(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 808 145**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 05254**

(51) Int Cl[7] : **H 04 L 9/08,** G 06 F 17/00, G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 25.04.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 26.10.01 Bulletin 01/43.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *GEMPLUS Société en commandite par actions* — FR.

(72) **Inventeur(s) :** NACCACHE DAVID et DABBOUS NORA.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) PROCEDE DE CALCUL D'UNE DONNEE DE CONTROLE.

(57) L'invention concerne un procédé de calcul d'une donnée de contrôle d'un algorithme à clé secrète à N bits, dont N-N/ n bits aléatoires et de chiffrement et N/ n bits de somme de contrôle, caractérisé en ce qu'il comporte les étapes suivantes:

- chiffrer un message déterminé de K bits à l'aide des N-N/ n bits de chiffrement de la clé,
- construire une donnée de contrôle en sélectionnant N/ n bits parmi les K bits du message chiffré,
- intégrer un des N/ n bits de ladite donnée de contrôle tous les n-1 bits de chiffrement de manière à constituer une clé secrète complète de N bits.

L'invention s'applique particulièrement au DES, la donnée de contrôle étant construite à partir d'un message constant.

FR 2 808 145 - A1

PROCEDE DE CALCUL D'UNE DONNEE DE CONTROLE

L'invention concerne un procédé de calcul d'une donnée de contrôle pour algorithme cryptographique à clé secrète. Une telle donnée de contrôle est essentiellement utilisée dans le cadre de l'algorithme DES (de l'anglais Data Encryption Standard), elle est alors connue sous le terme anglais de « checksum » et consiste à attacher des valeurs spécifiques redondantes à la clé secrète. Le procédé selon l'invention est basé sur le calcul d'une donnée de contrôle à partir d'un message déterminé (connu et préférentiellement constant). Dans la suite du texte, on utilisera le terme usuel de checksum pour désigner cette donnée de contrôle.

La présente invention concerne plus spécifiquement l'algorithme DES qui est en effet le seul algorithme à clé secrète actuellement connu qui utilise un calcul de checksum, objet de l'invention.

Le DES est un des algorithmes cryptographiques à clé secrète les plus connus et les plus utilisés. Un tel algorithme est dit symétrique car il exploite une unique clé de 64 bits, secrète et réversible pour chiffrer et déchiffrer des données.

Plus spécifiquement, le DES comporte une clé de 64 bits secrets dont 56 sont des bits de chiffrement (et déchiffrement) aléatoires et 8 sont des bits de checksum. En fonctionnement, le DES génère 16 sous-clés de 48 bits à partir des 56 bits aléatoires. Ainsi, dans chacun des 8 octets de la clé du DES, les 7 premiers sont aléatoires et utilisés pour calculer les sous-clés, et le dernier bit fait partie de la checksum. En général, les bits de cette checksum sont des bits de

parité, c'est à dire qu'ils sont calculés par une opération de « ou exclusif » sur les 7 premiers bits de chaque octet.

La checksum est essentiellement utilisée pour protéger la clé du DES contre des attaques mémoires ou DFA (de l'Anglais Differential Fault Attack) qui consistent à modifier un par un les bits de la clé pour tenter de la déterminer. Par exemple, les bits à 1 sont forcés à 0, un par un, et le DES est utilisé avec ces modifications pour chiffrer le même message jusqu'à ce que tous les bits de la clé soient à zéro (le message chiffré est alors constant). On remonte alors la chaîne des messages chiffrés et on peut ainsi parvenir à déterminer quels étaient les bits à 1 dans la clé initiale.

La checksum permet d'éviter de telles attaques. On peut en effet recalculer régulièrement la checksum (composée classiquement des bits de parité) et détecter ainsi une modification d'un ou plusieurs des bits de la clé.

En revanche, la connaissance de la checksum peut laisser filtrer des informations sur les bits de chiffrement de la clé, en révélant si le nombre de bits à 1 est pair ou impair dans chaque octet.

