(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
22 avril 2010 (22.04.2010)

PCT

(10) Numéro de publication internationale
WO 2010/043679 A1

(51) Classification internationale des brevets :
G06K 19/07 (2006.01) *G06F 21/00* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2009/063497

(22) Date de dépôt international :
15 octobre 2009 (15.10.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0856988 15 octobre 2008 (15.10.2008) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SAGEM DEFENSE SECURITE** [FR/FR]; 27 rue Leblanc, F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **RYCKELYNCK, Laurent** [FR/FR]; Sagem Défense Sécurité, 27 rue Leblanc, F-75015 Paris (FR).

(74) Mandataire : **MAILLET, Alain**; 5 place Newquay, BP 70250, F-35802 Dinard Cedex (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, 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, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Publiée :

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

[Suite sur la page suivante]

(54) **Title** : SECURE COMMUNICATION DEVICE

(54) **Titre** : DISPOSITIF DE COMMUNICATION SECURISE

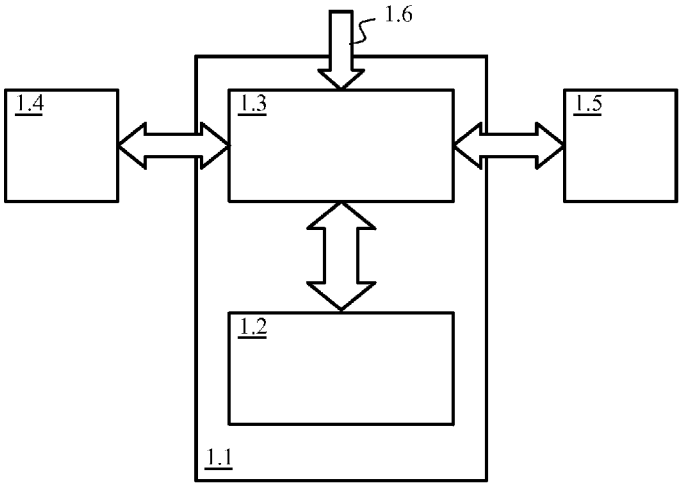

Fig. 1

(57) **Abstract** : The invention relates to a confidence core architecture that is more efficient in terms of design and evaluation than the usual architectures. The confidence core respects the partitioning principle of security recommendations, typically partitioning the red and black domains and the injection of keys. In this approach, the invention proposes the conversion of an existing single-interface component, namely an evaluated smart card component, into a multi-interface component that respects the partitioning principles. The component for carrying out the interface conversion is designed on a minimal, and if possible, an exclusively hardware basis that only implements the flow secure routing.

(57) **Abrégé** :

[Suite sur la page suivante]

WO 2010/043679 A1

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

L'invention propose une architecture de coeur de confiance plus efficace en terme de conception et en terme d'évaluation que les architectures habituelles. Ce coeur de confiance respecte les principes de cloisonnement des recommandations sécuritaires, typiquement le cloisonnement entre les domaines rouge, noir et l'injection des clés. Dans cette approche, l'invention propose de convertir un composant mono-interface existant, nommément un composant de carte à puce évalué, en un composant multi-interface qui respecte les principes de cloisonnement. Le composant réalisant cette conversion d'interface est conçu sur une base minimale et si possible exclusivement matérielle qui ne réalise que le routage sûr des flux.

Dispositif de communication sécurisé

La présente invention concerne la conception d'un composant matériel dédié à la sécurité d'un appareil de communication tel que, par exemple, un téléphone mobile.

On appelle cœur de confiance la portion restreinte d'un équipement sur laquelle reposent les objectifs de sécurité assignés à cet équipement dans la cible de sécurité.

De plus en plus d'appareils permettent d'accéder à des services sécurisés comme, par exemple des services bancaires ou l'accès à des services professionnels sécurisé. Ces appareils doivent être sécurisés et répondre à des normes particulièrement strictes au niveau de la sécurité. Pour pouvoir être utilisés lors des accès à ces services, ces appareils doivent être agréés par une autorité, ils subissent pour ce faire une procédure de certification. Cette procédure de certification permet de vérifier qu'ils répondent bien à un ensemble de critères de sécurité et peuvent donc être utilisés pour faire fonctionner le service sécurisé. Les terminaux de paiement et les cartes à puces bancaires sont des exemples d'appareils soumis à ces certifications de sécurité.

