline{Z})-\underline{s})\cdot\mathbf{S}^{-1}))=\underline{h}$. S'il y a plusieurs $\underline{M}$ possibles (MAP^{-1} renvoyant une préimage comprenant plusieurs éléments), le circuit électronique recherche parmi eux un élément $\underline{M}$ qui a la bonne empreinte $\underline{h}$. Si la première solution $\underline{Z}$ trouvée ne convient pas (le hash du ou de chacun des message(s) $\underline{M}$ estimé(s) n'est pas égal à $\underline{h}$ et ne correspond donc pas), le circuit électronique teste une autre des solutions $\underline{Z}$, jusqu'à tomber sur la bonne. Plus précisément, si aucune des solutions pour un $\underline{r}=(r_1,...,r_{n-m})\in\mathbb{F}_q^{n-m}$ donné ne convient, le circuit sélectionne un autre $\underline{r}=(r_1,...,r_{n-m})\in\mathbb{F}_q^{n-m}$ et recherche toutes les solutions pour ce $\underline{r}=(r_1,...,r_{n-m})\in\mathbb{F}_q^{n-m}$. Le calcul de hash permet ainsi de déterminer

laquelle des solutions est la bonne dans l'hypothèse où il y aurait plusieurs solutions.

Selon une mise en œuvre possible, le circuit électronique calcule une signature électronique de la manière suivante.

Le circuit électronique applique le procédé de déchiffrement précédemment décrit sur un message $\underline{M}$ à signer, auquel il a préalablement concaténé des valeurs tirées aléatoirement.

Soit $\mathrm{Hash}:\mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ une fonction de hachage cryptographique, qui peut être la même que la fonction de hachage utilisée pour le déchiffrement (on a alors $\mathbb{L} \simeq \mathbb{F}_q^m$) ou être une fonction de hachage différente (il importe évidemment que la fonction de hachage utilisée pour le chiffrement soit la même que celle utilisée pour le déchiffrement, et que la fonction de hachage utilisée pour la signature soit la même que celle utilisée pour la vérification de signature).

Pour signer un message $\underline{M} \in \mathbb{F}_q^n$, le circuit électronique calcule, selon un mode de réalisation possible, l'empreinte $\underline{a} = (a_1,...,a_m) = \mathrm{Hash}(\underline{M}) \in \mathbb{F}_q^m$ du message $\underline{M}$ à signer. Le circuit électronique tire aléatoirement $(n-m)$ valeurs $(r_1,...,r_{n-m}) \in \mathbb{F}_q^{n-m}$ et calcule une solution $\underline{Z} \in \mathbb{K}^t$ du système:

$$f_1^{\mathrm{Boost}}(\underline{Z}) = C'_1,...,f_t^{\mathrm{Boost}}(\underline{Z}) = C'_t \qquad (3)$$

avec: $(C'_1,...,C'_t) = \mathrm{MAP_I}\left(\varphi^{-1}\left(((\underline{a},r_1,...,r_{n-m}) - \underline{t})\cdot \mathbf{T}^{-1}\right)\right)$.

Le vecteur $\underline{sig} \in \varphi((\mathrm{MAP}^{-1}(\underline{Z}) - \underline{s})\cdot \mathbf{S}^{-1})$ tel que $F_{SEC}\left(\varphi^{-1}(\underline{sig})\right) = \varphi^{-1}\left(((\underline{a},r_1,...,r_{n-m}) - \underline{t})\cdot \mathbf{T}^{-1}\right)$ est une signature du message $\underline{M}$.

Pour un $(a_1,...,a_m,r_1,...,r_{n-m})$ donné, il est possible que l'équation

(3) n'ait aucune solution. Si c'est le cas, le circuit électronique répète le procédé avec d'autres valeurs pour $r_1, \ldots, r_{n-m}$. Par exemple, le circuit électronique génère de nouveaux nombres aléatoires $r_1, \ldots, r_{n-m}$, ou incrémente les nombres aléatoires précédemment générés. Pour vérifier que la signature $\underline{sig}$ est valide pour $\underline{M}$, le circuit électronique compare $\underline{a} = Hash(\underline{M})$ avec l'évaluation de la signature $\underline{sig}$ en la clé publique. Autrement dit, le circuit électronique teste si $\left(g_1\left(\underline{sig}\right), \ldots, g_m\left(\underline{sig}\right)\right) = \underline{a}$.

