

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 28.05.09.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 03.12.10 Bulletin 10/48.

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) : PROTON WORLD INTERNATIONAL
NV — BE et STMICROELECTRONICS ROUSSET SAS
Société par actions simplifiée — FR.

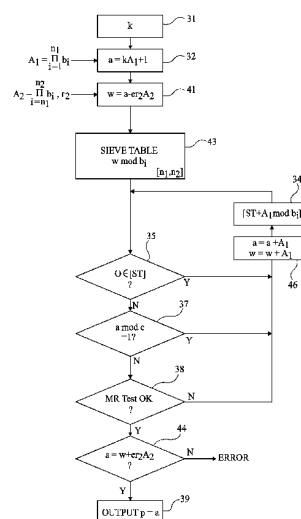
72 Inventeur(s) : DAEMEN JOAN, CUYPERS FRANCK,
VAN ASSCHE GILLES et LIARDÉ PIERRE YVAN.

73 Titulaire(s) : PROTON WORLD INTERNATIONAL NV,
STMICROELECTRONICS ROUSSET SAS Société par
actions simplifiée.

74 Mandataire(s) : CABINET BEAUMONT.

54 PROTECTION D'UNE GENERATION DE NOMBRES PREMIERS POUR ALGORITHME RSA.

57 L'invention concerne un procédé de protection d'une
génération, par un circuit électronique, d'au moins un nom-
bre premier (p) en testant le caractère premier de nombres
candidats (a) successifs, comportant: pour chaque nombre
candidat: le calcul (41, 46) d'un nombre témoin (w) faisant
intervenir au moins un premier nombre aléatoire (r₂), et au
moins un test de primalité (38) basé sur des calculs d'expo-
nentiation modulaire; et pour un nombre candidat ayant sa-
tisfait audit test de primalité: un test de cohérence (44) entre
le nombre candidat et son nombre témoin.



**PROTECTION D'UNE GENERATION DE NOMBRES PREMIERS POUR ALGORITHME
RSA**

Domaine de l'invention

La présente invention concerne de façon générale les circuits électroniques et, plus particulièrement, les circuits exécutant des algorithmes de chiffrement asymétriques de type RSA. L'invention concerne plus précisément la protection, lors
5 de la génération de nombres premiers dans un circuit électronique, contre des attaques par canaux cachés (Side Channel Attacks), par exemple par analyse statistique de la consommation du circuit (SPA - Simple Power Analysis) ou de sa signature
10 électromagnétique, ou contre des attaques par injections de fautes.

La présente invention s'applique à tout circuit électronique exploitant un algorithme exploitant une factorisation de nombres premiers et, plus particulièrement, aux cartes à
15 puces.

Exposé de l'art antérieur

L'algorithme RSA est l'un des algorithmes de chiffrement asymétrique (à clé publique) parmi les plus utilisés. Cet algorithme est utilisé pour chiffrer/déchiffrer des données
20 ou pour signer des données et permettre leur authentification. Il se base sur l'utilisation d'une paire de clés comportant une

clé publique et d'une clé privée. En chiffrement/déchiffrement, la clé publique est utilisée, par un émetteur, pour chiffrer des données à communiquer de façon confidentielle à un récepteur, ce dernier utilisant sa clé privée (ou secrète) pour déchiffrer les données. Pour une authentification, la clé privée est utilisée par l'émetteur pour signer les données alors que la clé publique est utilisée par le récepteur pour authentifier la signature.

La clé publique est une clé accessible de façon relativement large pour permettre à l'émetteur des données chiffrées ou au récepteur des données signées d'exploiter ces données. Par contre, la clé privée est réservée au circuit ayant créé la paire de clés. Le cas échéant, le titulaire de la paire de clés communique directement la clé publique à l'autre partie pour lui permettre de traiter les données.

La génération de la paire de clés publique et privée fait appel à une utilisation de deux nombres "p" et "q", différents et premiers entre eux, de taille relativement importante (typiquement 1024 ou 2048 bits). Le produit de ces nombres premiers représente le module de chiffrement "n". Les nombres p et q sont choisis pour que les nombres p-1 et q-1 soient premiers avec une quantité "e", appelée exposant public, ce dernier étant donc premier avec l'indicatrice d'Euler " $\phi(n)$ " du produit n ($\phi(n) = (p-1)(q-1)$). Il en résulte qu'il existe un entier "d" tel que le produit e*d congrue à 1 modulo $\phi(n)$. La paire n et e représente la clé publique tandis que la paire n et d représente la clé privée. L'exposant privé d représente l'inverse de l'exposant e, modulo (p-1)(q-1). Les nombres premiers p et q sont présents uniquement dans le circuit contenant la clé privée.

La robustesse de l'algorithme RSA dépend des nombres premiers p et q. Pour "casser" l'algorithme RSA à partir de la clé publique, il faut être en mesure de factoriser le nombre n, donc d'obtenir les nombres premiers p et q. Une fois cette factorisation connue, on peut calculer l'exposant privé d à partir de l'exposant public e (d s'obtient en calculant

l'inverse de e modulo $(p-1)(q-1)$). On considère aujourd'hui qu'en utilisant des modules n de taille suffisamment grande (typiquement de l'ordre de 1500 bits), les algorithmes actuels ne permettent pas, dans un temps raisonnable, de factoriser le
5 nombre n .

Toutefois, l'introduction des nombres p et q dans le circuit électronique ou leur génération par ce circuit est particulièrement critique en terme de sécurité, car leur découverte à ce moment de la vie du circuit par un pirate lui fournit
10 la factorisation du nombre n .

Une première technique de génération des clés RSA consiste à générer ces clés hors du circuit électronique. Les quantités p et q sont introduites dans le circuit électronique dans une phase de personnalisation. Cette technique est insen-
15 sible à des piratages par injection de fautes dans la mesure où les clés ne sont pas générées par le circuit électronique lui-même.

Une deuxième technique connue consiste à faire générer les nombres premiers par le circuit électronique lui-même dans
20 un environnement sécurisé (en pratique dans une installation protégée, à accès réservé). Cette technique ne pose pas non plus de problème d'attaques lors de la génération des nombres premiers.

Toutefois, de plus en plus souvent, on cherche à ce
25 que les circuits électroniques puissent générer leurs clés RSA hors de ces environnements sécurisés. Cela permet, par exemple, de régénérer de nouvelles clés en cas de répudiation d'une clé précédente (clé supposée piratée). Une telle génération s'effectue, par exemple, lors d'une personnalisation du circuit
30 électronique dans un environnement non sécurisé ou lors d'une première utilisation. (par exemple, pour des circuits utilisés pour des calculs de signatures ou des identifiants électroniques). Selon un exemple d'application aux passeports électroniques, on souhaite que la clé soit générée par la puce
35 électronique contenue dans le passeport une fois que celui-ci

est dans les mains de son titulaire. Ainsi, cette clé ne peut pas avoir servi au préalable dans une procédure d'authentification du passeport.

