(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 969 787**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **10 61252**

(51) Int Cl[8] : ***G 06 F 21/00*** *(2012.01), G 06 F 9/455*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 24.12.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 29.06.12 Bulletin 12/26.

(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) :** *MORPHO Société anonyme* — FR.

(72) **Inventeur(s) :** BOULET FREDERIC, BARTHE MICHAEL et LE THANH- HA.

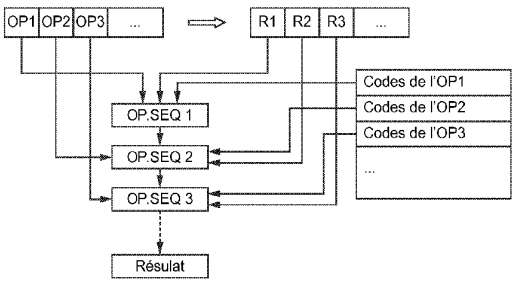
(73) **Titulaire(s) :** MORPHO Société anonyme.

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) PROTECTION DES APPLETS CONTRE LES ANALYSES PAR CANAUX CACHES.

(57) L'invention se rapporte notamment à un dispositif électronique équipé d'une machine virtuelle pour exécuter une applet. La machine virtuelle est agencée pour reconnaître les instructions de l'applet et exécuter un code correspondant à chaque instruction. La machine virtuelle comprend un module d'association agencé pour associer plusieurs codes distincts mais fonctionnellement identiques à une même instruction, et un module de sélection agencé pour sélectionner le code à exécuter pour ladite instruction de manière aléatoire.

L'invention se rapporte également à un procédé de sécurisation de dispositif contre électronique contre les attaques par canaux cachés.



FR 2 969 787 - A1

PROTECTION DES APPLETS CONTRE LES ANALYSES PAR CANAUX CACHES

L'invention concerne des méthodes de protection des applets contre les analyses par canaux cachés ainsi qu'un dispositif mettant en œuvre de telles protections.

On appelle applet tout programme exécuté par une machine virtuelle. Par exemple, un programme rédigé en langage Java-Card et ayant vocation à être exécuté par la JVM d'une carte à puce est appelé applet. On parle, par analogie, d'applet .NET, ou d'applet Multos, pour des programmes développés dans un environnement .NET pour cartes à puces (respectivement un environnement Multos). Les instructions comprises dans une applet sont souvent appelées op-codes, pour «operation code», dans le contexte Java-Card.

Une machine virtuelle est une entité qui est capable d'exécuter une applet enregistrée sous forme d'une succession d'instructions, et qui, lors d'une exécution de l'applet, traduit chaque instruction en une opération élémentaire ou en une séquence d'opérations élémentaires et exécute cette ou ces opération(s) élémentaire(s). Une machine virtuelle permet de dissocier l'interface au moyen de laquelle le programme est enregistré ou transmis, de la plateforme qui réalise les opérations élémentaires. Des exemples de machines virtuelles comprennent notamment les JVM (Java Virtual Machine), ou encore diverses implémentations de la CLI (Common Language Infrastructure) telles que la CLR (Common Language Runtime), pour le langage C# (environnement .NET). Les machines virtuelles sont souvent purement logicielles. Elles permettent alors d'exécuter une même applet sur toutes sortes de plateformes très différentes les unes des autres sous réserve qu'il existe une machine virtuelle adaptée pour chacune de ces plateformes. Mais il est également possible d'utiliser des machines virtuelles matérielles (par exemple un circuit électronique dédié) ou des machines virtuelles associant une partie logicielle et une partie matérielle.

On appelle ingénierie inverse d'une applet une activité qui a pour but de

comprendre la manière dont l'applet a été conçue afin de copier, modifier ou détourner l'applet, le plus souvent sans l'accord de ses auteurs et/ou détenteurs.

Une analyse par canaux cachés est une analyse basée sur des informations obtenues à partir de l'implémentation physique d'un dispositif électronique. Ces informations sont souvent des variations de certaines grandeurs physiques qui sont provoquées par l'exécution d'un programme dans le dispositif électronique. Ces grandeurs physiques (appelées «canaux cachés»), peuvent être, notamment, la consommation électrique du dispositif, ou le champ électromagnétique qui est produit par le dispositif, et peuvent permettre de distinguer les tâches accomplies en fonction de la consommation électrique qu'elles requièrent ou du rayonnement électromagnétique qu'elles occasionnent. On peut aussi mesurer les vibrations émises (certains composants sont susceptibles de vibrer, et ce d'une manière différente selon ce qu'ils font), ou encore les variations de température, ou la durée passée à exécuter une tâche particulière (« timing attacks »), etc.

Une analyse élémentaire peut consister simplement à identifier une caractéristique donnée en fonction d'une mesure donnée sur le dispositif électronique ciblé. C'est le cas par exemple des attaques dites SPA (pour Simple Power Analysis). Des analyses plus sophistiquées peuvent s'appuyer sur des études statistiques sur la base d'un grand nombre de mesures (c'est le cas par exemple des attaques DPA, pour Differential Power Analysis, et plus particulièrement des attaques HODPA, pour High Order DPA).

Dans le contexte de Java-card, on cherche souvent à maintenir secrètes les successions d'instructions comprises dans les applets, afin d'éviter que certaines de ces instructions ne soient modifiées pour détourner l'applet, ou pour changer un résultat produit lors d'une exécution de l'applet.

Cependant, il est parfois possible de retrouver la succession des instructions qui constituent un programme en analysant des canaux cachés, ainsi que c'est expliqué notamment dans Dennis Vermoen, “Reverse engineering of Java Card applets using power analysis”, MSc Thesis, Delft Technology University (performed in Riscure), 2006. Cela implique une

vulnérabilité potentiellement importante des applets Java-card. L'analyse par canaux cachés a été également utilisée par des organisations autorisées (par exemple Information Technology Evaluation Facility – ITSEF) pour évaluer la sécurité des cartes Java, ainsi que c'est expliqué dans Serge Chaumette and Damien Sauveron "An efficient and simple way to test the security of Java Cards", in Proceedings of 3rd International Workshop on Security in Information Systems (WOSIS 2005). Sagem Sécurité est titulaire d'un brevet "Protection d'un programme interprété par une machine virtuelle", numéro FR2903508B1 proposant de masquer les instructions afin de se protéger contre ce type d'analyse.

Pour tenter de découvrir les instructions d'une applet un attaquant peut par exemple procéder en deux étapes.

Dans une étape de caractérisation, l'attaquant charge des applets d'apprentissage sur la carte (pour certaines cartes Java, cette manipulation est en effet autorisée, pour d'autres il peut être nécessaire d'effectuer une première attaque afin de charger les applets d'apprentissage). Les applets d'apprentissage sont codées par l'attaquant d'une manière lui permettant de caractériser les instructions par des modèles correspondants. Un modèle correspond à un signal lié à un canal caché d'une instruction. L'ensemble des modèles forme alors une base de modèles des instructions qui ont été caractérisées.

Dans une étape de détection, l'attaquant mesure le signal issu d'un canal caché pendant l'exécution de l'applet qu'il souhaite découvrir. Ensuite, il utilise la base de modèles construite dans l'étape de caractérisation pour retrouver la séquence d'instructions de l'applet. La détection se base sur la cohérence entre le signal acquis pendant l'étape de détection et les modèles stockés dans la base. L'une des mesures de cohérence les plus simples est la corrélation.