Le cœur de confiance est donc le dispositif implémentant dans l'appareil la communication entre un domaine dit rouge et un domaine dit noir. Ce dispositif est un

dispositif de communication entre deux zones de niveaux de sécurité différents. Par convention, le domaine rouge traite une information intelligible et sensible protégée par son environnement, on parle aussi d'information rouge. Le domaine noir représente l'environnement hostile qui ne protège pas l'information. Dans ce domaine, l'information doit être protégée. Une architecture de confiance ne permet pas de passages directs d'informations du domaine rouge vers le domaine noir et réciproquement.

L'information sensible est ainsi protégée, en confidentialité et/ou en intégrité et/ou en authenticité, par son passage au travers du cœur de confiance dont c'est le rôle. De manière réciproque, l'information protégée provenant du domaine noir est rendue intelligible et/ou vérifiée et/ou authentifiée après être passée par le cœur de confiance.

La certification de sécurité de l'appareil revient à certifier le cœur de confiance. Si celui-ci est conforme aux normes de sécurité, la certification du reste de l'appareil n'est pas nécessaire.

Les mécanismes mis en œuvre pour assurer ces fonctions de chiffrement déchiffrement, signature, vérification de signature, calcul d'intégrité et vérification d'intégrité mettent en œuvre des algorithmes cryptographiques.

La robustesse de la protection offerte par le cœur de confiance est obtenue d'une part par la complexité mathématique des algorithmes cryptographiques qu'il intègre, d'autre part par sa capacité à garder secrets les clés ou éléments secrets utilisés par ces algorithmes cryptographiques.

La Fig. 1 illustre l'architecture d'un cœur de confiance selon l'art antérieur. Le cœur de confiance 1.1 est composé d'un processeur 1.2 qui est chargé d'exécuter le programme de confiance. Ce processeur communique avec un composant dédié 1.3 chargé des opérations cryptographiques et des entrées-sorties avec l'extérieur. Ce composant est typiquement réalisé sous la forme d'un ASIC (*Application-Specific Integrated Circuit* en anglais). Ce composant 1.3 permet la communication avec le domaine rouge 1.4 d'une part et avec le domaine noir 1.5 d'autre part. Un lien de communication 1.6 permet l'injection dans le composant cryptographique des clés nécessaires à son fonctionnement.

La certification d'un tel cœur de confiance nécessite la certification de toutes les fonctionnalités du cœur tant au niveau du processeur et des programmes qu'il

embarque que du composant cryptographique. D'autre part, la conception d'un tel cœur de confiance est un processus long, complexe et coûteux.

L'invention propose une architecture de coeur de confiance plus efficace en terme de conception et en terme d'évaluation que les architectures habituelles. Il s'agit de combiner deux composants de conception et d'évaluation simple pour obtenir un coeur de confiance évaluable simplement. Ce cœur de confiance respecte les principes de cloisonnement des recommandations sécuritaires, typiquement le cloisonnement entre les domaines rouge, noir et l'injection des clés. Dans cette approche, l'invention propose de convertir un composant mono-interface existant, nommément un composant de carte à puce évalué, en un composant multi-interface qui respecte les principes de cloisonnement. Le composant réalisant cette conversion d'interface est conçu sur une base minimale et si possible exclusivement matérielle qui ne réalise que le routage sûr des flux.

L'invention permet de réduire d'un facteur important le coût de conception. En effet, la base du coeur de confiance constituée d'un composant de carte à puce existe et la fonction complémentaire d'aiguillage est réduite au minimum. L'innovation permet de manière induite de réduire aussi d'un facteur important le coût d'une évaluation, le composant de carte à puce étant déjà évalué et le schéma d'évaluation est maîtrisé. Par ailleurs, la fonction aiguillage par sa conception minimaliste est elle aussi évaluable simplement. La combinaison des conceptions et des évaluations est alors plus efficace que la conception et l'évaluation d'un composant monolithique.

L'invention concerne un dispositif de communication sécurisé entre deux zones de niveaux de sécurité différents qui comprend un composant de carte à puce qui garantit la confidentialité de l'information et la mise en œuvre d'algorithmes cryptographiques sans fuite d'informations et un composant d'aiguillage permettant alternativement la communication entre le composant de carte à puce et chacune des deux zones de niveaux de sécurité différents, ainsi que l'introduction de clés cryptographiques dans le composant de carte à puce.

Selon un mode particulier de réalisation de l'invention, le composant d'aiguillage comprend trois voies disposant chacune d'un interrupteur de telle sorte que lorsqu'un des interrupteurs est fermé, les deux autres sont nécessairement ouverts.