5 L'exposant public e peut être un paramètre du système à clé publique (Public Key Infrastructure - PKI) et est le même pour toutes les clés. Il est, par exemple, introduit dans le circuit électronique lors de sa fabrication (en mémoire morte ROM) ou dans une phase de personnalisation (en mémoire EEPROM).

10 L'exposant public e peut également être généré par le circuit électronique, par exemple par tirage d'un nombre aléatoire, et être ensuite communiqué aux éléments avec lesquels il doit communiquer.

15 La clé publique (exposant public et module de chiffrement) est donc soit connue du récepteur (signature) ou de l'émetteur (chiffrement), soit communiquée à celui-ci (à chaque transaction ou une fois pour toute) par le circuit électronique possédant la clé privée. La clé publique doit par ailleurs généralement être certifiée.

20 La génération de grands nombres premiers est coûteuse en temps et en calcul. En particulier, les tests dits de primalité qui permettent de valider le caractère premier ou non d'un nombre mettent généralement en oeuvre des exponentiations modulaires gourmandes en calcul (par exemple, le test de primalité dit de Miller-Rabin). C'est pourquoi, on cherche à
25 n'effectuer ces tests que pour des nombres candidats ayant déjà passé avec succès des tests par rapport à des nombres premiers relativement petits. Ces tests correspondent à des divisions par des nombres premiers relativement petits ou à des comparaisons par rapport à des tables de nombres premiers. Par exemple, on
30 peut effectuer un test de Miller-Rabin avec une petite base (deux par exemple) ou effectuer un calcul de plus grand commun diviseur (par exemple ajouter des octets modulo 255 pour obtenir un résultat inférieur à 255 et calculer ensuite le plus grand commun diviseur de ce résultat avec 255. S'il est différent de

1, on obtient avec un seul texte que le nombre n'est pas divisible par les trois facteurs de 255, à savoir 3, 5 et 17).

Lorsque les nombres premiers sont générés par le circuit électronique dans un environnement non sécurisé, le circuit est susceptible de subir des attaques par injection de fautes (perturbation de l'alimentation, attaques laser, etc.) exploitées par analyse des entrée-sorties ou de la consommation du circuit, ou de subir des attaques par canaux cachés (SPA ou DPA - Differential Power Analysis, ou analyse électromagnétique).

Un autre risque lié à la génération des nombres premiers par le circuit électronique est une attaque visant à modifier le nombre finalement sélectionné. Une attaque en fin de test Miller-Rabin peut servir à modifier le nombre pris en compte par l'algorithme. Si l'un des nombres p ou q n'est pas premier, le module de chiffrement n est plus facilement factorisable, ce qui affaiblit la sécurité de l'algorithme RSA.

Résumé

Il serait souhaitable de protéger la génération de nombres premiers et, par ce biais, la génération des clés d'un algorithme utilisant une factorisation de nombres premiers, lorsque ces nombres sont générés par le circuit électronique exploitant ces clés.

Il serait par ailleurs souhaitable de pouvoir détecter une modification d'un nombre premier fourni par le processus de génération.

Il serait par ailleurs souhaitable de pouvoir masquer la génération des nombres premiers.

Pour atteindre tout ou partie de ces objets ainsi que d'autres, il est prévu un procédé de protection d'une génération, par un circuit électronique, d'au moins un nombre premier en testant le caractère premier de nombres candidats successifs, comportant :

pour chaque nombre candidat :

le calcul d'un nombre témoin faisant intervenir au moins un premier nombre aléatoire ; et

au moins un test de primalité basé sur des calculs d'exponentiation modulaire ; et

5 pour un nombre candidat ayant satisfait audit test de primalité :

un test de cohérence entre le nombre candidat et son nombre témoin.

10 Selon un mode de réalisation de la présente invention, le nombre témoin est obtenu en soustrayant ou en ajoutant au nombre candidat une quantité dépendant dudit premier nombre aléatoire.

Selon un mode de réalisation de la présente invention, chaque nombre candidat est soumis, avant le test de primalité
15 basé sur des calculs d'exponentiation modulaire, à au moins un test de primalité basé sur une table crible comportant autant d'éléments qu'il existe de nombres premiers entre un premier seuil et un second seuil, un nombre candidat initial étant obtenu en multipliant un nombre quelconque par un premier produit
20 des nombres premiers inférieurs au premier seuil.

Selon un mode de réalisation de la présente invention, le passage d'un nombre candidat au suivant comporte l'ajout, aux nombres candidat et témoin courants, dudit premier produit.

Selon un mode de réalisation de la présente invention,
25 le passage d'un nombre candidat au suivant comporte l'ajout, aux nombres candidat et témoin courants, d'un multiple dudit premier produit, le coefficient multiplicateur étant fonction au moins d'un nombre aléatoire et d'un second produit des nombres premiers compris entre les premier et second seuils.

30 Selon un mode de réalisation de la présente invention, ledit coefficient multiplicateur est en outre fonction d'un exposant public de l'algorithme RSA.

Selon un mode de réalisation de la présente invention, la table crible est basée sur les nombres témoin.

Selon un mode de réalisation de la présente invention, la table crible est, à chaque nouveau nombre candidat, mise à jour en ajoutant à chacun des ses éléments, ledit premier produit, modulo l'élément concerné.

5 Selon un mode de réalisation de la présente invention, chaque nombre candidat est soumis, avant le test de primalité basé sur des calculs d'exponentiation modulaire, à un test de conformité par rapport à un exposant public de l'algorithme RSA.

 Selon un mode de réalisation de la présente invention,
10 le test de primalité basé sur des calculs d'exponentiation modulaire est un test Miller-Rabin.

Il est également prévu un circuit électronique comportant des moyens pour la mise en oeuvre du procédé décrit.

Brève description des dessins

15 Ces objets, caractéristiques et avantages, ainsi que d'autres seront exposés en détail dans la description suivante de modes de réalisation particuliers faite à titre non-limitatif en relation avec les figures jointes parmi lesquelles :

 la figure 1 est un schéma bloc d'un mode de
20 réalisation d'un circuit intégré du type auquel s'applique à titre d'exemple de la présente invention ;

 la figure 2A illustre de façon très schématique un chiffrement au moyen d'un algorithme RSA ;

 la figure 2B illustre de façon schématique un
25 déchiffrement au moyen d'un algorithme RSA ;

 la figure 3 est un schéma bloc illustrant un système de transmission de données chiffrées ;

 la figure 4 est un schéma bloc illustrant des étapes usuelles de génération de nombres premiers au sein d'un circuit
30 électronique mettant en oeuvre un algorithme de type RSA ;

 la figure 5 est un schéma bloc représentant des étapes d'un mode de réalisation du procédé de génération d'un nombre premier ; et

la figure 6 représente partiellement, sous forme de blocs, un autre mode de réalisation du procédé de génération d'un nombre premier.