Si l'égalité n'est pas vérifiée, alors $\underline{sig}$ n'est pas une signature valide du message $\underline{M}$.

Un exemple particulier de réalisation est illustré ci-dessous:

Soit $(q, n, m, t, D) \in \mathbb{N}^5$ avec q une puissance d'un nombre premier et $t = 1$. Par exemple, q peut être une puissance de 2. Le circuit électronique utilise comme polynôme HFE un polynôme F_{SEC} tel que: $F_{SEC} = F_{Boost} \circ X^{q^d} \in \mathbb{F}_{q^n}[X]$, avec $d, 1 < d < n$, et $F_{Boost} \in \mathbb{F}_{q^n}[X]$ un polynôme de type HFE de degré D_{Boost}.

Ainsi, F_{SEC} est un polynôme type HFE de degré $D_{SEC} = q^d . D_{Boost}$. Ceci revient à poser $\mathbb{K} = \mathbb{F}_{q^n}$, $f_1^{Boost} = F_{Boost}$, $MAP_I: X \mapsto X$ et $MAP: X \mapsto X^{q^d}$. Comme $D_{Boost} = D_{SEC} / q^d$, le circuit électronique peut déterminer les racines de F_{Boost} en un temps inférieur à $O\left(C\left(D_{SEC}\right)\right)$. On entend par là que l'on trouve les racines du polynômes F_{Boost} plus vite que les racines du polynôme F_{SEC}, ce qui permet d'accélérer le traitement par rapport à l'algorithme HFE conventionnel de l'état de l'art.

Dans cet exemple de réalisation, le polynôme de type HFE est la composée de deux polynômes. Que ce soit une composée n'influence pas la sécurité (ne la réduit pas). Mais le fait que ce polynôme soit une composée permet, pour le titulaire de la clé privée qui connaît la décomposition, de résoudre plus facilement et donc plus rapidement l'équation, et donc d'effectuer une opération à clé privée plus rapidement. Il suffit de rechercher en deux étapes les solutions de polynômes de plus bas degré.

Ainsi, si l'on note $Z \in \mathbb{F}_{q^n}$ une racine de F_{SEC}, on constate que:

$$F_{Boost}(MAP(Z)) = F_{Boost}(Z^{q^d}) = F_{SEC}(Z).$$

MAP donc transforme bien les racines de F_{SEC} en les racines de F_{Boost}. L'inverse de MAP est $MAP^{-1}: X \mapsto X^{q^{n-d}}$. En effet, $MAP^{-1}(MAP(X)) = MAP^{-1}(X^{q^d}) = X^{q^n} = X$ dans $\mathbb{F}_{q^n}$. Comme $D_{Boost} = D_{SEC}/q^d$, les racines de F_{Boost} peuvent être calculées en un temps inférieur à $O(C(D_{SEC}))$. On entend par là que l'on trouve les racines du polynômes F_{Boost} plus vite que les racines du polynôme F_{SEC}, ce qui permet d'accélérer le traitement par rapport à l'algorithme HFE conventionnel de l'état de l'art. Dans cet exemple, MAP et MAP^{-1} sont linéaires.

Un autre exemple particulier de réalisation est illustré ci-après.

Soit $(q, n, m, t, D) \in \mathbb{N}^5$ avec $q = 2,\ t = 1,\ n \geq 3$.

Soit $F_{SEC} = F_{Boost} \circ X^3 \in \mathbb{F}_{2^n}[X]$, avec F_{SEC} un polynôme type HFE de degré D_{SEC} et $F_{Boost} \in \mathbb{F}_{q^n}[X]$ un polynôme de degré D_{Boost}. Les termes de F_{SEC} sont tous divisibles par X^3. F_{SEC} est de degré $D_{SEC} \leq 3 \cdot D_{Boost}$.