Ainsi, le succès d'une ingénierie inverse par l'analyse de canaux cachés dépend généralement de deux étapes de caractérisation et de détection. En ce qui concerne l'étape de caractérisation, un attaquant peut être confronté notamment à l'une des quatre situations suivantes, illustrées sur la figure 1:

C1 – obtention aisée de modèles corrects,

C2 – obtention difficile de modèles corrects,

C3 – impossibilité d'obtenir des modèles,

C4 – obtention de faux modèles.

La situation C1 correspond par exemple à un cas dans lequel aucune contre-mesure matérielle ni logicielle n'est implémentée, ou seules des contre-mesures élémentaires (peu efficaces) sont implémentées. Un exemple typique de ce type de contre-mesures est l'addition d'un bruit aléatoire sur le canal (par exemple la consommation électrique ou le rayonnement électromagnétique). Cependant, ce bruit aléatoire peut être isolé en exécutant les applets de caractérisation un grand nombre de fois et en moyennant les signaux.

La situation C2 peut se produire notamment si certaines contre-mesures matérielles ou logicielles sont implémentées. La solution utilisant un bruit déterministe proposée dans le brevet FR2903508B1 permet de rendre l'extraction des modèles plus difficile. Les contre-mesures pour désynchroniser les signaux (par exemple: jitter, division d'horloge...) peuvent perturber l'obtention des modèles mais il est souvent possible de les retrouver grâce à des techniques de traitement du signal. La solution selon FR2903508B1 est relativement coûteuse en termes de performance. De plus, si le bruit déterministe n'est pas correctement généré (c'est-à-dire s'il ne conduit pas à des signatures fortement ressemblantes aux signatures naturellement générées lors de l'exécution de l'instruction considérée), un attaquant pourrait parvenir à l'extraire des signaux bruts.

La situation C3 pourrait se présenter en cas de très forte sécurisation, par exemple grâce à des interventions de bas niveau, à un niveau matériel, directement dans un composant exécutant l'applet, ou encore à un niveau logiciel, dans un interpréteur (machine virtuelle exécutant l'applet). Le but de ces interventions est généralement de rendre les modèles soit constant, soit non constant mais identiques, de manière à ce qu'il soit impossible de distinguer une instruction d'une autre. Cependant, en pratique il est très

difficile de garantir une telle propriété, et le cas C3 est relativement théorique.

La situation C4 peut se présenter lorsque que le dispositif attaqué est conçu pour fournir de faux modèles (c'est-à-dire des modèles qui ne correspondent pas aux modèles de l'applet attaquée), lors de la phase d'apprentissage. Selon le brevet FR2903508B1 on peut créer de faux types de bruit, c'est-à-dire générer des types de bruit différents dans les deux étapes de caractérisation et de détection, pour perturber la détection. Cependant, les modèles (cachés derrières le bruit) sont typiquement les mêmes. Si l'attaquant arrive à trouver un moyen pour isoler le bruit additif (par exemple isoler un signal venant du crypto-processeur qui est utilisé comme bruit), il est possible qu'il parvienne à faire une ingénierie inverse de l'applet attaquée par l'analyse de canaux cachés.

On peut généralement considérer que les possibilités C3 et C4 ne peuvent donner lieu à l'étape de détection. Les possibilités C1 et C2 permettent quant à elles, en général, une détection des instructions dans la deuxième étape dans laquelle deux situations peuvent être envisagées:

D1 - modèles facile à détecter pendant l'exécution,

D2 - modèles difficiles à détecter

La situation dans laquelle il serait impossible de détecter les modèles est en général la suite de la situation C3, et n'est donc pas étudiée.

Cinq des scénarios pouvant se produire dans une ingénierie inverse d'applet par l'analyse de canaux cachés sont représentés sur la figure 1 par S1, S2, S3, S4 et S5. La combinaison C2-D1 est typiquement très rare. En effet, s'il est difficile pour l'attaquant de créer des applets de caractérisation pour observer le dispositif cible et déterminer des modèles, il est vraisemblable que la phase de détection ultérieure soit elle aussi difficile compte tenu de l'incertitude pesant sur la qualité des modèles.

Afin de se prémunir contre ces attaques, il est possible de sécuriser le dispositif électronique lui-même. Par exemple, on peut superposer un bruit sur l'alimentation électrique afin de rendre son exploitation plus difficile, lisser la consommation électrique (par exemple avec des condensateurs), limiter les

émissions électromagnétiques par des blindages adéquats, etc. On peut aussi utiliser une horloge interne particulière, ayant pour caractéristique d'avoir une fréquence de fonctionnement variable de manière aléatoire, ce qui rend les mesures difficiles à exploiter (les instructions de l'applet étant alors effectuées à une cadence qui ne cesse de varier, et qui est a priori inconnue de l'attaquant). Il existe également d'autres techniques, consistant par exemple à contrôler l'accès physique et/ou l'accès logique au dispositif électronique. Par exemple, les cartes à puces Java-Card peuvent conditionner l'exécution d'une applet à la présentation correcte d'un code PIN. Ainsi, une personne qui volerait la carte à puce en espérant en extraire des informations, ne pourrait exécuter l'applet ciblée sans présenter le bon code PIN (qu'un utilisateur averti apprend par cœur et ne communique à personne), et ne serait donc pas en mesure d'effectuer l'attaque.

Cependant ces contremesures sont imparfaites.

L'invention vise à améliorer la situation.

Un aspect de l'invention concerne un dispositif électronique équipé d'une machine virtuelle pour exécuter une applet, la machine virtuelle étant agencée pour reconnaître les instructions de l'applet et exécuter un code correspondant à chaque instruction. Le dispositif électronique est, par exemple, une carte à puce (SIM, carte bancaire, carte de santé, etc.), un document d'identité électronique (passeport électronique, carte d'identité électronique, visa électronique, etc.), une clé USB, un token, etc. La machine virtuelle comprend un module d'association agencé pour associer, à une même instruction, plusieurs codes distincts mais fonctionnellement identiques. Ainsi, la machine virtuelle dispose de plusieurs manières d'exécuter une même instruction. Il est possible de protéger plusieurs instructions, chacune d'elles étant associées à plusieurs codes distincts mais fonctionnellement identiques. La définition des ensembles de codes à associer à chaque instruction peut être effectuée en amont (par exemple lors de la conception du dispositif), et le module d'association peut alors se contenter de mémoriser la liste de codes prédéfinis

associés à chaque instruction concernée. La machine virtuelle comprend également un module de sélection agencé pour sélectionner le code à exécuter pour l'instruction considérée de manière aléatoire. Par aléatoire, on entend qu'il n'est pas possible, pour une entité extérieure au dispositif, de déduire facilement des propriétés déterministes qui permettraient de prédire les sélections futures en fonction des sélections passées. La sélection peut s'opérer par exemple grâce à un générateur dit « pseudo aléatoire », tel qu'un générateur congruentiel linéaire, qui peut être logiciel ou matériel. La série de nombres aléatoires générés par un tel générateur est déterministe, mais de période longue, et s'appuie sur un secret qui n'est pas partagé avec l'extérieur. Le module d'association et le module de sélection sont, par exemple, des modules logiciels exécutés par un processeur du dispositif, ou des modules en logique câblée (par exemple pour une machine virtuelle réalisée à l'aide d'un composant électronique dédié).

Ainsi, des exécutions successives d'une même applet faisant appel à une instruction associée à plusieurs codes donnent lieu à des observations différentes, et rendent très difficile de déduire de ces observations ce qui se passe réellement dans l'applet. Cette protection est avantageuse, car l'une des caractéristiques couramment mises en avant des dispositifs mettant en œuvre des interpréteurs (par exemple des cartes à puce java) est leur caractère ouvert, et donc la possibilité pour un tiers de charger des applets. Un utilisateur malhonnête du dispositif pourrait chercher à tirer partie de cette ouverture pour charger des applets d'apprentissage et tenter d'attaquer le dispositif.