Selon un mode particulier de réalisation de l'invention, chacune des voies comprend en outre un module d'adaptation de protocole permettant l'éventuelle

conversion de protocole si besoin entre l'interface extérieure et le composant de carte à puce.

Les caractéristiques de l'invention mentionnées ci-dessus, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un exemple de réalisation, ladite description étant faite en relation avec les dessins joints, parmi lesquels :

La Fig. 1 illustre l'architecture d'un cœur de confiance selon l'art antérieur ;

La Fig. 2 illustre l'architecture d'un cœur de confiance selon l'invention ;

La Fig. 3 illustre l'architecture d'un exemple de composant de carte à puce utilisé dans l'invention ;

La Fig. 4 illustre l'architecture d'un exemple de réalisation du composant d'aiguillage.

La Fig. 2 illustre l'architecture d'un cœur de confiance selon l'invention. Il s'architecture autour d'un composant classique de carte à puce 2.2. Ce composant est un micro contrôleur résistant aux agressions physiques, protégé contre la rétro conception (*reverse engineering* en anglais), contre l'introduction d'erreurs par faisceau de particules. Il garantit la confidentialité de l'information et la mise en œuvre d'algorithmes cryptographiques sans fuite d'informations. Le composant de carte à puce possède déjà les objectifs de sécurité que l'on désire obtenir du cœur de confiance. Un composant de carte à puce, c'est-à-dire le composant physique et le logiciel qu'il embarque, apporte une réponse aux objectifs habituels d'équipements de protection de l'information : conservation sûre d'éléments secrets, chiffrement déchiffrement, contrôle d'accès à la ressource, etc. C'est un bon exemple de ressource sécuritaire périphérique évaluée.

Pour réaliser le cœur de confiance, il faut apporter à ce composant un composant d'aiguillage qui permet de réaliser les chemins de données vers la zone rouge, la zone noire et l'introduction des clés cryptographiques. Ce composant d'aiguillage permet alternativement la communication entre le composant de carte à puce et chacune des deux zones de niveaux de sécurité différents, ainsi que l'introduction de clés cryptographiques dans le composant de carte à puce.

C'est le rôle du composant 2.3. Il permet d'établir un chemin sécurisé et unidirectionnel entre le composant de carte à puce et soit la zone rouge, soit la zone noire ou les clés. Ce composant est conçu de manière à ce qu'à un instant donné un seul de ces chemins puisse être actif.

Le dispositif est conçu de telle sorte que le chemin par lequel les clés sont introduites dans le composant de carte à puce soit unique. Il assure ainsi qu'aucune fuite d'informations ne puisse avoir lieu à la fois pendant l'introduction et pendant la suite de l'utilisation du cœur de confiance.

L'avantage de cette conception est que le composant de carte à puce est déjà certifié. Pour certifier le cœur de confiance selon l'invention, il suffira donc de certifier le composant d'aiguillage 2.3.

La Fig. 3 illustre l'architecture typique d'un composant de carte à puce 2.2 pouvant être utilisé dans l'invention. Branché sur le bus de communication 3.11, on trouve un processeur 3.8. Ce processeur est directement connecté à un circuit d'horloge 3.9 et à un composant de gestion de la remise à zéro (*Reset Logic* en anglais) 3.10, ainsi qu'à un circuit de sécurité 3.1. Un module de gestion des entrées-sorties 3.7 permet la communication avec l'extérieur et en l'occurrence avec le composant d'aiguillage. Un module 3.6 permet la génération de nombres aléatoires utilisés dans les algorithmes cryptographiques. Un module de calcul cryptographique dédié 3.5 assure les fonctions cryptographiques. La mémoire se décompose en un premier module de mémoire E2PROM (*Electrically Erasable Programmable Read-Only Memory* en anglais) 3.4 qui contient les données et le logiciel embarqué, un second module de RAM (*Random Access Memory* en anglais) 3.3 qui contient les données et le programme de manière temporaire pendant son exécution. Un troisième module de mémoire ROM (*Read Only Memory* en anglais) ou FLASH 3.2 qui contient également des logiciels embarqués dédiés carte à puce.

