(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
27 juin 2002 (27.06.2002)

PCT

(10) Numéro de publication internationale
WO 02/51064 A1

(51) Classification internationale des brevets[7] : H04L 9/06

(21) Numéro de la demande internationale :
PCT/FR01/03646

(22) Date de dépôt international :
20 novembre 2001 (20.11.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/16579 19 décembre 2000 (19.12.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de GEMENOS, F-13420 GEMENOS (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **CORON, Jean-Sébastien** [FR/FR]; 4 rue Léon Delagrange, F-75015 PARIS (FR).

(74) Mandataire : **BRUYERE, Pierre**; Gemplus, BP 100, F-13881 Gemenos Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :
— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*
— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

[Suite sur la page suivante]

(54) **Title:** COUNTER-MEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY ENCRYPTION ALGORITHM

(54) **Titre :** PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE

(57) **Abstract:** The invention concerns a method for efficiently shifting from a boolean data representation to an arithmetic data representation and inversely. Said representations are frequently used in the context of a secret key algorithm which must be protected against differential power analysis. The invention is particularly designed to be used in an electronic portable object such as a smart card.

(57) **Abrégé :** La présente invention concerne une méthode permettant de passer efficacement d'une représentation booléenne des données vers une représentation arithmétique des données et réciproquement. Ces représentations sont fréquemment utilisées dans le cadre d'un algorithme à clef secrète qui doit être protégé contre les attaques par mesure de courant. La présente invention est particulièrement destinée à être utilisée dans un objet portable électronique de type carte à puce.

WO 02/51064 A1

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN ŒUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE

La présente invention concerne un procédé de contre-mesure pour un algorithme de chiffrement à clé secrète.

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé secrète était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé secrète. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

Il existe de nombreux algorithmes à clé secrète dans lesquels l'algorithme effectue des manipulations bits par bits d'une donnée qui dépend du message à chiffrer.

Par exemple, lorsque l'algorithme de chiffrement comprend une permutation de données, l'implémentation sur carte à puce de cette permutation fait intervenir des manipulations bits par bits de la donnée à permuter.

En analysant la consommation de courant lors de l'exécution par le microprocesseur de ces manipulations bits par bits, il est possible de retrouver une partie ou la totalité de la donnée manipulée.

La connaissance de cette donnée fournit des informations sur les résultats intermédiaires de l'exécution de l'algorithme de chiffrement, qui permettent de retrouver la clef secrète de chiffrement.

Dans l'algorithme de chiffrement DES (pour Data Encryption Standard), l'algorithme chiffre un message clair de 64 bits en un message chiffré de 64 bits avec une clé de 64 bits comprenant 8 bits de parité. L'algorithme DES comprend 16 tours.

A chaque tour, l'algorithme DES effectue les manipulations suivantes :

1) Expansion-permutation avec la partie droite de la donnée en entrée. Cette opération fait intervenir des manipulations bits par bits de la donnée.
2) Opération de type OU-EXCLUSIF avec une sous-clé de la clé secrète.
3) Lecture dans la table de type SBOX.
4) Permutation de la donnée. Cette opération fait intervenir des manipulations bits par bits de la donnée.
5) Opération de type OU-EXCLUSIF avec la partie gauche de la donnée en entrée.

L'exécution des opérations 1) et 4) fait intervenir des manipulations de données bits par bits. En enregistrant au préalable la consommation de courant correspondant à une exécution de l'algorithme lorsque ce bit est à 1 et la consommation de courant lorsque ce bit est à 0, il est possible de retrouver la valeur de ce bit en comparant la consommation de courant avec ce qui a été enregistré au préalable.

Il est possible de protéger l'exécution des opérations 1) et 4) faisant intervenir des manipulations de données bits par bits contre des attaques de type DPA.