Description détaillée

5 Par souci de clarté, de mêmes éléments ont été désignés par de mêmes références aux différentes figures. De plus, seules les étapes et éléments utiles à la compréhension de l'invention ont été représentés et seront décrits. En particulier, l'exploitation faite par le circuit électronique de
10 l'algorithme utilisant les clés basées sur les nombres premiers n'a pas été détaillée, l'invention étant compatible avec toute exploitation usuelle (chiffrement, calcul de signature) des nombres premiers générés.

L'invention sera décrite par la suite en relation avec
15 un exemple d'application à l'algorithme RSA utilisé en chiffrement/déchiffrement. On notera toutefois que l'invention s'applique quelle que soit l'utilisation faite de l'algorithme RSA à partir des nombres premiers générés, en particulier, l'invention s'applique à des signatures RSA. Plus généralement,
20 l'invention s'applique à tout algorithme dont les clés dépendent d'une factorisation de nombre premiers, par exemple, le système de chiffrement dit de Rabin.

La figure 1 représente, de façon très schématique et sous forme de blocs, un exemple de circuit électronique 1 (par
25 exemple d'une carte à puce) du type auquel s'applique la présente invention. Un tel circuit comporte une unité de traitement 11 (PU), susceptible de communiquer, par l'intermédiaire d'un ou plusieurs bus 12 de données, d'adresses et de commandes, avec différents éléments parmi lesquels une ou
30 plusieurs mémoires non volatiles 13 (NVM), généralement une mémoire ROM contenant tout ou partie des programmes et une mémoire EEPROM destinée à contenir les clés RSA, une ou plusieurs mémoires volatiles 14 (typiquement de type RAM) et des circuits d'interface 15 (I/O) d'entrée-sortie permettant au circuit 1 de
35 communiquer avec l'extérieur. Dans les applications que vise

plus particulièrement la présente invention, le circuit 1 comporte également un processeur de chiffrement ou de calcul de signature 16 (CP), le cas échéant confondu avec l'unité centrale 11. Le circuit 1 est susceptible de mettre en oeuvre différentes fonctions réalisées par des éléments matériels et/ou logiciels qui ont été symbolisées par un bloc 17 (FCT) en pointillés. Une de ces fonctions, symbolisée par un bloc 18 (PN GEN), représente la fonction de génération de nombres premiers pour servir de clés d'un algorithme de type RSA. D'autres composants et circuits peuvent équiper le circuit électronique 1 en fonction de sa destination. En outre, des liaisons directes (non représentées) entre certains sous-ensembles du circuit pour échanger des données, adresses et/ou commandes peuvent être prévues.

Les figures 2A et 2B illustrent la mise en oeuvre d'un algorithme de type RSA. La cellule de calcul RSA est symbolisée par un bloc 20 en figure 2A (côté chiffrement) et par un bloc 21 en figure 2B (côté déchiffrement). Ces cellules de calcul peuvent en pratique être identiques, qu'elles soient logicielles ou matérielles.

Le chiffrement d'un message M de données, représenté sous la forme d'un nombre entier, est introduit dans le bloc de calcul RSA qui contient ou reçoit par ailleurs le module de chiffrement n et l'exposant de chiffrement e de la clé publique. Le nombre entier M est inférieur au module de chiffrement n. Le bloc RSA calcule le message chiffré C qui représente l'exponentiation modulaire $M^e \bmod n$.

Côté déchiffrement par le circuit possédant la clé privée (n, d), le message C est soumis à une exponentiation modulaire sur la base de l'exposant d et du modulo n, c'est-à-dire que la cellule 21 fournit le message M représentant $C^d \bmod n$.

La figure 3 est un schéma bloc illustrant un exemple de transmission de données DATA (bloc 24) représentant un contenu numérique quelconque par un émetteur 22 à destination

d'un récepteur 23. Le récepteur dispose des clés RSA et commence, si elle n'est pas connue de l'émetteur, par lui transmettre la clé publique, c'est-à-dire le module de factorisation n et l'exposant public e . Cela permet à l'émetteur de chiffrer les données et de les transmettre sous forme de message chiffré C . Le récepteur 23 utilise sa clé privé (n, d) pour déchiffrer les messages et obtenir les données DATA (bloc 25).

Les transmissions sont susceptibles de subir des tentatives de piratage visant à découvrir la factorisation du nombre n . L'invention ne vise pas ces attaques une fois les clés générées mais les attaques susceptibles d'être introduites lors de la génération des nombres premiers qui intervient une seule fois (ou à chaque génération d'un nouvelle paire de clé).

La génération d'un nombre premier consiste à modifier un nombre candidat jusqu'à ce qu'il soit premier. Comme indiqué précédemment, on effectue des tests simplifiés pour vérifier que le candidat est bien premier avec des nombres relativement petits avant de le soumettre à un test de primalité adapté aux grands nombres. Les tests adaptés aux grands nombres sont généralement basés sur le théorème de Fermat d'après lequel si " u " est un nombre premier, v^{u-1} est congru à 1 modulo u pour tout entier " v ", c'est-à-dire qu'il n'existe pas de factorisation possible du nombre " u " par un entier autre que 1 ou u . Le test de primalité désormais le plus utilisé pour la génération de nombres premiers est le test dit de Miller-Rabin. Ce test met en oeuvre des calculs d'exponentiation modulaire pour vérifier que le candidat n'est pas divisible par un autre nombre que 1 et est décrit, par exemple, dans l'ouvrage "Handbook of Applied Cryptography" de A. Menezes, P. van Oorschot et S. Vanstone, paru en 1996 (CRC Press), chapitre 4, point 4.2.3, page 138-140. En fait, les tests de primalité ne sont pas parfaits mais la probabilité d'erreur est suffisamment faible pour que l'on puisse considérer le candidat comme premier.

La figure 4 est un schéma bloc illustrant les étapes d'un procédé de génération usuel d'un nombre premier (noté

arbitrairement p), destiné à représenter l'un des deux nombres premiers du module de factorisation RSA. Le procédé de la figure 4 est généralement mis en oeuvre deux fois successivement pour obtenir les nombres p et q .

5 On commence par sélectionner un nombre quelconque (bloc 31, RANDOM) k , par exemple sous l'effet d'un tirage aléatoire. Puis, on modifie ce nombre de sorte à obtenir un candidat non divisible par les nombres premiers inférieur à un premier seuil n_1 .