Nous avons ici $\mathbb{K} = \mathbb{F}_{2^n}$, $f_1^{Boost} = F_{Boost}$, $MAP_I: X \mapsto X$ et $MAP: X \mapsto X^3$.

Cet exemple se distingue de l'exemple précédent notamment en ce que 3 (dans X^3) n'est pas une puissance (d'exposant strictement supérieur à 1) d'un nombre premier (et notamment, 3 n'est pas une puissance de 2).

Soit Z une racine de F_{SEC}. On a: $F_{Boost}(MAP(Z))=F_{Boost}(Z^3)=F_{SEC}(Z)$. MAP transforme donc bien les racines de F_{SEC} en les racines de F_{Boost}. Comme $D_{Boost}=D_{SEC}/3$, les racines de F_{Boost} sont calculables en un temps inférieur à $O(C(D_{SEC}))$. On entend par là que l'on trouve les racines du polynômes F_{Boost} plus vite que les racines du polynôme F_{SEC}, ce qui permet d'accélérer le traitement par rapport à l'algorithme HFE conventionnel de l'état de l'art.

Un troisième exemple particulier de réalisation est illustré ci-après.

Soit $(q, n, m, t, D) \in \mathbb{N}^5$ avec $q = 2$, $t = 2$, $n \geq 3$.

Soit $F_{SEC} = F(X^2) + X \in \mathbb{F}_{2^n}[X]$, avec F un polynôme type HFE de degré D. On définit: $\mathbb{K} = \mathbb{F}_{2^n}$, $f_1^{Boost}(Y_1,Y_2)=F(Y_1)+Y_2$, $f_2^{Boost}(Y_1,Y_2)=Y_1-(Y_2)^2$ $MAP_I:X \mapsto (X,0)$, et $MAP(X)=(X^2,X)$. Soit Z une racine de F_{SEC}.

On a: $f_1^{Boost}(MAP(Z))=F(Z^2)+Z=F_{SEC}(Z)=0$, et

$f_2^{Boost}(MAP(Z))=Z^2-Z^2=0$.

MAP transforme donc bien une racine de F_{SEC} en une racine commune de f_1^{Boost} et de f_2^{Boost}.

Dans cet exemple, MAP^{-1} est donnée par $(Y_1, Y_2) \mapsto Y_2$.

De façon plus générale, il a été exposé qu'au lieu d'une simple composition il est possible de mettre en place une transformation (grâce à la

fonction de mappage MAP) qui permet de transformer la représentation d'un polynôme de type HFE conventionnel grâce à ensemble de polynômes supplémentaires permettant de simplifier (et donc accélérer) le calcul.

L'invention ne se limite pas aux formes de réalisation décrites ci-avant à titre d'exemple. Elle s'étend à d'autres variantes.

Les divers circuits électroniques et sous circuits électroniques envisagés peuvent être chacun tout circuit électronique approprié, par exemple un circuit électronique dédié, un FPGA, un ASIC, un microcontrôleur, un DSP, ou encore un circuit comprenant un processeur et une mémoire, la mémoire stockant un programme d'ordinateur approprié.

Les mémoires utilisables ne se limitent pas aux exemples donnés à titre purement illustratif mais couvrent tout type de mémoire fonctionnellement équivalent.

Les modes de réalisation décrits en relation avec les procédés selon l'invention se transposent aux circuits électroniques, ainsi qu'aux programmes d'ordinateur et aux supports de stockage selon l'invention, et réciproquement.