Pour cela, avant l'exécution d'une opération de type permutation, notée par la suite P, sur une donnée, notée par la suite D, on effectue le tirage d'un nombre aléatoire, noté par la suite U, ayant la même taille que D. On combine D et U par une opération de type OU-EXCLUSIF, pour obtenir une donnée notée H. On effectue l'opération P successivement sur U et sur H, pour obtenir les résultats notés PU et PH respectivement. Le résultat de l 'opération P sur D s'obtient en combinant PU et PH par une opération de type OU-EXCLUSIF.

Ce procédé s'applique aux opérations 1) et 4) décrites précédemment.

Par l'application de ce procédé à une opération de type permutation, les données sur lesquelles on effectue une manipulation bit par bit sont aléatoires. Il n'est alors plus possible de réaliser l'attaque de type DPA décrite précédemment. En effet l'attaque de type DPA décrite précédemment nécessite l'enregistrement préalable de la consommation de courant lorsqu'un bit déterminé de la donnée manipulée est à 1 et de la consommation de courant lorsque ce bit est à 0. Avec le procédé décrit précédemment, cet enregistrement n'est plus possible car les données manipulées U et H sont aléatoires, et sont donc susceptibles de changer lors de chaque nouvelle exécution. De plus les données manipulées U et H ne sont pas connues à l'extérieur de la carte.

Cependant, il arrive dans certains cas qu'un procédé de chiffrement à clef secrète utilise également des opérations arithmétiques de type addition modulo une puissance de deux. Il convient dans ce cas de protéger également ces opérations. Soit D la donnée à protéger. La méthode consiste à ajouter à D un aléa R modulo une puissance de deux. Ainsi, la donnée D+R est aléatoire et l'attaquant ne peut pas obtenir d'information sur D.

Ainsi, il arrive dans certains cas qu'un procédé de chiffrement à clef secrète manipule à la fois des données de la forme D xor R, où xor dénote l'opération de type OU-EXCLUSIF, et des données de la forme D+R, où + dénote l'addition de deux entiers modulo une puissance de deux.

Le procédé de l'invention consiste en une méthode permettant de passer rapidement et de façon sécurisée d'une représentation à l'autre. La représentation D xor R sera appelée par la suite représentation booléenne et la représentation D+R sera appelée représentation arithmétique.

Le premier procédé de l'invention décrit une méthode permettant de passer efficacement d'une représentation booléenne à une représentation arithmétique. On note x la donnée initiale à protéger, et on note x' la donnée protégée. On note K la taille en bits des entiers manipulés. On a ainsi x=x' xor r, où r est un entier aléatoire. Le procédé comporte les étapes suivantes :

1) Pour toutes les valeurs de l'entier y possibles, générer une table T contenant les valeurs :
   $T(y)=(y \text{ xor } r)-r$
2) Mettre dans un entier A la valeur de T(x')

Le procédé décrit précédemment permet d'obtenir une valeur A telle que x=A+r, en utilisant une table T prenant en entrée un entier de K bits et renvoyant en sortie un entier de K bits, la table T étant dite table de K bits vers K bits. On obtient ainsi une représentation arithmétique de l'entier x. Il est impossible pour l'attaquant de déduire du procédé précédent une quelconque information sur l'entier x, car la variable x n'a jamais été manipulée.

Le premier procédé de l'invention comprend une variante permettant de réduire la taille de la table T utilisée. En effet, le premier procédé tel que décrit précédemment nécessite une table de taille K bits vers K bits, lorsque la taille des entiers manipulé est de K bits. La table contient donc 2^K entiers de K bits, ce qui pour des valeurs de K supérieures à 8 rend le procédé impraticable. La variante du premier procédé permet d'effectuer des conversions sur des entiers longs, par exemple, de taille 32 bits, tout en utilisant une table de K bits vers K bits, avec K petit, par exemple K=4.

La variante du premier procédé consiste à effectuer une conversion d'un masquage booléen vers un masquage arithmétique pour des entiers de taille 2.K bits, en utilisant la table T précédente de K bits vers K bits. La variante décrite utilise une autre table dite table de retenue et notée C, prenant en entrée un entier r, qui est initialisée de la façon suivante :

1) Générer un entier aléatoire γ de taille K bits.