10 Selon un exemple, le nombre k est multiplié (bloc 32, X) par le produit A_1 des nombres premiers b_i inférieurs au seuil n_1 . Le seuil n_1 est choisi relativement petit (par exemple $n_1 = 3$, donc $A_1 = 6$, ou $n_1 = 5$, donc $A_1 = 30$). Puis, on ajoute ou on retranche l'unité (bloc 32', ± 1) au produit calculé pour
15 qu'il ne soit divisible, dans l'exemple où $n_1 = 3$, ni par 2, ni par 3. On obtient un premier candidat $a = k.A_1 \pm 1$, premier avec les nombres 2 et 3.

 La taille souhaitée pour les nombres p et q est fixée. Par conséquent, la taille des candidats a doit correspondre à
20 celle souhaitée pour les nombres p et q . La taille du nombre k dépend donc de celle du nombre A_1 . Dans l'exemple ci-dessus, pour un nombre a de 1024 bits et un nombre A_1 de 30, le nombre k est choisi sur 1019 bits.

 Selon un autre exemple, le nombre k est modifié en
25 effectuant l'opération $k = k - (k \bmod A_1)$ pour le rendre divisible par A_1 . Puis, on ajoute un nombre x inférieur A_1 que l'on sélectionne arbitrairement dans une table de nombres premiers avec A_1 . On obtient alors un candidat a , premier avec les nombres premiers inférieurs à n_1 . Dans cet exemple, le nombre k
30 a la même taille que celle souhaitée pour le nombre a .

 L'étape suivante (bloc 33) consiste à construire une table crible ST (SIEVE TABLE) dont chacun des termes représente le résultat de la division du candidat a par un des nombres premiers compris entre le premier seuil n_1 et un deuxième seuil
35 n_2 supérieur. Cela revient à remplir la table avec les valeurs

a mod b_i pour b_i compris entre n_1 et n_2 . Un tel remplissage fait appel à des divisions impliquant le candidat qui sont sensibles à des attaques par canaux cachés. Le seuil n_2 est choisi pour que la table ne soit pas trop importante en taille et pour que
5 les calculs qui seront faits ultérieurement, pour chaque candidat, restent moins gourmands (en temps et énergie requise pour les calculs) par rapport à un test de Miller-Rabin sur le candidat. Par exemple, le seuil n_2 est égal à 128 ou 256.

Une fois la table crible initialisée, les opérations
10 suivantes sont effectuées tant que le candidat a ne correspond pas à un nombre premier acceptable pour la mise en oeuvre de l'algorithme RSA.

On commence par vérifier que le candidat est premier avec tous les nombres contenus dans l'intervalle $[n_1, n_2]$. Cela
15 revient à vérifier (bloc 35, $0 \in [ST]$?) que cette table ne contient pas de valeur nulle. La présence d'une valeur nulle signifie que le candidat a est un multiple du nombre premier correspondant de la table.

Si le test 35 confirme (sortie N du bloc 35) que le
20 candidat est premier avec tous les nombres de l'intervalle $[n_1, n_2]$, on vérifie (bloc 37) si le candidat convient pour une mise en oeuvre de l'algorithme RSA. Pour cela, il faut vérifier que le nombre $a-1$ est premier avec e . En pratique, on regarde si la valeur $a \bmod e$ (le reste de la division euclidienne de a par e)
25 est égale à 1. Dans la négative, le candidat a est compatible avec le RSA, c'est-à-dire qu'il respectera la condition que l'exposant e est un entier premier avec l'indicatrice d'Euler $(p-1)(q-1)$.

Une fois le test 37 passé (sortie N), le candidat est
30 finalement soumis à plusieurs exécutions (généralement de quelques exécutions à quelques dizaines d'exécutions) d'un test de primalité de Miller-Rabin (bloc 38, RM tests OK ?). S'il satisfait à ce test (sortie Y du bloc 38), le candidat a est fourni (bloc 39, OUTPUT $p=a$) en tant que nombre premier p .

Dès qu'un des tests 35, 37 ou 38 indique que le candidat ne convient pas (sorties Y des blocs 35 et 37 ou N du bloc 38), un nouveau candidat est choisi. Pour cela, on commence (bloc 36, $a = a + A_1$) par ajouter la valeur A_1 au candidat refusé. Puis, on met à jour la table crible [ST]. Cela revient à
 5 ajouter (bloc 34, $[ST] + A_1 \bmod b_i$) la quantité A_1 modulo b_i à chacun des éléments (identifiés par i) de la table et le procédé revient à l'étape 34. Bien que cela n'ait pas été représenté, on met également à jour une variable contenant la valeur $a \bmod e$
 10 qui servira ensuite au test 37.

Une fois un premier nombre premier p obtenu, le procédé est mis en oeuvre de nouveau pour sélectionner le deuxième nombre premier q nécessaire à la mise en oeuvre de l'algorithme RSA. Une étape supplémentaire est alors de
 15 s'assurer que les nombres p et q sont premiers entre eux (étape non illustrée en figure 4). Comme il s'agit de nombres premiers, il suffit de vérifier qu'ils sont différents.

La succession des étapes de génération des nombres premiers est particulièrement sensible aux attaques par canaux cachés ou par injection de fautes. De telles attaques peuvent
 20 avoir pour objectif de découvrir le nombre premier généré ou de forcer la génération d'un nombre non premier. Dans les deux cas, cela peut permettre à un pirate de découvrir la clé privée.

La figure 5 est un schéma bloc illustrant un mode de
 25 réalisation du procédé de génération de nombres premiers, protégé contre d'éventuelles attaques par canaux cachés (analyse de la consommation ou analyse de la réponse électromagnétique) ou par injection de fautes. Ce schéma bloc est à rapprocher de celui de la figure 4.

30 Comme précédemment, on commence par choisir un seuil n_1 conditionnant un produit A_1 utilisé dans les tests de primalité. Par exemple, le seuil n_1 vaut 3 ou 5 et le produit A_1 vaut 6 ou 30. D'autres valeurs de n_1 pourront être choisies.

Puis (bloc 31, a), on tire un nombre quelconque k . que
 35 l'on modifie pour le rendre non divisible par les nombres

premiers inférieurs au seuil n_1 . Comme précédemment, la taille du nombre k dépend donc de celle du nombre A_1 . Par exemple (bloc 32, $a = k.A_1 + 1$), le nombre k est multiplié par le produit A_1 et additionné à 1 (en variante, 1 est soustrait à ce résultat).

5 D'autres façons de générer le premier candidat a peuvent être utilisées.

L'étape suivante (bloc 41, $w = a - e.r_2.A_2$) consiste à générer un nombre témoin w qui sera utilisé en fin du processus de génération pour s'assurer que le candidat a n'a pas été
10 perturbé et pour protéger les divisions par les petits nombres premiers contre des attaques par canaux cachés.