Selon un mode de réalisation, les différents codes associés à l'instruction se distinguent par leur durée d'exécution par le dispositif. Ainsi, la durée d'exécution d'une applet fluctue de manière imprévisible, non seulement de façon globale (durée totale d'exécution de l'applet) mais également au niveau de chaque instruction associée à plusieurs codes.

Selon un mode de réalisation, les différents codes associés à ladite instruction se distinguent par la consommation électrique ou par le rayonnement électromagnétique qu'ils génèrent lors de leur exécution par le dispositif. Ainsi, des mesures de rayonnement électromagnétique ou de

consommation électrique lors de l'exécution d'une applet ne permettent pas de déduire aisément ce que l'applet est en train de faire, la signature électromagnétique (ou de consommation) étant variable pour chaque instruction associée à plusieurs codes.

Selon un mode de réalisation, la machine virtuelle est agencée pour opérer la sélection aléatoire du code à exécuter pour chaque instruction associée à plusieurs codes en s'appuyant sur une mesure de caractéristique physique du dispositif. Par exemple, il est possible de mesurer, à l'aide d'un convertisseur analogique-numérique, le bruit d'une résistance, qui a propriétés physiques stochastiques. La ou les mesures physiques peuvent être utilisées directement, ou être utilisées comme graines d'un générateur pseudo aléatoire logiciel, ou être post traitées (par exemple à l'aide d'un crypto-processeur) afin d'améliorer leurs propriétés statistiques. S'appuyer sur une caractéristique physique permet d'augmenter la qualité (le caractère imprévisible) de la sélection.

Selon un mode de réalisation, deux instructions étant associées chacune à plusieurs codes, l'un au moins des codes associés à la première instruction possède au moins une caractéristique commune avec l'un des codes associés à la deuxième instruction, les caractéristiques communes comprenant la durée d'exécution par le dispositif, ainsi que la consommation électrique et le rayonnement électromagnétique générés lors d'une exécution du code par le dispositif. Selon un mode de réalisation, les caractéristiques communes se limitent à l'une ou à plusieurs de ces trois caractéristiques. Ainsi, un attaquant éventuel sera parfois confronté à une situation dans laquelle deux instructions différentes ont pourtant la même signature (c'est-à-dire la même durée d'exécution, et/ou la même consommation électrique, et/ou les mêmes émissions électromagnétiques), ce qui rend difficile l'identification des instructions. Pour adapter la durée d'exécution, il est possible de se caler sur la durée la plus longue (entre les deux instructions), cependant, il est recommandé de ne pas se contenter d'ajouter une simple boucle d'attente à l'instruction la plus rapide, car une boucle d'attente a une signature électromagnétique a priori différente de celle d'une instruction quelconque. Il

est conseillé, au lieu d'une simple attente, de faire des calculs ou opérations semblables à ceux de l'instruction la plus longue, calcul ou opérations dont les résultats peuvent être ignorés.

Selon un mode de réalisation, la machine virtuelle est agencée pour identifier les instructions les plus fréquentes et pour n'utiliser plusieurs codes que pour lesdites instructions les plus fréquentes. La machine virtuelle peut identifier les instructions les plus fréquentes (pour lesquelles plusieurs codes sont disponibles), par exemple en utilisant une liste pré-stockée d'instructions (cette liste étant définie par exemple lors de la conception du dispositif). On peut ainsi déterminer statistiquement que telle ou telle instruction est plus fréquente. Il est également possible d'analyser le code de l'applet considérée afin d'identifier les instructions les plus fréquentes pour cette applet particulière.

Selon un mode de réalisation, les cinq instructions les plus fréquentes sont les instructions sload, sconst_0, baload, getfield_a_this, sstore, et l'on peut ne modifier que ces cinq instructions, voire un sous ensemble quelconque de ces cinq instructions.

Selon un mode de réalisation, les instructions les plus fréquentes comprennent l'une des instructions parmi les instructions d'addition, de soustraction, de multiplication, de modulo, et de ou exclusif, et l'on ne modifie avantageusement que des instructions appartenant à ce sous ensemble d'instructions (addition, soustraction, multiplication, modulo, et ou exclusif). De telles instructions arithmétiques élémentaires, très courantes, ont une grande probabilité d'apparaître dans n'importe quelle applet, et d'apparaître assez souvent. En se concentrant sur la protection de quelques instructions très fréquentes, on peut minimiser la complexité de mise en œuvre de la protection (en évitant de protéger l'intégralité du jeu d'instructions), tout en s'assurant que la protection sera assez efficace (grâce à la fréquence d'apparition des instructions choisies, qui induit ainsi un attaquant éventuel en erreur, la signature de ces instructions ne cessant de changer).

Selon un mode de réalisation, la machine virtuelle est agencée pour identifier les instructions les plus sensibles et pour n'utiliser plusieurs codes que pour ces instructions les plus sensibles. Ainsi, on protège les opérations

les plus critiques (un attaquant s'intéresse souvent à certaines parties seulement de l'applet). De même que pour l'identification des instructions les plus fréquentes, l'identification des instructions les plus sensibles peut être statique, c'est-à-dire que la liste des instructions les plus sensibles peut être préprogrammée dans la machine virtuelle au moment de la conception de la machine virtuelle et/ou du dispositif qui l'intègre. Selon un mode de réalisation, les instructions les plus sensibles comprennent l'une des instructions parmi les instructions mettant en œuvre des algorithmes cryptographiques ainsi que les instructions de contrôle d'accès (notamment les instructions de vérification de code PIN, ou de mots de passe).

Un autre aspect de l'invention concerne un procédé de sécurisation d'un dispositif électronique contre les attaques par canaux cachés, le dispositif électronique étant équipé d'une machine virtuelle reconnaissant les instructions d'une applet et exécutant un code correspondant à chaque instruction. Une instruction (au moins) étant associée à plusieurs codes distincts mais fonctionnellement identiques, la machine virtuelle sélectionne le code à exécuter pour cette instruction associée à plusieurs codes de manière aléatoire.

Selon un mode de réalisation, les différents codes associés à ladite instruction se distinguent par leur durée d'exécution par le dispositif.

Selon un mode de réalisation, les différents codes associés à ladite instruction se distinguent par la consommation électrique ou par le rayonnement électromagnétique qu'ils génèrent lors de leur exécution par le dispositif.

Selon un mode de réalisation, la machine virtuelle opère la sélection du code à exécuter pour ladite instruction en s'appuyant sur une mesure de caractéristique physique du dispositif. On peut ne pas utiliser directement cette caractéristique physique (bruit électrique dans un composant échantillonné par un convertisseur analogique-numérique, etc.), mais plutôt un paramètre calculé à partir de la caractéristique physique, et qui peut par exemple présenter de meilleures propriétés statistiques.

Selon un mode de réalisation, deux instructions étant associées chacune à plusieurs codes, l'un au moins des codes associés à la première instruction

possède au moins une caractéristique commune avec l'un des codes associés à la deuxième instruction, les caractéristiques communes comprenant la durée d'exécution par le dispositif, ainsi que la consommation électrique et le rayonnement électromagnétique générés lors d'une exécution du code par le dispositif.

Selon un mode de réalisation, la machine virtuelle identifie les instructions les plus fréquentes et n'utilise plusieurs codes que pour lesdites instructions les plus fréquentes.

D'autres aspects, buts et avantages de l'invention apparaîtront à la lecture de la description d'un de ses modes de réalisation.