REVENDICATIONS

1. Procédé de mise en œuvre accélérée, par un circuit électronique (SC), d'un algorithme cryptographique HFE exploitant une clé privée HFE basée sur un polynôme (F_{SEC}) de type HFE, sur un morphisme (φ), et sur une première (S) et une deuxième (T) transformations affines, le procédé comprenant:

/E1/ une utilisation, par le circuit électronique (SC), d'au moins un polynôme ($f_1^{Boost},...,f_t^{Boost}$) supplémentaire compris dans la clé privée HFE, et

/E2/ une utilisation, par le circuit électronique (SC), d'une première (MAP) et d'une deuxième (MAP_I) fonctions de mappage comprises dans la clé privée HFE, et associant chacune, à un paramètre d'entrée (A, C') donné, autant de paramètres de sortie ($A_1,...,A_t,C'_1,...,C'_t$) qu'il y a de polynômes ($f_1^{Boost},...,f_t^{Boost}$) supplémentaires dans la clé privée HFE,

l'au moins un polynôme ($f_1^{Boost},...,f_t^{Boost}$) supplémentaire et les fonctions de mappage (MAP, MAP_I) étant tels que, pour un paramètre (C') donné, et pour toute racine (A) du polynôme (F_{SEC}) de type HFE moins ledit paramètre (C') donné, le résultat ($A_1,...,A_t$) de la première fonction de mappage (MAP) appliquée à ladite racine (A) est une racine de chaque polynôme (f_i^{Boost}) supplémentaire moins un paramètre de sortie (C'_i), correspondant audit chaque polynôme (f_i^{Boost}) supplémentaire, de la deuxième fonction de mappage (MAP_I) appliquée audit paramètre (C') donné.

2. Procédé selon la revendication 1, comprenant une génération, par le circuit électronique (SC), de ladite clé privée HFE, ladite génération comprenant:

/G1/ une génération, par le circuit électronique (SC), dudit au moins un polynôme ($f_1^{Boost},...,f_t^{Boost}$) supplémentaire et

/G2/ une génération, par le circuit électronique (SC), desdites fonctions de mappage (MAP, MAP_I).

3. Procédé selon la revendication 1 ou 2, comprenant une opération de déchiffrement mise en œuvre par :

/D1/ une réception, par le circuit électronique (SC), d'un message sous forme chiffrée et d'un hash calculé sur le message sous forme non chiffrée,

/D2/ une application, par le circuit électronique (SC), de l'inverse de la deuxième transformation affine (T) au message sous forme chiffrée afin d'obtenir un message chiffré intermédiaire,

/D3/ une application, par le circuit électronique (SC), de l'inverse du morphisme (φ) au message chiffré intermédiaire,

/D4/ une obtention d'au moins un paramètre de sortie ($C'_1,\ldots,C'_l$), par application, par le circuit électronique (SC), de la deuxième fonction de mappage (MAP_I) au résultat de ladite application de l'inverse du morphisme (φ),

/D5/ une résolution, par le circuit électronique (SC), d'un système d'équation(s) tel que chaque polynôme (f_i^{Boost}) supplémentaire soit égal au paramètre de sortie (C'_i) respectif obtenu à l'étape précédente,

/D6/ une application, par le circuit électronique (SC), de l'inverse de la première fonction de mappage (MAP) à une solution du système d'équation(s),

/D7/ une application, par le circuit électronique (SC), du morphisme (φ) au résultat de l'inverse de la première fonction de mappage (MAP) obtenu à l'étape précédente,

/D8/ une obtention d'une estimation du message sous forme non chiffrée, par application, par le circuit électronique (SC), de l'inverse de la première transformation affine (S) au résultat du morphisme (φ) obtenu à l'étape précédente,

/D9/ un calcul, par le circuit électronique (SC), d'un hash de l'estimation du message sous forme non chiffrée,

/D10/ si le hash de l'estimation du message sous forme non chiffrée est différent du hash reçu, l'obtention d'une autre estimation du message sous forme non chiffrée selon les étapes précédentes, jusqu'à ce que les deux hash soient égaux.