L'objectif de la présente invention est de résoudre cet inconvénient et de proposer un procédé de calcul d'une checksum qui ne divulgue aucune information sur les bits secrets de la clé.

A cette fin, le procédé propose de construire une checksum à partir d'un message déterminé, encodé à l'aide des seuls bits de chiffrement de la clé, et d'intégrer les bits de cette checksum aux bits de chiffrement de la clé pour reconstituer une clé complète. L'algorithme sera ensuite utilisé selon un

fonctionnement classique avec une clé composée des bits de chiffrement aléatoires et de cette checksum construite.

L'invention a plus particulièrement pour objet un procédé de calcul d'une donnée de contrôle d'un algorithme à clé secrète à N bits, dont N-N/n bits aléatoires de chiffrement et N/n bits de donnée de contrôle, caractérisé en ce qu'il comporte les étapes suivantes :

- chiffrer un message déterminé de K bits à l'aide des N-N/n bits de chiffrement de la clé,
- construire une donnée de contrôle en sélectionnant N/n bits parmi les K bits du message chiffré,
- intégrer un des N/n bits de ladite donnée de contrôle tous les n-1 bits de chiffrement de la clé de manière à constituer une clé secrète complète de N bits.

Selon une caractéristique, le message déterminé est un message constant.

Selon une particularité, les K bits d'entrée du message constant ont la même valeur.

Selon une autre caractéristique, la donnée de contrôle est composée des N/n premiers bits du message chiffré.

Selon une caractéristique, K est égal à N.

Selon une application préférentielle, l'algorithme à clé secrète est le DES, ladite clé ayant 64 bits, dont 56 bits de chiffrement et 8 bits de donnée de contrôle.

Selon une caractéristique, l'algorithme à clé secrète étant implémenté dans un composant électronique, la construction de la donnée de contrôle est effectuée une seule fois par clé, lors de la

fabrication du composant électronique ou lors de la première utilisation du composant électronique avec une clé donnée.

Selon une caractéristique, le procédé consiste en outre à vérifier l'intégrité de la clé secrète complète en comparant une donnée de contrôle recalculée, à partir du même message déterminé, avec la donnée de contrôle construite.

Selon une caractéristique, la vérification de la donnée de contrôle est réalisée à chaque mise sous tension du composant électronique.

Selon une autre caractéristique, la vérification de la donnée de contrôle est réalisée avant chaque appel à l'algorithme.

Selon une caractéristique, lorsque la vérification de la donnée de contrôle est erronée, le procédé comporte une fonction de blocage de l'algorithme avec la clé secrète construite et/ou une fonction de blocage du composant électronique.

L'invention s'applique à tout support sécurisé, de type carte à puce, ou à tout dispositif de calcul, de type ordinateur muni d'un logiciel de chiffrement, comportant un composant électronique apte à mettre en œuvre le procédé selon l'invention.

Le procédé selon l'invention permet de construire une checksum qui ne révèle aucune information sur la clé secrète à laquelle elle est associée. En effet, la checksum n'est plus du tout liée à la parité des bits de chiffrement de la clé.

En outre, cette checksum ne contenant aucune information sensible, il n'est même pas nécessaire de la masquer.

La sécurité de la clé reste néanmoins assurée puisque la vérification qu'aucune attaque n'a été intentée demeure, en calculant une nouvelle checksum et en la comparant à la checksum initialement construite.

Le procédé selon l'invention requiert un premier fonctionnement de l'algorithme avec les seuls bits de chiffrement de la clé, de manière à recalculer la checksum pour vérification, ce qui représente un coût en temps. Cependant, ce coût en temps est compensé par le gain en sécurité qu'apporte le procédé selon l'invention.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est faite ci-après et qui est donnée à titre d'exemple illustratif et non limitatif.