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

- la figure 1 illustre différents scénarios d'une ingénierie inverse d'applet par analyse de canaux cachés ;
- la figure 2 est un diagramme illustrant une mise en œuvre de protection d'applet réalisée selon un mode de réalisation de l'invention.

Selon un mode de réalisation, la protection d'un programme interprété par une machine virtuelle contre une ingénierie inverse utilisant une analyse par canaux cachés (appelée «side-channel analysis» en anglais) est basée sur l'utilisation de modèles alternatifs permettant de rendre les phases de caractérisation et de détection plus difficiles.

Une instruction (op-code) peut ainsi correspondre à plusieurs codes différents, donc à plusieurs modèles différents.

De plus, un même modèle peut correspondre à plusieurs instructions différentes. Par exemple, une opération d'addition (ADD) est généralement très proche de l'opération de soustraction (SUB). Il est possible de coder l'ADD et le SUB de telle manière que leurs signatures soient identiques ou très proches. Par exemple, on peut envisager de mettre en œuvre l'addition ADD, qui prend en paramètres deux opérandes Op1 et Op2, de la manière suivante :

```
Lecture Op1
Lecture Op2
X = Complément Op2
Calcul Op1+Op2
Ecriture Résultat en mémoire
```

On voit ici que l'on calcule le complément du deuxième paramètre de l'opération, mais que le résultat de ce calcul n'est pas utilisé. On peut mettre en œuvre l'opération SUB correspondante de la manière suivante :

```
Lecture Op1
Lecture Op2
X = Complément Op2
Calcul Op1+X
Ecriture Résultat en mémoire
```

On constate que cette opération SUB effectue exactement les mêmes étapes que l'opération ADD, sauf qu'elle utilise comme paramètre, à la ligne 4, le complément X au lieu du paramètre Op2. Cependant, ceci ne s'observe typiquement pas sur les émissions électromagnétiques ou autres générées par l'exécution des opérations ADD et SUB, car seule change l'adresse utilisée, (l'adresse de X n'étant pas l'adresse d'Op2). Or lire une donnée à une première adresse ou à une autre adresse d'un même composant mémoire génère en principe les mêmes traces. On aboutit à une opération ADD qui peut être légèrement plus lente qu'une opération ADD conventionnelle puisqu'elle calcule un complément X apparemment inutile (qui n'est pas utilisé ultérieurement), mais en revanche le fait que ce complément soit calculé permet d'obtenir la même signature que pour l'opération SUB. Selon un mode de réalisation, le complément est une étape effectuée de façon matérielle en parallèle avec les autres étapes, et ne ralentit pas l'opération ADD.

Il est également possible d'obtenir une même signature pour des opérations assez différentes, par exemple une opération à un opérande (complément, négation, décalage de 1 bit, etc.) et une opération à deux opérandes (addition, multiplication, etc.). On peut notamment lire deux fois d'affilée l'opérande unique afin de simuler la lecture de deux opérandes.

Selon un mode de réalisation, les modèles d'une même instruction sont différents non seulement au niveau de forme (la puissance de consommation, le rayonnement électromagnétique) mais aussi au niveau de durée (le temps d'exécution), par exemple par ajout d'opérations inutiles. Les opérations inutiles peuvent être des opérations NOP. Il est conseillé de ne pas utiliser exclusivement des NOP pour ce type de tâche (prolongation artificielle de la durée d'exécution) car il se pourrait alors qu'un attaquant soit en mesure de repérer les NOPs et de les considérer comme des indicateurs de « bourrage temporel », dont la durée d'exécution doit être déduite pour déterminer la vraie durée d'exécution.

Selon un mode de réalisation, on n'autorise certains modèles que pour les applets stockées dans un certain type de mémoire (par exemple en ROM). La mémoire ROM contient typiquement des applets fortement contrôlées car elles ont nécessairement été « chargées » lors d'une étape de masquage du composant ROM ce qui implique une connaissance de l'applet par les industriels chargés de fabriquer ce composant ROM, qui ont donc l'opportunité de vérifier sont contenu. Pour de nombreux types d'applets (et notamment pour les applets java), il est facile (et connu de l'état de l'art) d'obtenir le code source de l'applet même lorsque l'on ne dispose que de son code binaire (ce qui peut être le cas des industriels ci-dessus).

Selon un mode de réalisation, les modèles ROM ne sont pas valables pour les applets chargées dans des mémoires autres que la ROM, telles que des mémoires EEPROM ou FLASH, ou encore RAM protégée par batterie. Ceci est avantageux, car de telles mémoires (réinscriptibles) sont généralement beaucoup plus accessibles que la mémoire ROM et peuvent notamment être éventuellement manipulées par des attaquants afin d'y stocker des applets de caractérisation choisies (ce qui est impossible ou du moins peut être rendu impossible dans le cas de la mémoire ROM, grâce à un contrôle par les industriels précités et/ou par leurs clients et/ou prescripteurs).

Selon un mode de réalisation, les modèles sont différents selon les zones de mémoire. Par exemple, certains systèmes d'exploitation de dispositifs électroniques partitionnent les mémoires réinscriptibles (telles que l'EEPROM et la FLASH), en définissant au moins :

- une première zone accessible aux tiers pour charger des applets de façon contrôlée selon un premier niveau de protection, et

- une deuxième zone accessible au fabriquant du dispositif, pour charger des correctifs (« patchs », « softmasks », etc.) ou des applets (éventuellement des mises à jour d'applet), la deuxième zone étant généralement contrôlée selon un deuxième niveau de protection (souvent plus élevé que le premier niveau de protection).

Il peut y avoir des zones supplémentaires en plus des deux zones précitées. Le deuxième niveau de protection peut être déterminé et non modifiable, alors que le premier niveau de protection peut être modifiable. Ce premier niveau peut être modifiable par exemple par un opérateur de télécommunications (typiquement dans le cas de dispositif électroniques prenant la forme de cartes SIM), par une institution financière (typiquement dans le cas de cartes bancaires), ou encore par toute entité ayant acheté le dispositif électronique et l'ayant mis à disposition d'un utilisateur final.

Ainsi, en adaptant les modèles utilisés selon les types et/ou les zones de mémoire, il est encore plus difficile pour un attaquant de caractériser les instructions, car les applets de caractérisation éventuellement implémentées par l'attaquant ne sont pas pertinentes pour toutes les applets, et en particulier pour les applets stockées dans certains types de mémoires ou dans certaines zones mémoire réputées plus sensibles et non accessibles à l'attaquant. Ceci peut notamment concerner des applets système, telles que des applets offrant des fonctions d'authentification ou encore des fonctions de partage de justificatifs d'identité (« credentials » en anglais). Les fonctions d'authentification peuvent notamment comprendre une/des authentification(s) biométriques (vérification d'empreintes digitales par technique « match-on-card », vérification d'Iris, etc.), des vérifications de mots de passe, de codes PIN, etc. Les fonctions de partage de justificatifs d'identité peuvent comprendre par exemple des fonctions de partage de code PIN par une applet système permettant d'éviter à toutes les applets utilisateurs de chacune devoir demander un même code PIN à l'utilisateur, ce qui serait nuisible à la convivialité de l'utilisation du dispositif électronique (les utilisateurs sont typiquement agacés de devoir saisir plusieurs fois le même code secret), et

serait même généralement nuisible à la sécurité. En effet chaque nouvelle saisie d'un code PIN peut faire l'objet d'une attaque (ingénierie sociale, par exemple personne observant la saisie du code PIN et le mémorisant, ou encore système d'espionnage de type « key logger » à savoir intercepteur de frappes clavier). De plus chaque nouvelle transmission d'un code PIN au dispositif électronique peut potentiellement faire l'objet d'une attaque.

