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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
11 septembre 2009 (11.09.2009)

PCT

(10) Numéro de publication internationale
WO 2009/109715 A3

(51) Classification internationale des brevets :
G06F 7/72 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2009/000072

(22) Date de dépôt international :
23 janvier 2009 (23.01.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
08 00345 23 janvier 2008 (23.01.2008) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **INSIDE CONTACTLESS** [FR/FR]; 41 Parc Club du Golf, F-13856 Aix en Provence Cedex 3 (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BENTEO, Bruno** [FR/FR]; 11, rue Bernard Mule, F-31400 Toulouse (FR). **FEIX, Benoît** [FR/FR]; Résidence Cyntharista Bât. B., Ave4nue Cytharista, F-13600 La Ciotat (FR). **NEROT, Sebastien** [FR/FR]; Quartier les Nirons, F-13860 Peyrolles en Provence (FR).

(74) Mandataire : **MARCHAND, André**; OMNIPAT, 24 Place des Martyrs de la Résistance, F-13100 Aix en Provence (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

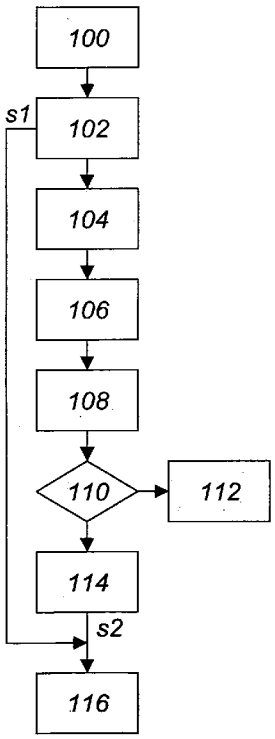
(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) Title : COUNTERMEASURE METHOD AND DEVICES FOR ASYMMETRICAL CRYPTOGRAPHY WITH SIGNATURE DIAGRAM

(54) Titre : PROCEDE ET DISPOSITIFS DE CONTRE-MESURE POUR CRYPTOGRAPHIE ASYMETRIQUE A SCHEMA DE SIGNATURE

Figure 4



(57) Abstract : The invention relates to a method for countermeasures in an electronic component that uses a private-key asymmetrical cryptography algorithm, including the steps of generating (102) a first output data (s1) using a primitive, and (104) a protection parameter. The method further comprises the steps of converting (106), using said protection parameter, at least one of the elements of the set including the private key and an intermediate parameter obtained from the first output data (s1) in order to provide respectively first and second operands, and generating (108, 114) a second output data (s2) from an operation in which the first and second operands are involved.

(57) Abrégé : Ce procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme de cryptographie asymétrique à clé privée, comprend les étapes consistant à générer (102) une première donnée de sortie (s1), à l'aide d'une primitive, et (104) un paramètre de protection. Il comporte en outre les étapes consistant à transformer (106), à l'aide du paramètre de protection, au moins l'un des éléments de l'ensemble constitué de la clé privée et d'un paramètre intermédiaire obtenu à partir de la première donnée de sortie (s1), pour fournir respectivement des premier et second opérandes, et à générer (108, 114), à partir d'une opération impliquant les premier et second opérandes, une seconde donnée de sortie (s2).

WO 2009/109715 A3

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii))*

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

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))*

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

14 janvier 2010

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/000072

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/72

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)
G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 291 763 A (ST MICROELECTRONICS SA [FR]) 12 March 2003 (2003-03-12)	1,3-5,7, 11,12, 14-16, 18,22,23
Y	abstract page 1, paragraph 1 page 4, paragraph 27 - paragraph 30 page 8, paragraph 81 - paragraph 85	2,6,13, 17

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 août 2009	30/11/2009

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	Post, Katharina

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/000072

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CORON J-S: "RESISTANCE AGAINST DIFFERENTIAL POWER ANALYSIS FOR ELLIPTIC CURVE CRYPTOSYSTEMS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONALWORKSHOP, XX, XX, 1 August 1999 (1999-08-01), pages 292-302, XP000952243 abstract page 300, paragraph 5	2,6,13, 17
A	D. NACCACHE ET AL.: "Experimenting with Faults, Lattice and the DSA" PKC '05, LECTURE NOTES IN COMPUTER SCIENCE, vol. 3386, 2005, pages 16-28, XP002495194 Berlin, Germany, ISBN 978-3-540-24454-7 cited in the application the whole document	1-7, 11-18, 22,23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2009/000072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1291763 A	12-03-2003	FR 2829335 A1	07-03-2003
		JP 2003177668 A	27-06-2003
		US 2003044014 A1	06-03-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/000072