4. Procédé selon l'une des revendications précédentes, comprenant une opération de signature mise en œuvre par :

/S1/ un calcul, par le circuit électronique (SC), d'un hash d'un message à signer,

/S2/ une génération, par le circuit électronique (SC), d'un nombre aléatoire de taille égale à la taille d'un élément de l'ensemble d'arrivée du morphisme (φ) moins la taille du hash du message à signer,

/S3/ une application, par le circuit électronique (SC), de l'inverse de la deuxième transformation affine (T) à une concaténation du nombre aléatoire et du hash du message à signer,

/S4/ une application, par le circuit électronique (SC), de l'inverse du morphisme (φ) au résultat de l'application de l'inverse de la deuxième transformation affine (T),

/S5/ une obtention d'au moins un paramètre de sortie ($C'_1,\ldots,C'_l$), par application, par le circuit électronique (SC), de la deuxième fonction de mappage (MAP_I) au résultat de ladite application de l'inverse du morphisme (φ),

/S6/ une résolution, par le circuit électronique (SC), d'un système d'équation(s) tel que chaque polynôme (f_i^{Boost}) supplémentaire soit égal au paramètre de sortie (C'_i) respectif obtenu à l'étape précédente,

/S7/ si le système d'équation(s) n'admet pas de solution, une répétition des étapes précédentes avec un autre nombre aléatoire,

/S8/ une application, par le circuit électronique (SC), de l'inverse de la première fonction de mappage (MAP) à une solution du système d'équation(s),

/S9/ une application, par le circuit électronique (SC), du morphisme (φ) au résultat de l'inverse de la première fonction de mappage (MAP) obtenu à l'étape précédente,

/S10/ une obtention d'une signature du message à signer, par application, par le circuit électronique (SC), de l'inverse de la première transformation affine (S) au résultat du morphisme (φ) obtenu à l'étape précédente.

5. Procédé selon l'une des revendications précédentes, dans lequel la clé privée HFE comprend un unique polynôme supplémentaire, dans lequel la première fonction de mappage (MAP) est un monôme, et dans lequel le polynôme de type HFE (F_{SEC}) est égal à la composition du polynôme supplémentaire avec la première fonction de mappage (MAP).

6. Programme d'ordinateur comprenant une suite d'instructions mettant en œuvre les étapes du procédé selon l'une des revendications 1 à 5 lorsqu'elles sont exécutées par un processeur.

7. Support de stockage non transitoire lisible par ordinateur comprenant un programme d'ordinateur selon la revendication 6.

8. Circuit électronique (SC) agencé pour mettre en œuvre de façon accélérée un algorithme cryptographique HFE exploitant une clé privée HFE basée sur un polynôme (F_{SEC}) de type HFE, sur un morphisme (φ), et sur une première (S) et une deuxième (T) transformations affines, le circuit électronique (SC) comprenant:

un sous circuit électronique d'utilisation d'au moins un polynôme ($f_1^{Boost},...,f_t^{Boost}$) supplémentaire compris dans la clé privée HFE, et

un sous circuit électronique d'utilisation d'une première (MAP) et d'une deuxième (MAP_I) fonctions de mappage comprises dans la clé privée HFE, et associant chacune, à un paramètre d'entrée (A, C') donné, autant de paramètres de sortie ($A_1,...,A_t,C'_1,...,C'_t$) qu'il y a de polynômes ($f_1^{Boost},...,f_t^{Boost}$) supplémentaires dans la clé privée HFE,

l'au moins un polynôme ($f_1^{Boost},...,f_t^{Boost}$) supplémentaire et les fonctions de mappage (MAP, MAP_I) étant tels que, pour un paramètre (C') donné, et pour toute racine (A) du polynôme (F_{SEC}) de type HFE moins ledit paramètre (C') donné, le résultat ($A_1,...,A_t$) de la première fonction de mappage (MAP) appliquée à ladite racine (A) est une racine de chaque polynôme (f_i^{Boost}) supplémentaire moins un paramètre de sortie (C'_i), correspondant audit chaque polynôme (f_i^{Boost}) supplémentaire, de la deuxième fonction de mappage (MAP_I) appliquée audit paramètre (C') donné.