2) Pour tous les entiers A de K bits, définir

$C(A)=1+\gamma \mod 2^K$ si $A+r \geq 2^K$

$C(A)=\gamma$ si $A+r < 2^K$

Le procédé de conversion de la variante prend en entrée 2 entiers x' et r' de taille 2.K bits, tels que x=x' xor r', et renvoie en sortie deux entiers A et r'' de taille 2.K bits, tels que $x=A+r'' \mod 2^{(2.K)}$. Le procédé comprend les étapes suivantes :

1) Séparer x' en $x_1' \,||\, x_2'$, où x_1' et x_2' sont des entiers de K bits.

2) Séparer r' en $r_1' \,||\, r_2'$, où r_1' et r_2' sont des entiers de K bits.

3) Remplacer x_1' par x_1' xor r

4) Remplacer x_1' par x_1' xor r_1'

5) Remplacer x_2' par x_2' xor r

6) Remplacer x_2' par x_2' xor r_2'

7) Effectuer $A_1=T(x_1')$ et $A_2=T(x_2')$

8) Remplacer A_1 par $A_1 - C(A_2) \mod 2^K$

9) Effectuer $r_1 = r + \gamma \mod 2^K$

10) Retourner $A= A_1 \,||\, A_2$ et $r'' = r_1 \,||\, r$

La variante de ce premier procédé peut être itérée de façon à effectuer une conversion booléenne vers arithmétique pour des entiers de taille supérieure à 2K bits, en utilisant une table T et une table C de K bits vers K bits.

Le second procédé de l'invention décrit une méthode permettant de passer efficacement d'une représentation arithmétique à une représentation booléenne. On note x la donnée initiale à protéger, et on note A la donnée protégée. On note K la taille en bits des entiers

manipulés. On a ainsi x=A+r, où r est un entier aléatoire. Le procédé comporte les étapes suivantes :

1. Pour toutes les valeurs de l'entier y possible, générer une table T contenant les valeurs :
   T(y)=(y+r) xor r.
2. Mettre dans la variable x' la valeur de T(A).

Le procédé décrit précédemment permet donc d'obtenir une valeur x' telle que x=x' xor r, en utilisant une table T de K bits vers K bits. On obtient ainsi une représentation booléenne de la variable x. Il est impossible pour l'attaquant de déduire du procédé précédent une quelconque information sur l'entier x, car la variable x n'a jamais été manipulée.

Le second procédé de l'invention comprend une variante permettant de réduire la taille de la table T utilisée. En effet, le second procédé tel que décrit précédemment nécessite une table de taille K bits vers K bits, lorsque la taille des entiers manipulés est de K bits. La table contient donc 2^K entiers de K bits, ce qui pour des valeurs de K supérieures à 8 rend le procédé impraticable. La variante du second procédé permet d'effectuer des conversions sur des entiers longs, par exemple, de taille 32 bits, tout en utilisant une table de K bits vers K bits, avec K petit, par exemple K=4.

La variante du second procédé consiste à effectuer une conversion d'un masquage arithmétique vers un masquage booléen pour des entiers de taille 2.K bits, en utilisant la table T précédente de K bits vers K bits. La variante du second procédé utilise également la table C définie dans la variante du premier procédé.

Le procédé de conversion de la variante prend en entrée deux entiers A et r' de taille 2.K bits tels que x=A+ r' mod 2^(2.K) et renvoie en sortie deux entiers x' et r'' de taille 2.K bits, tels que x=x' xor r''. Le procédé comprend les étapes suivantes :

1) Générer un aléa a de taille K bits.
2) Soit G=a||r
3) Remplacer A par A-G mod 2^(2.K)
4) Remplacer A par A+r'mod 2^(2.K)
5) Séparer A en A_1 ||A_2 avec A_1 et A_2 de taille K bits.
6) Remplacer A_1 par A_1 + C(A_2) mod 2^K
7) Remplacer a par a - γ mod 2^K
8) Remplacer A_1 par A_1 - r mod 2^K
9) Remplacer A_1 par A_1 + a mod 2^K
10) Effectuer $x'_1=T(A_1)$ et $x'_2=T(A_2)$
11) Remplacer x_1' par x_1' xor γ
12) Remplacer x_1' par x_1' xor r
13) Retourner $x'= x_1' || x_2'$ et $r''=\gamma||r$

La variante de ce second procédé peut être itérée de façon à effectuer une conversion arithmétique vers booléen pour des entiers de taille supérieure à 2K bits, en utilisant une table T et une table C de K bits vers K bits.