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F7/72

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)
G06F

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	EP 1 291 763 A (ST MICROELECTRONICS SA [FR]) 12 mars 2003 (2003-03-12)	1,3-5,7, 11,12, 14-16, 18,22,23
Y	abrégé page 1, alinéa 1 page 4, alinéa 27 - alinéa 30 page 8, alinéa 81 - alinéa 85	2,6,13, 17

-/--

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

[X] 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
20 août 2009	30/11/2009

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	Post, Katharina

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/000072

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	CORON J-S: "RESISTANCE AGAINST DIFFERENTIAL POWER ANALYSIS FOR ELLIPTIC CURVE CRYPTOSYSTEMS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONALWORKSHOP, XX, XX, 1 août 1999 (1999-08-01), pages 292-302, XP000952243 abrégé page 300, alinéa 5	2,6,13, 17
A	D. NACCACHE ET AL.: "Experimenting with Faults, Lattice and the DSA" PKC '05, LECTURE NOTES IN COMPUTER SCIENCE, vol. 3386, 2005, pages 16-28, XP002495194 Berlin, Germany, ISBN 978-3-540-24454-7 cité dans la demande le document en entier	1-7, 11-18, 22,23

Demande internationale n°
PCT/FR2009/000072

RAPPORT DE RECHERCHE INTERNATIONALE

Cadre n°. II Observations – lorsqu'il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (suite du point 2 de la première feuille)

Le rapport de recherche internationale n'a pas été établi en ce qui concerne certaines revendications conformément à l'article 17.2)a) pour les raisons suivantes :

1. ☐ Les revendications n^{os}
se rapportent à un objet à l'égard duquel l'administration chargée de la recherche internationale n'est pas tenue de procéder à la recherche, à savoir :

2. ☐ Les revendications n^{os}
parce qu'elles se rapportent à des parties de la demande internationale qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectueé, en particulier :

3. ☐ Les revendications n^{os}
parce qu'elles sont des revendications dépendantes et ne sont pasrédigées conformément aux dispositions de la deuxième et de la troisième phrases de la règle 6.4.a).

Cadre n°. III Observations – lorsqu'il y a absence d'unité de l'invention (suite du point 3 de la première feuille)

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la demande internationale, à savoir:

voir feuille supplémentaire

1. ☐ Comme toutes les taxes additionnelles exigées ont été payées dans les délais par le déposant, le présent rapport de recherche internationale porte sur toutes les revendications pouvant faire l'objet d'une recherche.

2. ☐ Comme toutes les revendications qui se prêtent à la recherche ont pu faire l'objet de cette recherche sans effort particulier justifiant des taxes additionnelles, l'administration chargée de la recherche internationale n'a sollicité le paiement d'aucunes taxes de cette nature.

3. ☐ Comme une partie seulement des taxes additionnelles demandées a été payée dans les délais par le déposant, le présent rapport de recherche internationale ne porte que sur les revendications pour lesquelles les taxes ont été payées, à savoir les revendications n^{os}:

4. ☒ Aucunes taxes additionnelles demandées n'ont été payées dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale ne porte que sur l'invention mentionnée en premier lieu dans les revendications; elle est couverte par les revendications n^{os}:
voir feuille additionnelle

Remarque quant à la réserve

☐ Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant et, le cas échéant, du paiement de la taxe de réserve.

☐ Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant mais la taxe de réserve n'a pas été payée dans le délai prescrit dans l'invitation.

☐ Le paiement des taxes additionnelles n'était assorti d'aucune réserve.

SUITE DES RENSEIGNEMENTS INDIQUES SUR PCT/ISA/ 210

L'administration chargée de la recherche internationale a trouvé plusieurs (groupes d') inventions dans la demande internationale, à savoir:

1. revendications: 1-5,7,11-16, 18,22,23

   le procédé cité ci-dessus et le dispositif correspondant dans lesquelles la clé privée est transformée

1.1. revendications: 6, 17

   le procédé cité ci-dessus et le dispositif dans lesquelles un algorithme de cryptographie à schéma de signature de type ECDSA est utilisé

---

2. revendications: 8-10, 19-21

   le procédé cité ci-dessus et le dispositif dans lesquelles la génération du paramètre de protection utilise au moins une fonction génératrice

---

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2009/000072

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1291763 A	12-03-2003	FR 2829335 A1	07-03-2003
		JP 2003177668 A	27-06-2003
		US 2003044014 A1	06-03-2003