9. Circuit électronique (SC) selon la revendication 8, comprenant, afin de mettre en œuvre une opération de déchiffrement :

un sous circuit électronique de réception d'un message sous forme chiffrée et d'un hash calculé sur le message sous forme non chiffrée,

un sous circuit électronique d'application de l'inverse de la deuxième transformation affine (T) au message sous forme chiffrée afin d'obtenir un message chiffré intermédiaire,

un sous circuit électronique d'application de l'inverse du morphisme (φ) au message chiffré intermédiaire,

un sous circuit électronique d'obtention d'au moins un paramètre de sortie ($C'_1,\ldots,C'_t$), par application de la deuxième fonction de mappage (MAP_I) au résultat de ladite application de l'inverse du morphisme (φ),

un sous circuit électronique de résolution d'un système d'équation(s) tel que chaque polynôme (f_i^{Boosi}) supplémentaire soit égal au paramètre de sortie (C'_i) respectif,

un sous circuit électronique d'application de l'inverse de la première fonction de mappage (MAP) à une solution du système d'équation(s),

un sous circuit électronique d'application du morphisme (φ) au résultat de l'inverse de la première fonction de mappage (MAP),

un sous circuit électronique d'obtention d'une estimation du message sous forme non chiffrée, par application de l'inverse de la première transformation affine (S) au résultat de l'application du morphisme (φ),

un sous circuit électronique de calcul d'un hash de l'estimation du message sous forme non chiffrée,

un sous circuit électronique de vérification agencé pour vérifier si le hash de l'estimation du message sous forme non chiffrée est différent du hash reçu, et dans l'affirmative pour déclencher l'obtention d'une autre estimation du message sous forme non chiffrée, jusqu'à ce que les deux hash soient égaux.

10. Circuit électronique (SC) selon la revendication 8 ou 9, dans lequel la clé privée HFE comprend un unique polynôme supplémentaire, dans lequel la

première fonction de mappage (MAP) est un monôme, et dans lequel le polynôme de type HFE (F_{SEC}) est égal à la composition du polynôme supplémentaire avec la première fonction de mappage (MAP).