La Fig. 4 illustre l'architecture du composant d'aiguillage 2.3. Ce composant comprend un lien 4.1 servant à communiquer avec le cœur de carte à puce. Ce lien permet la communication avec trois voies d'entrées-sorties 4.2, 4.4 et 4.6 via trois mécanismes d'interrupteurs permettant de fermer ou d'ouvrir chaque voie 4.3, 4.5 et 4.7. Chacune des voies est avantageusement pourvue d'un module d'adaptation 4.8, 4.9 et 4.10 permettant l'éventuelle conversion de protocole si besoin entre l'interface extérieure et le composant de carte à puce.

Les liens sont bidirectionnels, il s'agit typiquement d'interfaces de type série capables d'être converties de manière très simple dans un protocole géré par un composant de carte à puce, le protocole ISO 7816-3.

Le composant est conçu de telle sorte que, quand un interrupteur est passant, les autres sont nécessairement ouverts pour assurer le cloisonnement recherché. Aucune

transmission de données ne peut avoir lieu entre les différentes interfaces 4.2, 4.4 et 4.6 sans transiter par le composant de carte à puce qui assure donc la sécurité du dispositif. Ce composant d'aiguillage est au final le seul composant nécessitant une certification de sécurité qui reste simple du fait de la simplicité de conception de ce composant.

REVENDICATIONS

1/ Dispositif de communication sécurisé entre deux zones de niveaux de sécurité différents caractérisé en ce qu'il comprend :

- une ressource sécuritaire périphérique évaluée, telle qu'un composant de carte à puce, qui garantit la confidentialité de l'information et la mise en œuvre d'algorithmes cryptographiques sans fuite d'informations ;
- un composant d'aiguillage permettant alternativement la communication entre le composant de carte à puce, chacune des deux zones de niveau de sécurité différent et le chemin permettant l'introduction de clés cryptographiques dans le composant de carte à puce.

2/ Dispositif selon la revendication 1, caractérisé en ce que le composant d'aiguillage comprend trois voies disposant chacune d'un interrupteur de telle sorte que lorsqu'un des interrupteurs est fermé, les deux autres sont nécessairement ouverts.

3/ Dispositif selon la revendication 2, caractérisé en ce que chacune des voies comprend en outre un module d'adaptation de protocole permettant l'éventuelle conversion de protocole si besoin entre l'interface extérieure et le composant de carte à puce.