La description fait référence à un algorithme DES à clé secrète de 64 bits. En effet, parmi les algorithmes actuellement connus, seul le DES utilise une checksum pour contrer les attaques mémoires de type DFA. Néanmoins, le procédé selon l'invention pourrait être appliqué à d'autres algorithmes symétriques utilisant des clés secrètes éventuellement plus longues.

L'objet de l'invention est de construire une checksum qui ne révèle aucune information sur les 56 bits de chiffrement de la clé du DES.

A cet effet, un message déterminé M de K bits, c'est à dire non tenu secret, est encodé par les 56 bits de chiffrement du DES. Selon un mode de réalisation préférentiel, on choisit un message M de 64 bits constants, c'est à dire fixés et connus. Selon un mode de réalisation, le message M peut être composé de K bits ayant tous la même valeur, par exemple tous à 0.

Le message chiffré M' en sortie du DES comporte K bits (64 dans l'exemple) qui ne divulguent absolument rien des 56 bits de chiffrement utilisés par l'algorithme.

L'invention consiste alors à sélectionner 8 bits parmi les 64 bits du message chiffré M'. N'importe quels bits peuvent être sélectionnés, mais pour simplifier, on choisit préférentiellement les 8 premiers, c'est à dire le premier octet du texte chiffré M'. Ces 8 bits forment alors la checksum du DES Co.

Les bits de cette checksum construite Co sont ensuite intégrés aux 56 bits de chiffrement aléatoire pour former une clé complète de 64 bits. Chaque bit de la checksum est placé entre les bits de chiffrement tous les 7 bits.

La checksum Co ainsi construite l'est une fois pour toute pour une clé donnée, soit en fin de production lors de la fabrication du composant électronique sur lequel le DES est implémenté, soit lors de la première utilisation dudit composant avec cette clé. Il existe en effet des applications dans lesquelles la clé du DES peut être modifiée, une nouvelle construction de la checksum Co est alors nécessaire.

Par la suite, le DES retrouve un fonctionnement classique, c'est à dire qu'il code et décode des messages avec une clé de 64 bits dont 56 sont aléatoires et 8 sont une checksum ne contenant strictement aucune information sur lesdits bits de chiffrement.

Cependant, la protection contre d'éventuelles attaques mémoire de type DFA reste assurée en recalculant une checksum C_1 et en la comparant à celle

construite Co, par exemple à chaque mise sous tension du composant, ou avant chaque appel au DES.

La checksum de vérification C_1 est calculée avec les 56 bits de chiffrement de la clé à partir du message constant M initial, et déterminée par 8 des bits du message ainsi chiffré M' (on reprend les mêmes bits que pour Co, les premiers par exemple).

Si une attaque DFA a été intentée et qu'un bit de la clé a été modifié, la checksum C_1 calculée avec la clé attaquée à partir du même message constant M initial sera nécessairement différente de celle construite initialement et mémorisée Co. En effet, le DES étant un algorithme non linéaire, de nombreux bits du message chiffré M' seront modifiés par la modification d'un seul bit de la clé et la checksum C_1 reconstruite à partir de cette clé attaquée aura certainement des bits différents de Co.

En revanche, si C_1=Co, la clé n'a subi aucune attaque, et elle peut être utilisée en toute tranquillité.

Par contre, si $C_1 \neq C_0$, la clé a subi une attaque. Le procédé selon l'invention comporte alors une fonction de blocage de l'utilisation de l'algorithme de chiffrement/déchiffrement avec cette clé secrète complète construite, et/ou une fonction de blocage de l'utilisation du composant électronique sur lequel le procédé est implanté (par exemple une carte à puce).

REVENDICATIONS

1. Procédé de calcul d'une donnée de contrôle pour algorithme cryptographique à clé secrète à N bits, dont N-N/n bits aléatoires de chiffrement et N/n bits de donnée de contrôle, caractérisé en ce qu'il comporte les étapes suivantes :

- chiffrer un message déterminé (M) de K bits à l'aide des N-N/n bits de chiffrement de la clé,
- construire une donnée de contrôle (Co) en sélectionnant N/n bits parmi les K bits du message chiffré (M'),
- intégrer un des N/n bits de ladite donnée de contrôle (Co) tous les n-1 bits de chiffrement de manière à constituer une clé secrète complète de N bits.