Les modèles d'une même instruction sont activés alternativement suivant certaines règles définies pour la cible d'application. Par exemple, tous les modèles peuvent être activés d'une manière aléatoire, la règle pour une applet pouvant être déterminée selon le mécanisme défini dans la demande de brevet FR2903508 ("Protection d'un programme interprété par une machine virtuelle", déposée le 10 juillet 2006), c'est-à-dire qu'il est possible de prendre en compte un condensé de l'applet (par exemple le résultat d'une fonction SHA-1 appliquée au code binaire de l'applet), de façon faire varier les modèles de façon différente pour une même instruction selon qu'elle appartient à une applet ou à une autre.

Les modèles alternatifs peuvent être appliqués sur toutes les instructions ou un ensemble des instructions les plus critiques et/ou les plus appelées. On peut notamment cibler, par exemple, les instructions accédant à des mémoires de type NVRAM ou EEPROM, qui, étant fortement consommatrices d'électricité, sont souvent plus facilement détectables par analyse de consommation.

Selon un mode de réalisation, les effets engendrés par cette contre-mesure sont les suivants.

Dans le cas où un attaquant peut caractériser les modèles facilement avec des signaux bruts (cette situation peut arriver si le composant fuit beaucoup et qu'aucun bruit n'est ajouté, ou si le bruit est ajouté mais qu'il est facilement filtrable), l'utilisation des modèles alternatifs permet d'augmenter le nombre de modèles à déterminer par l'attaquant dans la phase de caractérisation et le nombre de candidats à identifier ('match' en anglais) dans la phase de détection. Par conséquent, la détection de modèles est rendue plus difficile.

Ainsi, on rend plus compliquée l'extraction de bruit que des attaquants peuvent tenter de mettre en œuvre afin de retrouver les modèles liés aux instructions.

Un attaquant pourrait être au courant de l'existence de modèles différents mis en œuvre par le dispositif électronique cible pour de mêmes instructions (selon le contexte dans lequel l'instruction est exécutée par le dispositif). Un tel attaquant peut alors chercher à prendre en compte cette caractéristique en tentant de déterminer la (ou les) règle(s) qui est (sont) utilisée(s) par le dispositif électronique cible pour choisir un modèle plutôt qu'un autre. Dans le cas où un attaquant ne peut pas caractériser les modèles avec des signaux bruts et où il est obligé d'enregistrer de nombreuses occurrences des signaux puis de moyenner ces signaux pour réduire le bruit :

- Si la (les) règle(s) de l'applet d'apprentissage utilisée par l'attaquant pour déterminer des modèles et la (les) règle(s) utilisée(s) par un dispositif électronique mettant en œuvre l'applet à attaquer ne sont pas identiques, les modèles d'une même instruction obtenus pendant deux phases distinctes sont typiquement différents. Par conséquent, les modèles obtenus pendant la phase de caractérisation ne peuvent pas être utilisés (car ils sont a priori faux) pour retrouver avec succès les instructions de l'applet à attaquer. L'attaque en devient donc bien plus difficile.
- Si la ou les règles sont identiques pour l'applet d'apprentissage et l'applet à attaquer, mais si les différents codes utilisés pour chaque instruction sont déterminés d'une manière telle que les modèles associés à ces codes n'ont pas une durée identique et ne sont pas appelés au même moment, alors on peut s'attendre à ce que la contremesure selon ce mode de réalisation génère une gigue et engendre des désynchronisations. En moyennant les signaux, les modèles moyennés d'une même instruction dans les deux étapes (caractérisation et détection) ne sont donc pas identiques. Par conséquent, la détection devient plus difficile.

Selon un mode de réalisation, on ne protège que quelques instructions (les plus fréquentes, c'est-à-dire qui sont statistiquement appelées fréquemment par les applets) ce qui permet d'avoir un faible impact de performance (de l'ordre de quelques pour cents, c'est-à-dire que la rapidité d'exécution de l'applet peut être quasiment inchangée). Ainsi, le simple fait de ne changer qu'une seule instruction très fréquente (par exemple l'addition) en lui associant par exemple quatre codes possibles au lieu d'un seul, peut suffire à rendre une attaque beaucoup plus complexe, tout en ayant un impact très négligeable aussi bien sur le temps de développement (au stade de la conception de l'interpréteur, du dispositif, des applets, etc.) que sur les performances (l'applet sécurisée étant presque aussi rapide qu'une applet non protégée selon ce mode de réalisation).

Selon un mode de réalisation, les instructions les plus fréquentes sont : sload, sconst_0, baload, getfield_a_this, sstore, et c'est un sous ensemble de ces instructions (voire toutes ces instructions) que l'on protège.

Les interpréteurs (par exemple de type JCVM pour JavaCard Virtual Machine) sont souvent des logiciels développés en langage C. Il est alors possible de modifier l'interpréteur dans ce langage, qui présente l'avantage d'une grande portabilité (il peut facilement être adapté d'un dispositif à un autre, qui possèderait par exemple un processeur de type différent).

Un mode de réalisation se limitant à protéger des instructions fréquentes est particulièrement avantageux, en particulier pour les produits ayant de fortes contraintes affectant les performances, telles qu'une faible capacité mémoire, un processeur lent, etc. Par exemple, les cartes à puces disposent de ressource de calcul et de stockage bien plus faibles que celles d'un ordinateur conventionnel, et ce mode de réalisation leur est particulièrement adapté.

Ne cibler que certaines instructions permet aussi d'éviter un long temps de développement et une taille importante de l'interpréteur. De plus, en faisant générer de la gigue par les instructions associées à différents codes (en utilisant des codes de durées d'exécution différentes), on perturbe également la génération et la détection des modèles des autres instructions qui n'ont qu'un seul modèle.

La figure 2 concerne une mise en œuvre de protection d'applet selon un mode de réalisation. Sur la figure 2, OPi désigne l'instruction numéro i (ayant pour op-code OPi). Ri désigne une règle de cet applet correspondant à l'instruction OPi. La règle Ri peut par exemple définir l'algorithme de sélection du code à exécuter pour l'instruction OPi. Il peut s'agir d'un algorithme pseudo aléatoire conventionnel, mais il peut également s'agir d'un algorithme qui, bien qu'aléatoire au sens où il n'est pas facilement prévisible, sélectionne les différents codes avec des probabilités inégales. OP.SEQi désigne l'étape d'exécution d'une instruction OPi dans la séquence d'instructions que constitue l'applet. Le code exécuté lors de OP.SEQi n'est pas toujours le même, il dépend d'une part de l'instruction OPi qui détermine la fonction qui doit être réalisée par le code, et par la règle Ri, qui détermine quel code (parmi tous les codes réalisant cette fonction) doit être exécuté.

Ainsi, une machine virtuelle selon le mode de réalisation représenté sur la figure 2 génère, à partir d'une applet représentée par une série d'instructions (OP1, OP2, OP3, ...), à partir d'une série de règles (R1, R2, R3, ...), et à partir d'une série d'ensembles de codes (Codes de l'OP1, Codes de l'OP2, Codes de l'OP3, ...), chaque ensemble de codes étant associé à une instruction, une séquence d'exécution (OP.SEQ1, OP.SEQ2, OP.SEQ3, ...) effectuant les tâches prévues dans l'applet, mais faisant appel à des codes choisis aléatoirement.

Bien entendu, la présente invention ne se limite pas à la forme de réalisation décrite ci-avant à titre d'exemple ; elle s'étend à d'autres variantes.