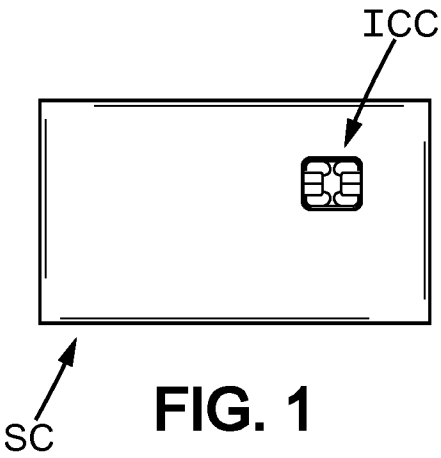


FIG. 1

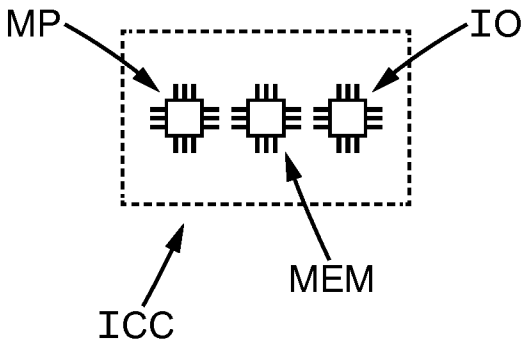


FIG. 2

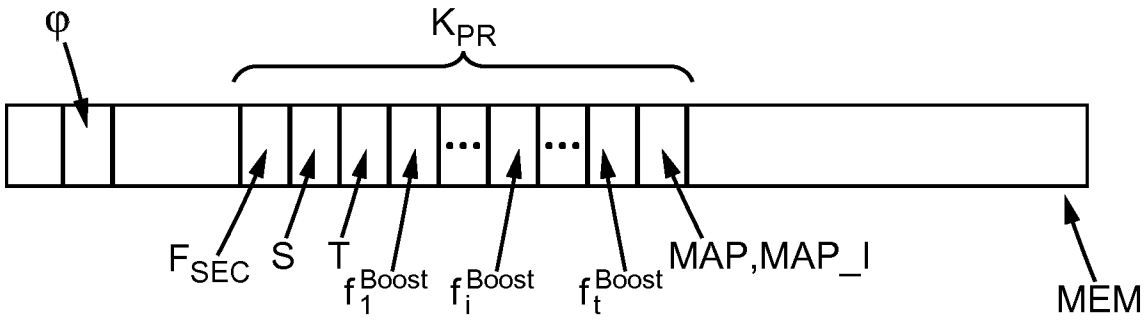


FIG. 3

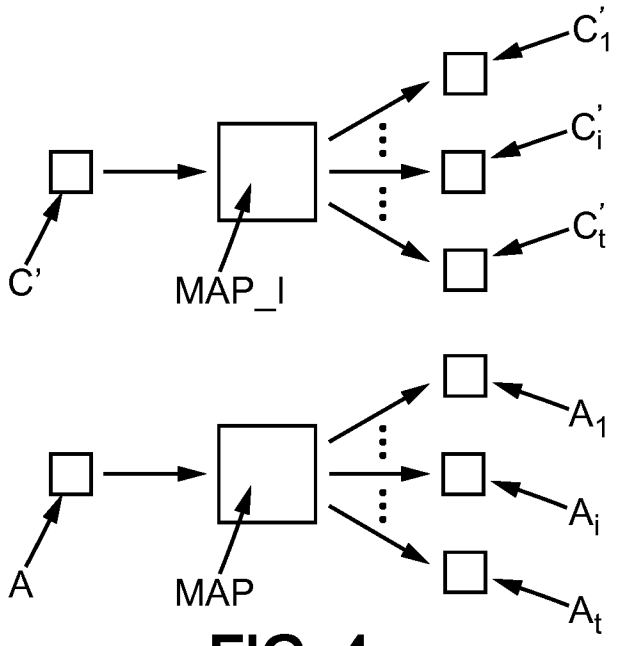


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/051686

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	WUQIANG SHEN ET AL: "TOT, a Fast Multivariate Public Key Cryptosystem with Basic Secure Trapdoor", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20131125:191504, 21 November 2013 (2013-11-21), pages 1-17, XP061015108, section 3	1-10

X	OLIVIER BILLET ET AL: "Analysis of Intermediate Field Systems", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20091108:042928, 5 November 2009 (2009-11-05), pages 1-8, XP061003653,	1-4,6-9
A	section 3	5,10

	-/--	

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

* Special categories of cited documents :

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

"E" earlier 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
10 October 2016	21/10/2016

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/FR2016/051686

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	CHRISTOPHER WOLF ET AL: "Asymmetric Cryptography: Hidden Field Equations", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20050806:144437, 6 August 2005 (2005-08-06), pages 1-22, XP061006290, section 2 -----	3,9

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2016/051686

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	WUQIANG SHEN ET AL: "TOT, a Fast Multivariate Public Key Cryptosystem with Basic Secure Trapdoor", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20131125:191504, 21 novembre 2013 (2013-11-21), pages 1-17, XP061015108, section 3	1-10

X	OLIVIER BILLET ET AL: "Analysis of Intermediate Field Systems", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20091108:042928, 5 novembre 2009 (2009-11-05), pages 1-8, XP061003653,	1-4,6-9
A	section 3	5,10

	-/--	

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

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

* Catégories spéciales de documents cités:

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

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

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

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

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

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

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

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

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

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 octobre 2016	21/10/2016

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
T	CHRISTOPHER WOLF ET AL: "Asymmetric Cryptography: Hidden Field Equations", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20050806:144437, 6 août 2005 (2005-08-06), pages 1-22, XP061006290, section 2 -----	3,9

1