Ainsi, ces deux procédés ainsi que leur variante respective permettent de passer efficacement et de manière sécurisée d'une représentation booléenne vers une représentation arithmétique et réciproquement. Ces deux procédés sont particulièrement destinés à être utilisés dans un objet portable électronique de type carte à puce.

REVENDICATIONS

1. Procédé de contre-mesure utilisant contre des attaques de type DPA une représentation arithmétique et une représentation booléenne consistant à empêcher l'enregistrement préalable de la consommation du courant générée par des manipulations de bits par bits en permettant de passer efficacement de ladite représentation booléenne des données, ladite représentation étant notée D xor R, xor désignant l'opération de OU-EXCLUSIF, vers ladite représentation arithmétique des données, ladite représentation étant notée D+R, ledit procédé utilisant une donnée x à protéger, la donnée protégée étant notée x' avec x=x' xor r, l'entier r étant un entier aléatoire, ledit procédé permettant d'obtenir une valeur A telle que x=A+r, ledit procédé étant caractérisé en ce qu'il comporte les 2 étapes suivantes :

   1)1 Pour toutes les valeurs de l'entier y possibles, générer une table T contenant les valeurs : T(y)=(y xor r)-r

   1)2 Mettre dans l'entier A la valeur de T(x')

2. Procédé de contre-mesure contre des attaques de type DPA,utilisant une représentation arithmétique et une représentation booléenne consistant à empêcher l'enregistrement préalable de la consommation de courant générée par des manipulations bits par bits, en permettant de passer efficacement de ladite représentation arithmétique des données, ladite représentation étant notée D+R , vers ladite représentation booléenne des données, ladite représentation étant notée D xor R, xor désignant

l'opération de OU-EXCLUSIF, ledit procédé utilisant une donnée x à protéger, la donnée protégée étant notée A avec x=A+r, l'entier r étant un entier aléatoire, ledit procédé permettant d'obtenir une valeur x' telle que x=x' xor r, ledit procédé étant caractérisé en ce qu'il comporte les 2 étapes suivantes :

2)1 Pour toutes les valeurs de l'entier y possibles, générer une table T contenant les valeurs : T(y)=(y+r) xor r

2)2 Mettre dans la variable x' la valeur de T(A).

3. Procédé de conversion selon la revendication 1 réalisant une conversion d'un masquage booléen vers un masquage arithmétique pour des entiers de taille 2.K bits, utilisant une table T de K bits vers K bits, ledit procédé utilisant une table dite table de retenue notée C, ladite table prenant en entrée un entier r et étant initialisée à l'aide des deux étapes suivantes :

1) Générer un entier aléatoire γ de taille K bits.

2) Pour tous les entiers A de K bits, définir

$C(A)=1+\gamma \mod 2^K$ si $A+r \geq 2^K$

$C(A)=\gamma$ si $A+r < 2^K$

ledit procédé prenant en entrée 2 entiers x' et r' de taille 2.K bits, tels que x=x' xor r', et renvoyant en sortie deux entiers A et r'' de taille 2.K bits, tels que $x=A+r'' \mod 2^{(2.K)}$, caractérisé en ce qu'il comprend les étapes suivantes :

1) Séparer x' en $x_1' \,||\, x_2'$, où x_1' et x_2' sont des entiers de K bits.