Ainsi, il a été décrit ci-avant un dispositif pouvant être une carte à puce. Cependant le dispositif mettant en œuvre l'invention peut également être, par exemple, un équipement mobile de communication, une étiquette d'identification sans contact, un lecteur d'étiquette d'identification sans contact, une carte à puce, un lecteur de telles cartes à puces, un système de contrôle d'accès, etc. Des types de cartes à puce pour lesquelles l'invention peut être avantageusement mise en œuvre peuvent être notamment des cartes à puces de santé, des cartes à puces d'identité ou de passeport, des cartes à puces

bancaires, des cartes à puces de contrôle d'accès ou des cartes à puces supports de jeux électroniques.

Les applets protégeables ne se limitent pas aux applets JavaCard, mais peuvent être par exemple des applets .NET, ou encore des applets Multos.

5

REVENDICATIONS

1. Dispositif électronique équipé d'une machine virtuelle pour exécuter une applet, la machine virtuelle étant agencée pour reconnaître les instructions de l'applet et exécuter un code correspondant à chaque instruction, caractérisé en ce que la machine virtuelle comprend un module d'association agencé pour associer plusieurs codes distincts mais fonctionnellement identiques à une même instruction, et un module de sélection agencé pour sélectionner le code à exécuter pour ladite instruction de manière aléatoire.

2. Dispositif selon la revendication 1, dans lequel les différents codes associés à ladite instruction se distinguent par leur durée d'exécution par le dispositif.

3. Dispositif selon la revendication 1 ou 2, dans lequel les différents codes associés à ladite instruction se distinguent par la consommation électrique ou par le rayonnement électromagnétique qu'ils génèrent lors de leur exécution par le dispositif.

4. Dispositif selon l'une des revendications précédentes, dans lequel la machine virtuelle est agencée pour opérer la sélection aléatoire du code à exécuter pour ladite instruction en s'appuyant sur une mesure de caractéristique physique du dispositif.

5. Dispositif selon l'une des revendications précédentes, dans lequel, deux instructions étant associées chacune à plusieurs codes, l'un au moins des codes associés à la première instruction possède au moins une caractéristique commune avec l'un des codes associés à la deuxième instruction, les caractéristiques communes possibles étant la durée d'exécution du code par le dispositif, ainsi que la consommation électrique et le rayonnement électromagnétique générés lors d'une exécution du code par le dispositif.

6. Dispositif selon l'une des revendications précédentes, dans lequel la machine virtuelle est agencée pour identifier les instructions les plus fréquentes et pour n'utiliser plusieurs codes que pour lesdites instructions les plus fréquentes.

7. Dispositif selon la revendication 6, dans lequel les instructions les plus fréquentes comprennent l'une des instructions parmi les instructions d'addition, de soustraction, de multiplication, de modulo, et de ou exclusif.

8. Dispositif selon l'une des revendications 1 à 5, dans lequel la machine virtuelle est agencée pour identifier les instructions les plus sensibles et pour n'utiliser plusieurs codes que pour lesdites instructions les plus sensibles.

9. Dispositif selon la revendication 8, dans lequel les instructions les plus sensibles comprennent l'une des instructions parmi les instructions mettant en œuvre des algorithmes cryptographiques ainsi que les instructions de contrôle d'accès.

10. Procédé de sécurisation d'un dispositif électronique contre les attaques par canaux cachés, le dispositif électronique étant équipé d'une machine virtuelle reconnaissant les instructions d'une applet et exécutant un code correspondant à chaque instruction, caractérisé en ce que, une instruction étant associée à plusieurs codes distincts mais fonctionnellement identiques, la machine virtuelle sélectionne le code à exécuter pour ladite instruction de manière aléatoire.

11. Procédé selon la revendication 10, dans lequel les différents codes associés à ladite instruction se distinguent par leur durée d'exécution par le dispositif.

12. Procédé selon la revendication 10 ou 11, dans lequel les différents codes associés à ladite instruction se distinguent par la consommation électrique ou par le rayonnement électromagnétique qu'ils génèrent lors de leur exécution par le dispositif.

13. Procédé selon l'une des revendications 10 à 12, dans lequel la machine virtuelle opère la sélection du code à exécuter pour ladite instruction en s'appuyant sur une mesure de caractéristique physique du dispositif.

14. Procédé selon l'une des revendications 10 à 13, dans lequel, deux instructions étant associées chacune à plusieurs codes, l'un au moins des codes associés à la première instruction possède au moins une caractéristique commune avec l'un des codes associés à la deuxième instruction, les caractéristiques communes possibles étant la durée d'exécution du code par le

dispositif, ainsi que la consommation électrique et le rayonnement électromagnétique générés lors d'une exécution du code par le dispositif.

15. Procédé selon l'une des revendications 10 à 14, dans lequel la machine virtuelle identifie les instructions les plus fréquentes et n'utilise plusieurs codes que pour lesdites instructions les plus fréquentes.

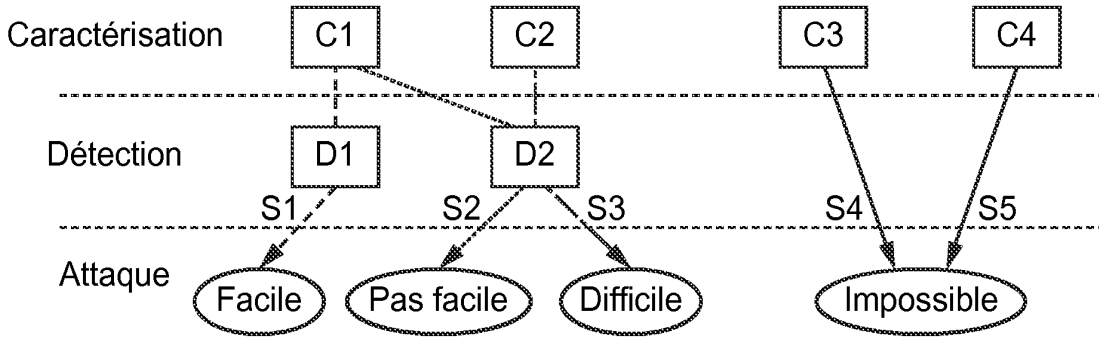

Caractérisation
C1
C2
C3
C4
Détection
D1
D2
S1
S2
S3
S4
S5
Attaque
Facile
Pas facile
Difficile
Impossible