La quantité w est obtenue, par exemple, en retranchant, au candidat a , la valeur $e.r_2.A_2$, où e représente l'exposant public (par exemple, sur 32 ou 64 bits), où r_2 représente
15 un nombre aléatoire et où A_2 représente le produit des nombres premiers dans un intervalle $[n_1, n_2]$. Le seuil n_2 représente, comme précédemment, un seuil utilisé ultérieurement pour la création d'une table crible. Par exemple, le seuil n_2 est choisi égal à 128 ou 256. D'autres valeurs de n_2 pourront être
20 choisies.

La taille du nombre aléatoire r_2 est égale à la taille du candidat a , diminuée de la taille de l'exposant public e et de la taille du produit A_2 . Ainsi, le terme soustrait a la même taille que le nombre a .

25 Ce mode de réalisation s'applique donc au cas où l'exposant public e est de taille relativement petite (inférieure à une centaine de bits). L'invention s'applique toutefois également à des nombre e plus grands (par exemple de la même taille que les nombre premiers à générer). Dans ce cas (non
30 représenté), le nombre e n'est pas pris en compte dans les tests de primalité qui précèdent le test de Miller-Rabin et son caractère premier avec le candidat sélectionné est vérifié à l'issue de ce test par un test spécifique (par division).

Par la suite, on supposera que le nombre e est
35 suffisamment petit pour être pris en compte dans la génération

des nombres p et q , ce qui évite un test de primalité complet sur le nombre e .

L'étape (bloc 43) suivant la génération du nombre w consiste à générer la table crible $[ST]$ à partir du témoin w . On
 5 verra en relation avec la figure 6 que la table crible peut également être générée à partir du candidat a .

Dans le mode de réalisation de la figure 5, la table $[ST]$ comporte autant d'éléments qu'il y a de nombres premiers b_i dans l'intervalle $[n_1, n_2]$. Chaque élément correspond à la
 10 division du témoin w par le nombre premier b_i correspondant et est égal à $a \bmod b_i$. Le fait que la quantité w soit créée en retranchant un multiple des quantités e et A_2 au nombre a permet que les valeurs de la table crible représentent à la fois le résultat $w \bmod b_i$ et $a \bmod b_i$.

15 Puis, on effectue de façon itérative tant qu'un candidat acceptable n'est pas trouvé les étapes suivantes.

On commence (bloc 35) par s'assurer que les nombres a et w sont premiers avec tous les nombres premiers b_i de l'intervalle $[n_1, n_2]$. Pour cela, on vérifie si l'un des
 20 éléments de la table $[ST]$ est nul. Dans la négative, on passe au test suivant (bloc 37, $a \bmod e = 1$?) pour vérifier la compatibilité du candidat avec l'exposant publique e .

Si un candidat a a passé tous les tests précédents (sortie N du bloc 37), il est soumis au test de Miller-Rabin
 25 (bloc 38).

Dès qu'un des tests 35, 37 ou 38 indique que le candidat ne convient pas, (sorties Y des blocs 35, 37 ou N du bloc 38), un nouveau candidat et un nouveau témoin sont calculés (bloc 46, $a = a + A_1$, $w = w + A_1$), en ajoutant, aux valeurs
 30 précédentes, la valeur A_1 . Puis (bloc 34, $[ST] + A_1 \bmod b_i$), on met à jour la table crible $[ST]$ en ajoutant la valeur A_1 à tous ses éléments modulo b_i . En pratique, on met également à jour une variable contenant la valeur $a \bmod e$ (donc servant au test 37) en $a \bmod e + A_1$.

Le nouveau candidat est alors soumis aux tests 35 et 37, 38 (l'ordre des tests 35 et 37 n'a pas d'importance).

Si le candidat est acceptable (sortie Y du bloc 38), une étape additionnelle (bloc 44, $a = w + e.r_2.A_2$?) permet de
5 vérifier l'intégrité du candidat par rapport au début du calcul, c'est-à-dire sa cohérence avec le témoin w . Par exemple, on ajoute au témoin w la valeur $e.r_2.A_2$ et on vérifie que le résultat est égal au candidat a . Dans l'affirmative (sortie Y du bloc 44), le candidat a est fourni (bloc 39, OUTPUT $p=a$) en tant
10 que nombre premier p . Sinon (sortie N du bloc 44), cela signifie qu'une perturbation est intervenue dans la génération du nombre premier. Le circuit passe alors en traitement d'erreur (ERROR). En variante, le test du bloc 44 vérifie que la quantité A_2 divise la valeur $a-w$. Une telle variante permet d'éviter de
15 mémoriser la quantité aléatoire r_2 . Selon une autre variante, l'étape 41 est remplacée par une addition et l'étape 44 par une soustraction.

Le traitement d'erreur est, par exemple, l'annulation du nombre premier généré (on redémarre le processus de l'étape
20 31) ou une invalidation du circuit. De telles actions à prendre en cas de détection d'une tentative de piratage sont en elle-même classiques et de multiples solutions existent selon les applications.

Le test de cohérence ou d'intégrité 44 permet d'éviter
25 une attaque imposant un nombre différent du nombre a , après le test de Miller-Rabin.

Une fois qu'un premier nombre premier p a été généré, le processus est repris pour générer un deuxième nombre premier q en vérifiant que les nombre p et q soient premiers entre eux.
30 Enfin, pour la mise en oeuvre de l'algorithme RSA, le module de factorisation n est calculé ($n = p.q$) et est transmis (avec l'exposant e) pour constituer la clé publique à toute entité susceptible d'en avoir besoin. Les nombres p et q sont stockés uniquement dans le circuit électronique 1.

Le fait de construire la table crible sur la base du nombre témoin w (au lieu du nombre a) permet de masquer cette construction.

La figure 6 est un schéma-bloc illustrant un autre mode de réalisation. Seules les étapes modifiées par rapport à la figure 5 sont représentés.