2) Séparer r' en r_1' || r_2' , où r_1' et r_2' sont des entiers de K bits.
3) Remplacer x_1' par x_1' xor r
4) Remplacer x_1' par x_1' xor r_1'
5) Remplacer x_2' par x_2' xor r
6) Remplacer x_2' par x_2' xor r_2'
7) Effectuer $A_1=T(x_1')$ et $A_2=T(x_2')$
8) Remplacer $A_1= A_1 - C(A_2) \mod 2^K$
9) Effectuer $r_1 = r + \gamma \mod 2^K$
10) Retourner $A= A_1 || A_2$ et $r'' = r_1 || r$

4. Procédé de conversion selon la revendication 3, caractérisé en ce qu'il est itéré pour effectuer une conversion d'un masquage booléen vers un masquage arithmétique pour des entiers de taille supérieure à 2K bits, en utilisant une table T et une table C de K bits vers K bits.

5. Procédé de conversion suivant les revendication 2 et 3 réalisant une conversion d'un masquage arithmétique vers un masquage booléen pour des entiers de taille 2.K bits, ledit procédé utilisant une table T précédente de K bits vers K bits, ledit procédé utilisant ladite table de retenue C, ledit procédé prenant en entrée deux entiers A et r' de taille 2.K bits tels que $x=A+ r' \mod 2^{(2.K)}$ et renvoyant en sortie deux entiers x' et r'' de taille 2.K bits, tels que x=x' xor r'', caractérisé en ce qu'il comprend les étapes suivantes :

1) Générer un aléa a de taille K bits.
2) Soit G=a||r
3) Remplacer A par $A-G \mod 2^{(2.K)}$
4) Remplacer A par $A+r' \mod 2^{(2.K)}$

5) Séparer A en $A_1 || A_2$ avec A_1 et A_2 de taille K bits.

6) Remplacer A_1 par $A_1 + C(A_2) \bmod 2^K$

7) Remplacer a par $a - \gamma \bmod 2^K$

8) Remplacer A_1 par $A_1 - r \bmod 2^K$

9) Remplacer A_1 par $A_1 + a \bmod 2^K$

10) Effectuer $x'_1 = T(A_1)$ et $x'_2 = T(A_2)$

11) Remplacer x_1' par x_1' xor γ

12) Remplacer x_1' par x_1' xor r

13) Retourner $x' = x_1' || x_2'$ et $r'' = \gamma || r$

6. Procédé de conversion selon la revendication 5, caractérisé en ce qu'il est itéré pour effectuer une conversion d'un masquage arithmétique vers un masquage booléen pour des entiers de taille supérieure à 2K bits, en utilisant une table T et une table C de K bits vers K bits.

7. Procédé de chiffrement à clef secrète, caractérisé en ce qu'il utilise l'une quelconque des revendications précédentes.

8. Procédé suivant l'une quelconque des revendications précédentes, caractérisé en ce qu'il s'applique à un objet électronique portable de type carte à puce.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/03646

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

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)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

WPI Data, EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CORON J -S ET AL: "On Boolean and arithmetic masking against differential power analysis" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2000. SECOND INTERNATIONAL WORKSHOP. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.1965), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2000. SECOND INTERNATIONAL WORKSHOP. PROCEEDINGS, WOR, 17 August 2000 (2000-08-17), pages 231-236, XP000989986 2000, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-41455-X page 234, line 23 -page 235, line 24	1,2

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

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

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 March 2002	21/03/2002

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/03646

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/06

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)
CIB 7 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 réalisable, termes de recherche utilisés)
WPI Data, EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	CORON J -S ET AL: "On Boolean and arithmetic masking against differential power analysis" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2000. SECOND INTERNATIONAL WORKSHOP. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.1965), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2000. SECOND INTERNATIONAL WORKSHOP. PROCEEDINGS, WOR, 17 août 2000 (2000-08-17), pages 231-236, XP000989986 2000, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-41455-X page 234, ligne 23 -page 235, ligne 24 _____	1,2

☐ 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'appartenenant 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'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion 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
12 mars 2002	21/03/2002

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G