FIG. 1

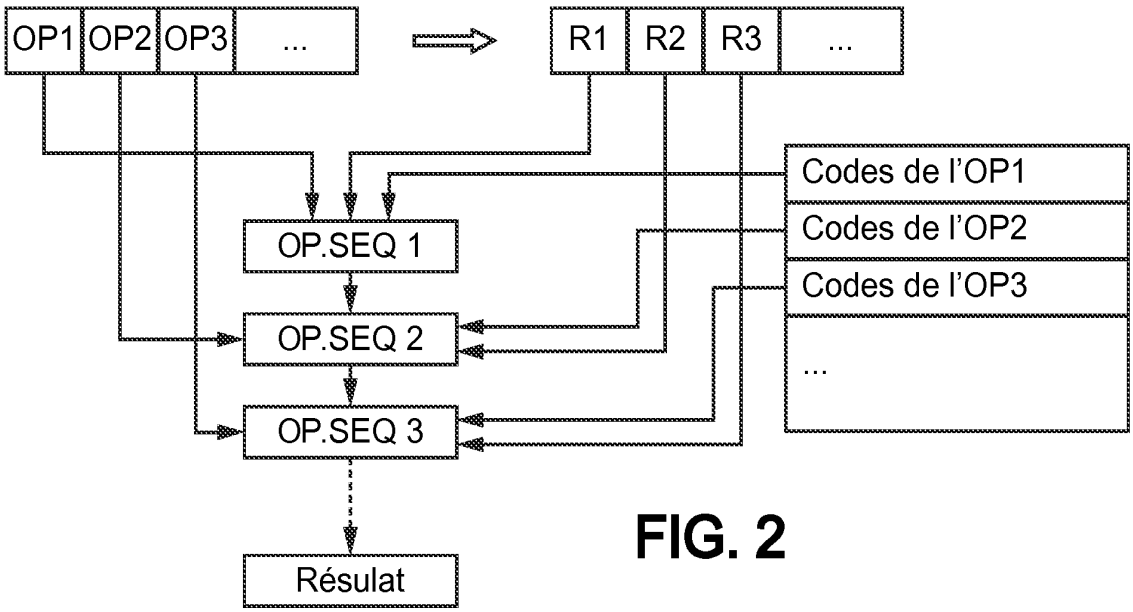

OP1
OP2
OP3
...
R1
R2
R3
...
Codes de l'OP1
Codes de l'OP2
Codes de l'OP3
...
OP.SEQ 1
OP.SEQ 2
OP.SEQ 3
Résulat

FIG. 2

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 750419
FR 1061252

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		
X	WO 02/50641 A1 (CP8 TECHNOLOGIES [FR]; GIRAUD NICOLAS [FR]; BROLH ABRAHAM [FR]; HAMEAU) 27 juin 2002 (2002-06-27) * page 1, ligne 7 - ligne 12 * * page 2, ligne 25 - ligne 36 * * page 3, ligne 8 - ligne 12 * * page 8, ligne 22 - page 9, ligne 34 * * page 11, ligne 1 - page 12, ligne 7 * * page 14, ligne 8 - ligne 12 * * figure 2 * -----	1-15	G06F21/00 G06F9/455

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

G06F

Date d'achèvement de la recherche	Examinateur
26 juillet 2011	Arbutina, Ljiljana

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)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1061252 FA 750419

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 26-07-2011
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0250641 A1	27-06-2002	AU 2811602 A	01-07-2002
		CN 1488091 A	07-04-2004
		EP 1346271 A1	24-09-2003
		FR 2818772 A1	28-06-2002
		MX PA03005710 A	12-11-2004

EPO FORM P0465

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

OPINION ÉCRITE SUR LA BREVETABILITÉ DE L'INVENTION

FA750419	Date de dépôt *(jour/mois/année)* 24.12.2010	Date de priorité *(jour/mois/année)*	N° d'enregistrement national FR1061252
Classification internationale des brevets (CIB) G06F21/00 G06F9/455			
Déposant MORPHO			

La présente opinion contient des indications et les pages correspondantes relatives aux points suivants :

- ☒ Point I — Base de l'opinion
- ☐ Point II — Priorité
- ☐ Point III — Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- ☐ Point IV — Absence d'unité de l'invention (Article L. 612-4 du Code de la Propriété Intellectuelle)
- ☒ Point V — Opinion motivée (Article R. 612-57 du Code de la Propriété Intellectuelle) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- ☐ Point VI — Certains documents cités
- ☐ Point VII — Irrégularités dans la demande
- ☐ Point VIII — Observations relatives à la demande

	Examinateur Arbutina, Ljiljana

OPINION ÉCRITE

N° d'enregistrement national

FR1061252

Point I Base de l'opinion

Cette opinion a été établie sur la base des dernières revendications déposées avant le commencement de la recherche.

Point V Opinion motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-15
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-15
Possibilité d'application industrielle	Oui :	Revendications	1-15
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Ad point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle ; citations et explications à l'appui de cette déclaration

Il est fait référence au document suivant :

D1 WO 02/50641 A1 (CP8 TECHNOLOGIES [FR]; GIRAUD NICOLAS [FR]; BROLH ABRAHAM [FR]; HAMEAU) 27 juin 2002 (2002-06-27)

1.0. La présente demande ne remplit pas les conditions de brevetabilité, l'objet des revendications 1 et 10 n'impliquant pas d'activité inventive.

D1, qui est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, divulgue un dispositif électronique équipé d'un logiciel (p.9, l.1-5), caractérisé en ce que le logiciel comprend un module d'association agencé pour associer plusieurs codes distincts mais fonctionnellement identiques à une même instruction (p.11, l.1-5, voir aussi fig.2), et un module de sélection agencé pour sélectionner le code à exécuter pour ladite instruction de manière aléatoire (p.11, l. 14-20).

Par conséquent, l'objet de la revendication 1 diffère de ce connu en ce que le logiciel divulgué dans D1 est utilisé dans une machine virtuelle.

Cette différence consiste simplement à utiliser une technique connue dans une situation analogue et ne peut pas être considérée inventive.

Le même raisonnement s'applique mutatis mutandis à l'objet de la revendication indépendante correspondante 10 qui n'est donc pas considéré comme inventif.

2.0. Les revendications dépendantes 2-9, 11-15 ne contiennent pas de caractéristiques qui satisfassent aux exigences d'activité inventive en étant combinées aux caractéristiques de l'une quelconque des revendications auxquelles lesdites revendications dépendantes sont liées, comme suit:

2.1. L'objet des revendications 2, 3, 6-9, 11, 12 et 15 est divulgué dans D1:

pour les revendication 2 et 11, voir p.9, l.27-34;

pour les revendication 3 et 12, voir p.11, l.11-12;

pour les revendication 6-9 et 15, voir p.8, l.22-30; p.14, l.8-12.

2.2. L'objet des revendication 4 et 13 consiste simplement à évoquer une technique de génération des nombres aléatoires connue et ne peut pas être considéré inventif;

2.3. Concernant l'objet des revendications 5 et 14, D1 divulgue l'application du procédé de sécurisation aux instructions différentes (voir p.14, l.8-12), incitant la personne du métier à réaliser un dispositif ayant plusieurs instructions sécurisées. L'objet des revendications 5 et 14 consiste simplement en une spécification des contraintes imposées sur le choix des codes de remplacement, n'impliquant pas en soi une activité inventive, vu que les revendications n'énoncent pas en termes plus concrets la manière dont ce but peut être atteint. En effet, dans le contexte du document D1, ayant pour le but de sécuriser certaines opérations vulnérables en rendant leurs identifications plus difficiles (voir p.3, l.8-12), la personne du métier va définir des contraintes sur les codes de remplacement énoncées dans les revendications 5 et 14, sans qu'une activité inventive soit impliquée.

CABINET PLASSERAUD

Via EPOLINE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint-Petersbourg
75800 Paris cedex 08

Attn : Monsieur le Directeur Général

Paris, le 31 octobre 2011

N/Réf. : LW/FCR-FR 10 61252

Demande de brevet **français** n° **10 61252**
Déposée le **24 décembre 2010**
Au nom de **MORPHO**

Réponse au rapport de recherche préliminaire – DELAI : 2 NOVEMBRE 2011

Monsieur le Directeur,

Nous vous prions de bien vouloir prolonger le délai de réponse au rapport de recherche préliminaire que vous nous avez notifié le 29 juillet 2011 au sujet de la demande de brevet identifiée ci-dessus (Article R.612-59 du Code de la Propriété Intellectuelle).

Nous vous prions d'agréer, Monsieur le Directeur, nos salutations distinguées.