Par rapport au mode de réalisation précédent, la table crible est basée sur le nombre candidat a . Elle est donc initialisée (bloc 43', SIEVE TABLE, $a \bmod b_i[n_1, n_2]$) par les termes $a \bmod b_i$ de l'intervalle $[n_1, n_2]$. Pour préserver une mise à jour de la table crible par l'ajout de la quantité A_1 , on construit une quantité f à ajouter d'un candidat au candidat suivant et d'un témoin au témoin suivant (bloc 46') de sorte que cette quantité f soit égale à $A_1 \bmod b_i$ et à $A_1 \bmod e$. Par exemple, on tire un nombre aléatoire r_1 , choisi indépendamment du nombre r_2 , et on le multiplie par le produit $e.A_2$. La taille du nombre r_1 est telle que la taille du produit $r_1.e.A_2$ est inférieure (de quelques octets à quelques dizaines d'octets) à la longueur requise pour le nombre premier à générer. Cela permet que le passage d'un candidat à un autre s'accompagne d'une modification d'un grand nombre des bits. Puis, on ajoute au produit l'unité 1. Ainsi, comme l'illustre la figure 6, on obtient un nouveau candidat et un nouveau témoin en ajoutant (bloc 46) aux valeurs précédentes, la valeur $f.A_1$ avec $f=e.r_1.A_2+1$. Les nouveaux candidat et témoin restent premiers avec les nombres premiers inférieurs au seuil n_1 . Comme A_2 est égal à 0 modulo b_i , le produit $(e.r_1.A_2+1)$ est égal à 1 mod b_i . La mise à jour de la table (bloc 34) peut donc être effectuée, comme dans le mode de réalisation précédent en ajoutant, à chacun des éléments de la table $[ST]$ modulo le nombre premier b_i de l'élément concerné, la valeur A_1 .

Divers modes de réalisation avec diverses variantes ont été décrits ci-dessus. On notera que l'homme de l'art pourra combiner divers éléments de ces divers modes de réalisation et variantes sans faire preuve d'activité inventive. De plus, la

mise en oeuvre pratique de l'invention à partir des indications fonctionnelles données ci-dessus est à la portée de l'homme du métier, que ce soit pour une implémentation matérielle ou logicielle.

5 En particulier, le choix des seuils n_1 et n_2 utilisés pour les tests précédant le test de Miller-Rabin dépend de l'application et du temps que l'on peut consacrer au test de Miller-Rabin lors de la génération des nombres premiers. Par exemple, bien qu'il soit préférable que la table crible ne soit
10 pas basée sur les nombres premiers inférieurs au premier seuil pour économiser des calculs, ce n'est pas indispensable.

De plus, le choix des tailles des quantités aléatoires est adapté en fonction des tailles souhaitées pour les nombres premiers p et q , donc pour le modulo n des exponentiations
15 modulaires de l'algorithme RSA.

En outre, bien que l'invention ait été décrite en relation avec un procédé mettant en oeuvre une seule table crible, on peut envisager d'utiliser plusieurs tables cribles en intercalant le test de primalité (étapes 34 et 35) de chaque
20 table avant la table suivante, chaque table ayant pour rôle de vérifier la primalité du nombre candidat par rapport à des nombres premiers compris dans des plages contigües définies par des seuils successifs. Une telle variante peut servir, dans un souci d'optimisation, à ne mettre à jour une table que si le
25 test de primalité basé sur la table précédente est validé.

REVENDEICATIONS

1. Procédé de protection d'une génération, par un circuit électronique (1), d'au moins un nombre premier (p) en testant le caractère premier de nombres candidats (a) successifs, comportant :

5 pour chaque nombre candidat :

 le calcul (41, 46) d'un nombre témoin (w) faisant intervenir au moins un premier nombre aléatoire (r_2) ; et

 au moins un test de primalité (38) basé sur des calculs d'exponentiation modulaire ; et

10 pour un nombre candidat ayant satisfait audit test de primalité :

 un test de cohérence (44) entre le nombre candidat et son nombre témoin.

2. Procédé selon la revendication 1, dans lequel le
15 nombre témoin (w) est obtenu en soustrayant ou en ajoutant au nombre candidat (a) une quantité dépendant dudit premier nombre aléatoire (r_2).

3. Procédé selon la revendication 2, dans lequel
20 chaque nombre candidat est soumis, avant le test de primalité basé sur des calculs d'exponentiation modulaire, à au moins un test de primalité basé sur une table crible ([ST]) comportant autant d'éléments qu'il existe de nombres premiers (b_i) entre un premier seuil (n_1) et un second seuil (n_2), un nombre candidat initial étant obtenu en multipliant un nombre quelconque (k) par
25 un premier produit (A_1) des nombres premiers inférieurs au premier seuil.

4. Procédé selon la revendication 3, dans lequel le
passage d'un nombre candidat au suivant comporte l'ajout (46),
aux nombres candidat et témoin courants, dudit premier produit
30 (A_1).

5. Procédé selon la revendication 3, dans lequel le
passage d'un nombre candidat au suivant comporte l'ajout (46'),
aux nombres candidat et témoin courants, d'un multiple
(($e.r_1.A_2+1$). A_1) dudit premier produit (A_1), le coefficient

multiplicateur étant fonction au moins d'un nombre aléatoire (r_2) et d'un second produit (A_2) des nombres premiers (b_i) compris entre les premier (n_1) et second (n_2) seuils.

5 6. Procédé selon la revendication 5, dans lequel ledit coefficient multiplicateur est en outre fonction d'un exposant public (e) de l'algorithme RSA.

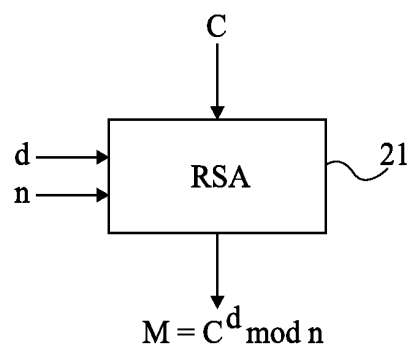
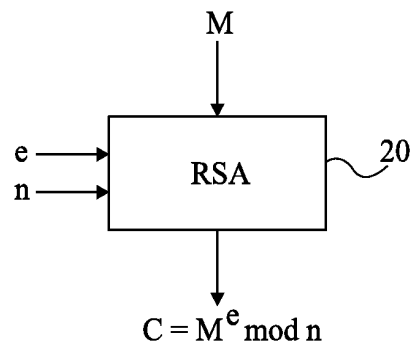
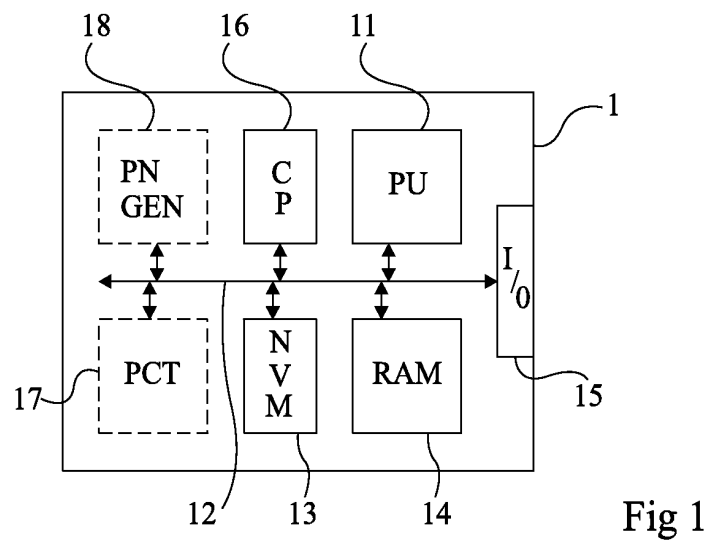
7. Procédé selon l'une quelconque des revendications 3 à 6, dans lequel la table crible ($[ST]$) est basée sur les nombres témoin (w).