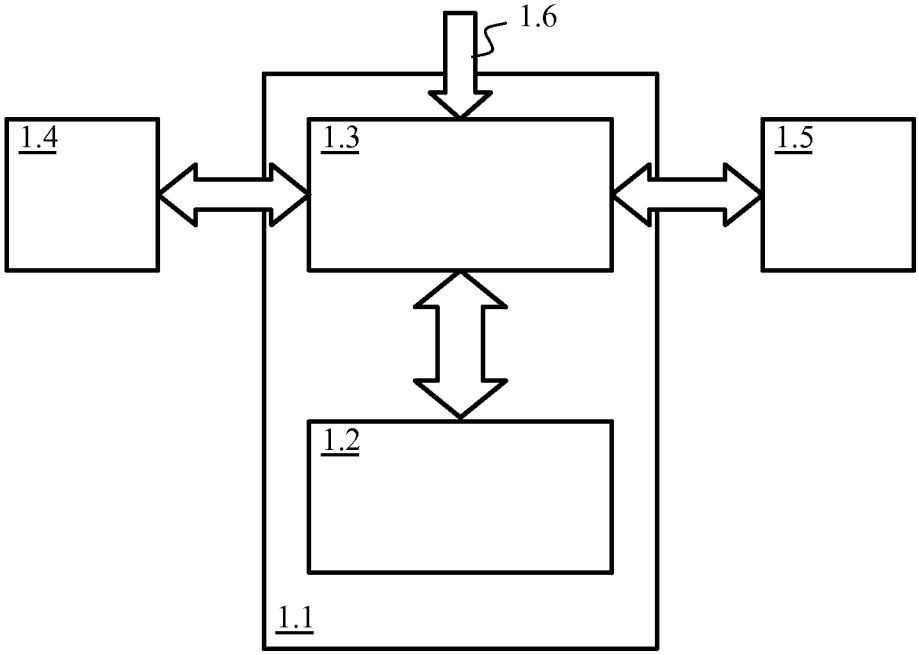

Fig. 1

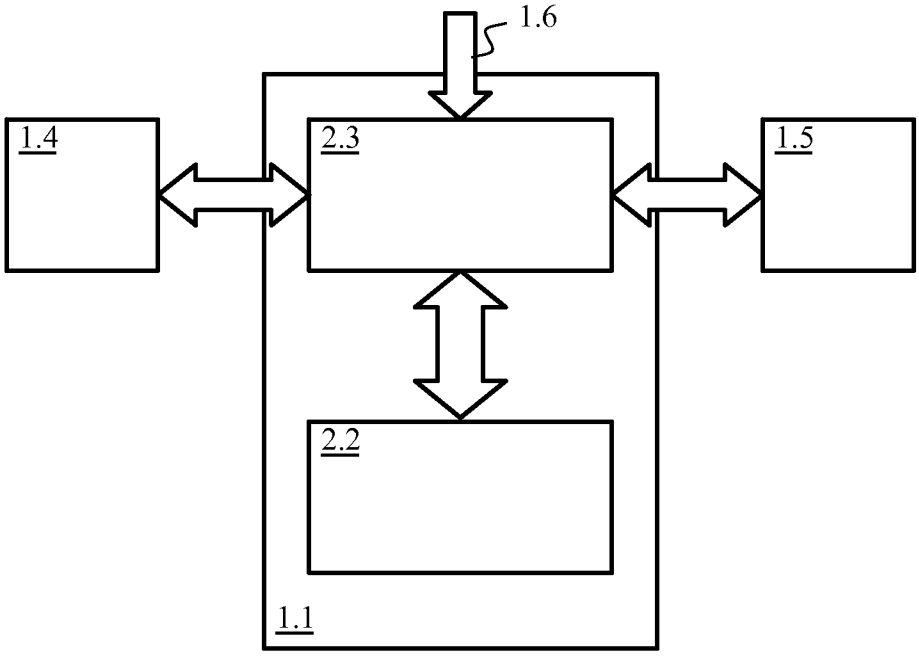

Fig. 2

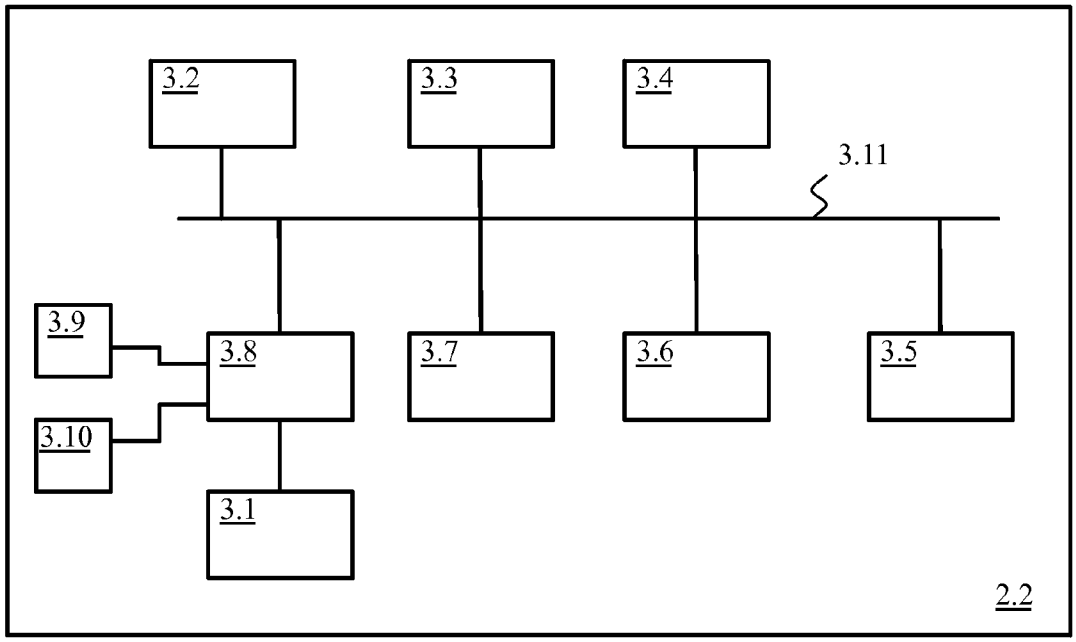

Fig. 3

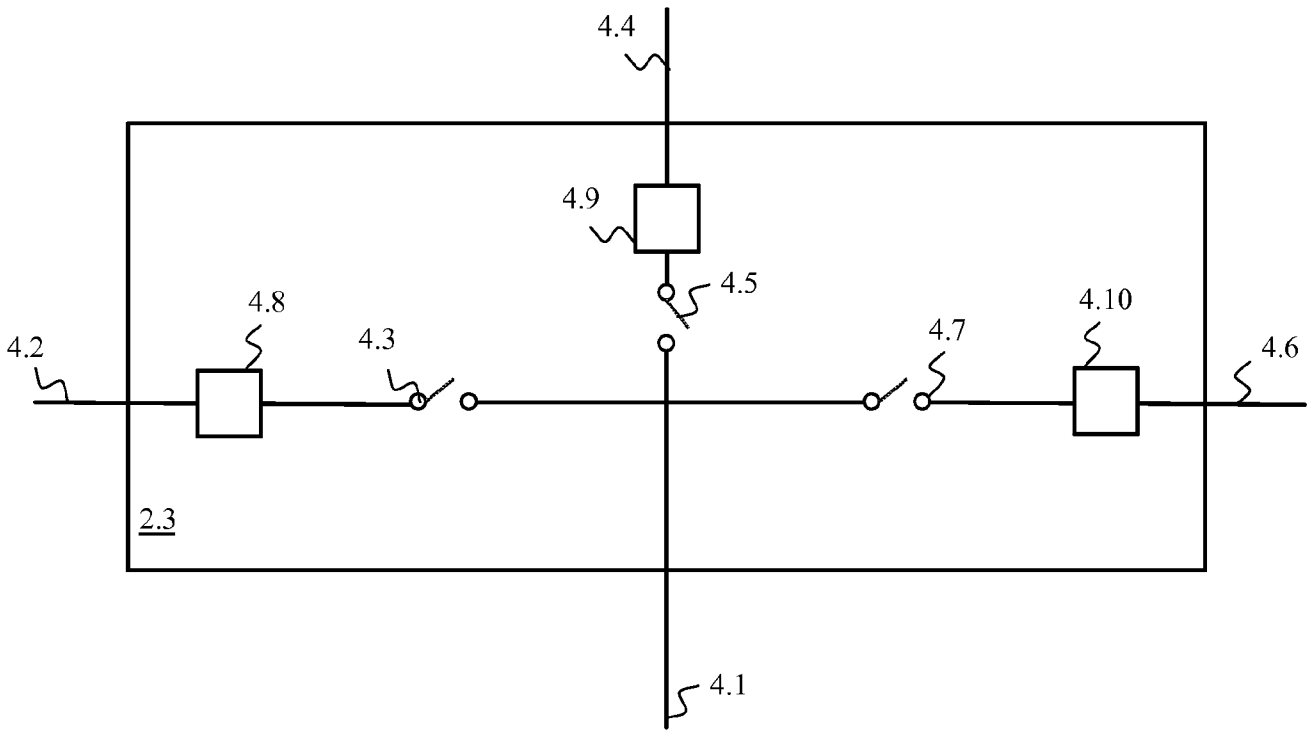

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/063497

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K19/07 G06F21/00

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)
G06K 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 1 258 831 A (MATSUSHITA ELECTRIC IND CO LTD [JP]) 20 November 2002 (2002-11-20) abstract paragraph [0089] - paragraph [0097] paragraph [0133] - paragraph [0139]	1-3
X	EP 1 313 063 A (TOKYO SHIBAURA ELECTRIC CO [JP]) 21 May 2003 (2003-05-21) abstract paragraph [0010]	1-3

☐ 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 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
22 March 2010	31/03/2010

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	Bertolissi, Edy

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/063497

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1258831 A	20-11-2002	DE 60213320 T2	23-08-2007
		US 2002170975 A1	21-11-2002
EP 1313063 A	21-05-2003	JP 2003132313 A	09-05-2003
		US 2003075601 A1	24-04-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2009/063497

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06K19/07 G06F21/00

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)
G06K 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 1 258 831 A (MATSUSHITA ELECTRIC IND CO LTD [JP]) 20 novembre 2002 (2002-11-20) abrégé alinéa [0089] - alinéa [0097] alinéa [0133] - alinéa [0139] -----	1-3
X	EP 1 313 063 A (TOKYO SHIBAURA ELECTRIC CO [JP]) 21 mai 2003 (2003-05-21) abrégé alinéa [0010] -----	1-3

☐ 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
22 mars 2010	31/03/2010

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	Bertolissi, Edy

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2009/063497

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1258831	A	20-11-2002	DE	60213320 T2	23-08-2007
			US	2002170975 A1	21-11-2002
EP 1313063	A	21-05-2003	JP	2003132313 A	09-05-2003
			US	2003075601 A1	24-04-2003