Lukasz WLODARCZYK
CPI n° 10-1112

CABINET PLASSERAUD

European Patent & Trademark Attorneys
Conseils en Propriété Industrielle

ASSOCIÉS
D. BOULINGUIEZ
F. BEROGIN
B. LOISEL
E. BURBAUD
G. KIESEL LE COSQUER
C. NARGOL WALLA
S. VERDURE
R. FLEURANCE
A. HASSINE
C.TOUATI
B.DEJARDINS
G.COUSIN
P.BOYLE
I.MEUNIER-COEUR

SECRÉTAIRE GÉNÉRAL
J-P MARTIN

COLLABORATEURS
G. RINGEISEN
P. BOIRE
P. ATTALI
G. VERMANDER
C.VOUGNY
F. BARBIER
E. BENSUSSAN
D.BOUBAL
S.PICARD
P. PRIEUR
I. SCHREIBER
G.PERIN
K.KIM SEIN AYE
F. NIEMANN
N. RICHARD
B. PÖPPING
E. MASSE
E. RENARD
P. LOUBAT
P. DUPIRE
M. CHATEAU
M. LEFRANC-BOZMAROV
O. HERBRETEAU
C.A. CARON
J. VINATIER-GILCHRIST
A. HUISMAN
G. LE FALHER
P. LOUVEL
B. AVELINE
C. JORON
F. GLAIZE
N. ROCABOY
A. DRUMOND
C. NDEDY-ETOGO
B. RELIGIEU X
N. WAJS
L. MENVILLE
B. COCHET
X. PRINCIVALLE
M. CHAVAROC
A. AYAV
K. ZHANG YI
D. HOCHEREAU
J. LIU ZHUN
A. TONG XIN JUN
C. HERITIER
A. TAKESITA
C. KOENIG
J. BERNAUD
M. GIRARDEAU
L. LIU QIAN
E. GRASSIN D'ALPHONSE
C. BERNARDI
E. MARCHAND
V. DUREISSEIX
A-L. LABALINE
D. BOURGAREL
L. WLODARCZYK
F. FABRE
T. MARCUS
E. GRUSON
C. BRANTIS
G. BU
K. SUZUKI-SAITO
J. WU JIA
B. BAO YU
T.VANYPRE
N.BARTHEL
V.LENG
J.LE BERRE
T.WOLF

www.plass.com

Via EPOLINE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 Bis, rue de St-Pétersbourg
75008 PARIS

Attn : Monsieur le Directeur Général

Paris, le 6 décembre 2011

N/Réf. : LW/FCR-FR 10 61252

Demande de brevet d'invention **français** n° **10 61252** du **24 décembre 2010**
Au nom de **MORPHO**

Réponse au rapport de recherche préliminaire – DELAI : 2 FEVRIER 2012

Monsieur le Directeur Général,

En réponse à la notification du rapport de recherche préliminaire concernant la demande de brevet référencée ci-dessus, le déposant présente les observations suivantes à l'appui des revendications initiales.

Un seul document, WO 02/50641 (D1), a été identifié comme pertinent à l'encontre des revendications.

Cependant, D1 ne divulgue ni ne suggère l'utilisation d'une machine virtuelle au sein d'un dispositif électronique, et encore moins la mise en œuvre du procédé revendiqué au sein d'une telle machine virtuelle plutôt qu'au niveau, par exemple, du système d'exploitation (ou toute autre entité) de ce dispositif électronique.

L'objet des revendications est donc nouveau et inventif.

Compte tenu de ce qui précède, le déposant considère qu'il n'existe plus d'obstacles à la délivrance du brevet et sollicite donc une suite favorable pour cette délivrance.

Dans cette attente, nous vous prions d'agréer, Monsieur le Directeur, nos sincères salutations.

/Lukasz WLODARCZYK/
CPI n° 10-1112

PARIS
52 rue de la victoire
75440 PARIS Cedex 09
Tél : +33 (0)1 40 16 70 00
Fax : +33 (0)1 42 80 01 59
info@plass.com

LYON
Immeuble le Rhône-Alpes
235 Cours Lafayette
69006 LYON
Tél : +33 (0)4 37 91 62 70
Fax : +33 (0)4 37 91 62 79
contact-lyon@plass.com

LILLE
96-98 Boulevard Carnot
BP 105 - 59 027 LILLE Cedex
en collaboration avec
Bureau Duthoit Legros Associés
Tél : +33 (0)3 28 14 14 90
Fax : +33 (0)3 28 14 14 95
contact-lille@plass.com

DIJON
Parc du Golf
14, rue du Golf
F - 21800 QUETIGNY-DIJON
Tél. +33 (0)3 80 27 37 47
Fax +33 (0)1 57 67 09 57
contact-dijon@plass.com

TOULOUSE
Immeuble Central Parc 2
7, avenue Parmentier
F-31200 TOULOUSE
Tél : +33 (0)5 34 42 48 00
Fax : +33 (0)5 61 32 92 47
contact-toulouse@plass.com

SHANGHAI
No. 570-578 West Hualhai Road
Red Town Building B-206
Shanghai China 200052
Tel. +86 21 6124 2975
Fax +86 21 6124 2976
contact-shanghai@plass.com

R E P U B L I Q U E F R A N C A I S E

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PIECE COMPLEMENTAIRE

Emetteur:

M. Lukasz WLODARCZYK
Cabinet Plasseraud
52 rue de la Victoire
75440 Paris Cedex 09
France

Adresse:

26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08

Téléphone : 0820 213 213
Télécopie : 01 53 04 52 65

Téléphone: 00 33 1 40 16 70 00
Télécopie : 00 33 1 42 80 01 59
Courrier électronique : info@plass.com

Lettre d'accompagnement relative à des pièces produites postérieurement au dépôt

La (Les) pièce(s) désignées ci-après est (sont) produite(s) postérieurement au dépôt, pour la demande suivante :

Numéro d'enregistrement national	1061252
Référence du demandeur ou du mandataire	FR 10 61252/LW

	Description des pièces	Nom du dossier original	Nom du dossier attribué
1	REPRRP	FR 10 61252 - Réponse RRP-cu.pdf	repRRP.pdf

		Coefficient utilisé	Barème des taxes	Montant à payer

	Paiement	
1	Paiement: indiquer le mode de paiement	Débit du compte de dépôt
	Devise: Par la présente, il est demandé à l'INPI de prélever du compte courant ci-après les taxes et frais repris à la page Taxes. Numéro du compte courant:	EUR

Annotations

Signatures

Lieu:	**Paris**
Date:	**09 décembre 2011**
Signé par:	**FR, CABINET PLASSERAUD, Lukasz WLODARCZYK**
Fonction:	**(Mandataire)**

1061252

R E P U B L I Q U E F R A N C A I S E

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PIECE COMPLEMENTAIRE

Récépissé électronique de la soumission

Il est certifié par la présente qu'un dépôt de pièce complémentaire a été reçu par le biais du dépôt électronique sécurisé de l'INPI.

Numéro de demande	1061252	
Numéro de soumission	1000133142	
Date de réception	09 décembre 2011	
Vos références	FR 10 61252/LW	
Demandeur	Morpho	
Pays	FR	
Documents envoyés	package-data.xml	fr-sfd-request.xml
	FRSFD.PDF (1 p.)	repRRP.pdf (1 p.)
Déposé par	EMAIL=wlodarczyk@plass.com,CN=Lukasz WLODARCZYK,O=CABINET PLASSERAUD,C=FR	
Méthode de dépôt	Dépôt électronique	
Date et heure de réception électronique	09 décembre 2011, 17:47:34 (CET)	
Empreinte officielle du dépôt	DA:F3:42:6C:10:DE:CF:9F:3F:28:2A:05:40:55:D8:54:F6:BD:58:92	

/INPI, section dépôt/