10 8. Procédé selon l'une quelconque des revendications 3 à 7, dans lequel la table crible ($[ST]$) est, à chaque nouveau nombre candidat (a), mise à jour en ajoutant à chacun des ses éléments, ledit premier produit (A_1), modulo l'élément concerné (b_i).

15 9. Procédé selon l'une quelconque des revendications 1 à 8, dans lequel chaque nombre candidat (a) est soumis, avant le test de primalité basé sur des calculs d'exponentiation modulaire (38), à un test (37) de conformité par rapport à un exposant public (e) de l'algorithme RSA.

20 10. Procédé selon l'une quelconque des revendications 1 à 9, dans lequel le test de primalité (38) basé sur des calculs d'exponentiation modulaire est un test Miller-Rabin.

25 11. Circuit électronique comportant des moyens pour la mise en oeuvre du procédé conforme à l'une quelconque des revendications 1 à 10.



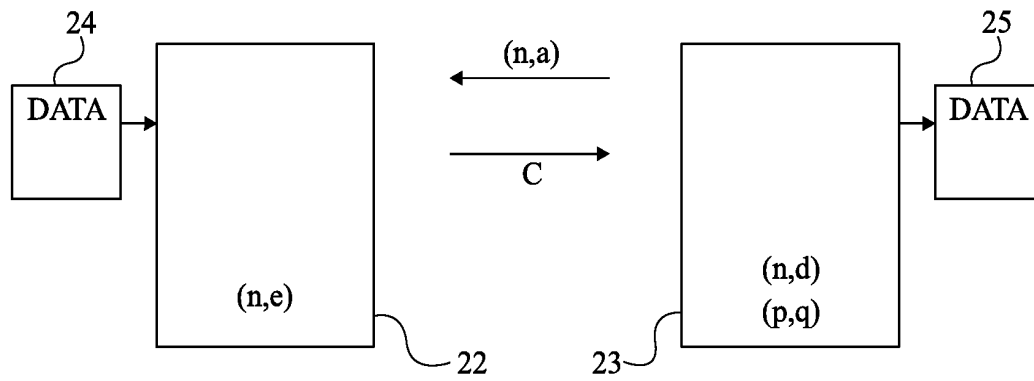


Fig 3

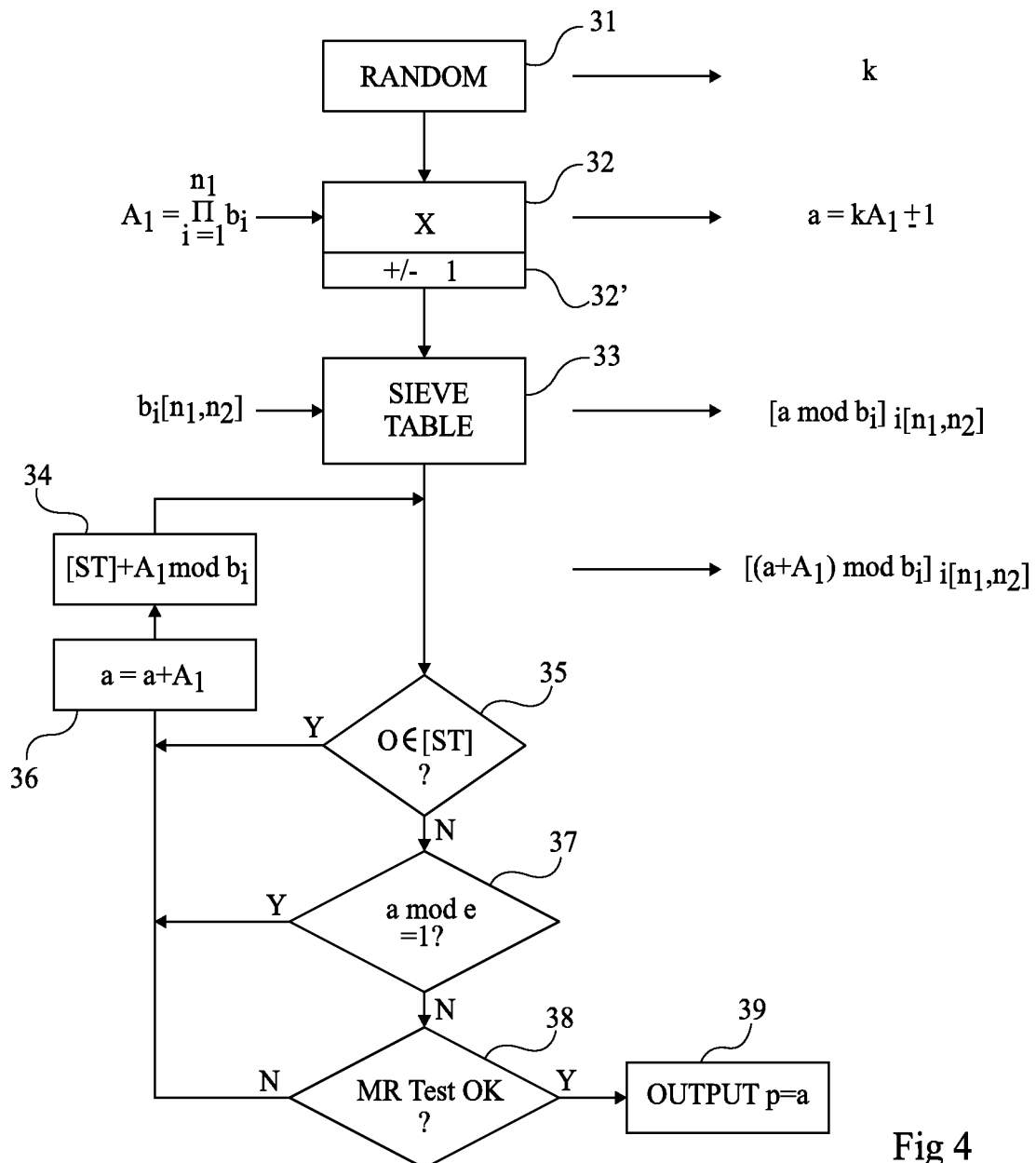


Fig 4

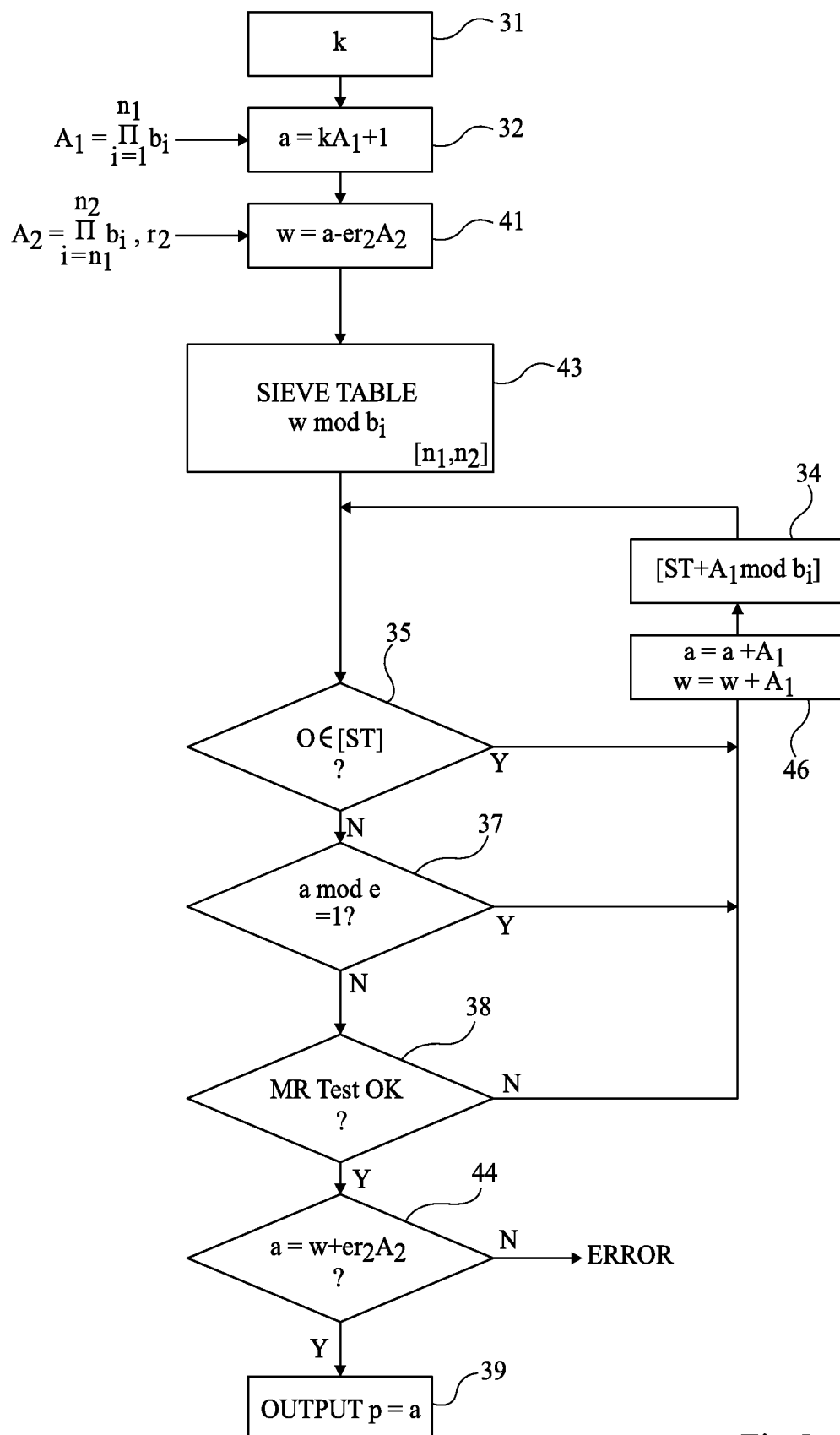


Fig 5

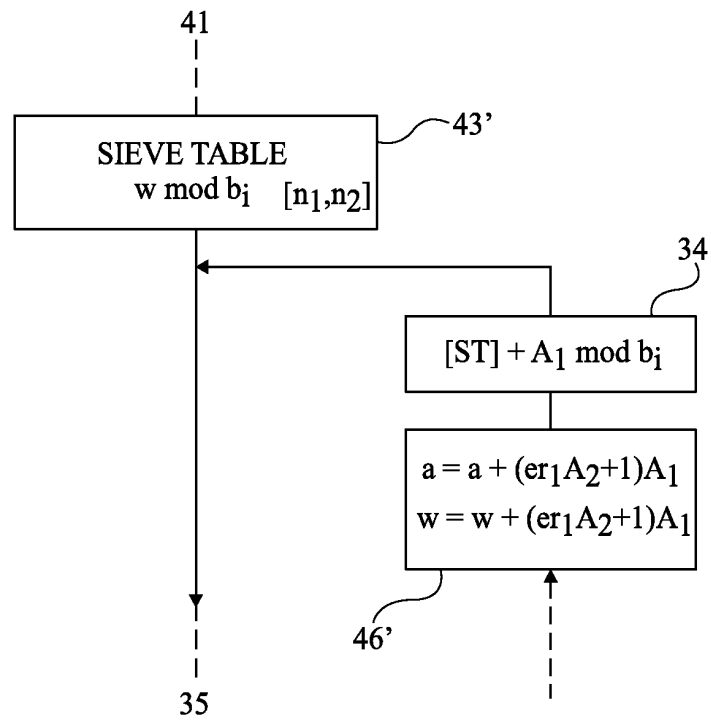


Fig 6



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 726048
FR 0953523

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 2003/108193 A1 (SOTOODEH MEHDI [US]) 12 juin 2003 (2003-06-12) * abrégé; figure 2 * * alinéa [0017] - alinéa [0019] * -----	1-11	H04L9/30 G06F7/58
A	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC, USA, XP000863996 * page 138 - page 140 * * page 285 - page 291 * -----	1-11	
A	US 2002/186837 A1 (HOPKINS W DALE [US] ET AL) 12 décembre 2002 (2002-12-12) * abrégé; figure 8 * * alinéa [0029] - alinéa [0040] * -----	1-11	
A	US 7 043 018 B1 (KASAHARA MASAO [JP] ET AL) 9 mai 2006 (2006-05-09) * abrégé; figure 3 * * colonne 3 * -----	1-11	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L G06F
Date d'achèvement de la recherche		Examineur	
23 février 2010		San Millán Maeso, J	
CATÉGORIE DES DOCUMENTS CITÉS		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	
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			

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0953523 FA 726048**

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 **23-02-2010**

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
US 2003108193 A1	12-06-2003	AUCUN	
US 2002186837 A1	12-12-2002	AUCUN	
US 7043018 B1	09-05-2006	JP 3518672 B2	12-04-2004
		JP 2000162968 A	16-06-2000