2. Procédé de calcul d'une donnée de contrôle selon la revendication 1, caractérisé en ce que le message déterminé (M) est un message constant.

3. Procédé de calcul d'une donnée de contrôle selon la revendication 2, caractérisé en ce que tous les bits d'entrée du message constant (M) ont la même valeur.

4. Procédé de calcul d'une donnée de contrôle selon l'une des revendications 1 à 3, caractérisé en ce que la donnée de contrôle (Co) est composée des N/n premiers bits du message chiffré (M').

5. Procédé de calcul d'une donnée de contrôle selon l'une des revendications 1 à 4, caractérisé en ce que K égal N.

6. Procédé de calcul d'une donnée de contrôle selon l'une quelconque des revendications précédentes, caractérisé en ce que l'algorithme à clé secrète est le DES (de l'anglais Data Encryption Standard), ladite clé ayant 64 bits, dont 56 bits de chiffrement et 8 bits de donnée de contrôle.

7. Procédé de calcul d'une donnée de contrôle selon l'une quelconque des revendications précédentes, l'algorithme à clé secrète étant implémenté dans un composant électronique, caractérisé en ce que la construction de la donnée de contrôle (Co) est effectuée une seule fois par clé.

8. Procédé selon la revendication 7, caractérisé en ce que la construction de la donnée de contrôle (Co) est réalisée lors de la fabrication du composant électronique muni de la clé.

9. Procédé selon la revendication 7, caractérisé en ce que la construction de la donnée de contrôle (Co) est réalisée lors de la première utilisation du composant électronique avec la clé.

10. Procédé de calcul d'une donnée de contrôle selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste en outre à vérifier l'intégrité de la clé secrète complète en comparant une donnée de contrôle recalculée (C_1), à partir du message

déterminé (M), avec la donnée de contrôle construite (Co).

11. Procédé selon la revendication 10, l'algorithme à clé secrète étant implémenté dans un composant électronique, caractérisé en ce que la vérification de la donnée de contrôle (C_1 = Co) est réalisée à chaque mise sous tension du composant électronique.

12. Procédé selon la revendication 10, caractérisé en ce que la vérification de la donnée de contrôle (C_1 = C_0) est réalisée avant chaque appel à l'algorithme.

13. Procédé selon l'une des revendications 10 à 12, caractérisé en ce qu'il comporte une fonction de blocage de l'algorithme avec la clé secrète complète construite lorsque la vérification de la donnée de contrôle est erronée (C1 ≠ C_0).

14. Procédé selon l'une des revendications 10 à 12, l'algorithme à clé secrète étant implémenté dans un composant électronique, caractérisé en ce que le procédé comporte une fonction de blocage de l'utilisation du composant lorsque la vérification de la donnée de contrôle est erronée (C_1 = C_0).

15. Support sécurisé, de type carte à puce, caractérisé en ce qu'il comporte un composant électronique apte à mettre en œuvre le procédé selon les revendications 1 à 14.

16. Dispositif de calcul, de type ordinateur muni d'un logiciel de chiffrement, caractérisé en ce qu'il

comporte un composant électronique apte à mettre en œuvre le procédé selon les revendications 1 à 13.

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2808145

N° d'enregistrement national

FA 586181
FR 0005254

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 4 262 358 A (MARINO JR JOSEPH T) 14 avril 1981 (1981-04-14) * colonne 1, ligne 27 - ligne 43 * ---	1	H04L9/08 G06F17/00 G06K19/07
A	US 5 063 596 A (DYKE JOHN) 5 novembre 1991 (1991-11-05) * colonne 11, ligne 5 - ligne 7 * -----	1	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04L

Date d'achèvement de la recherche	Examinateur
25 janvier 2001	Holper, G

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)