Code de distribution interne :

(A) [-] Publication au JO
(B) [-] Aux Présidents et Membres
(C) [-] Aux Présidents
(D) [X] Pas de distribution

Liste des données pour la décision du 22 novembre 2013

N° du recours : T 0438/10 - 3.5.06

N° de la demande : 02735524.7

N° de la publication : 1399807

C.I.B. : G06F7/72

Langue de la procédure : FR

Titre de l'invention :
BROUILLAGE D'UN CALCUL METTANT EN OEUVRE UNE FONCTION MODULAIRE

Titulaire du brevet :
STMicroelectronics S.A.

Opposant :
GIESECKE & DEVRIENT GmbH

Référence :
Brouillage d'un calcul/STMICROELECTRONICS

Normes juridiques appliquées :
CBE 1973 Art. 100a), 56

Mot-clé :
Activité inventive - (non)

Décisions citées :

Exergue :

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

N° du recours : T 0438/10 - 3.5.06

D E C I S I O N
de la Chambre de recours technique 3.5.06
du 22 novembre 2013

Requérant : (Opposant)	GIESECKE & DEVRIENT GmbH Prinzregentenstrasse 159 D-81677 München (DE)
Mandataire :	Niedermeier, Peter Giesecke & Devrient GmbH Patent- und Lizenzabteilung Prinzregentenstrasse 159 81677 München (DE)
Intimé : (Titulaire du brevet)	STMicroelectronics S.A. 29, Boulevard Romain Rolland 92120 Montrouge (FR)
Mandataire :	de Beaumont, Michel Cabinet Michel de Beaumont 1, rue Champollion 38000 Grenoble (FR)
Décision attaquée :	**Décision de la division d'opposition de l'Office européen des brevets postée le 29 décembre 2009 par laquelle l'opposition formée à l'égard du brevet européen n° 1399807 a été rejetée conformément aux dispositions de l'article 101(2) CBE.**

Composition de la Chambre :

Présidente : M. Tardo-Dino
Membres : M. Müller
A. Teale

Exposé des faits et conclusions

I. L'opposante a formé recours contre la décision de la division d'opposition, postée le 29 décembre 2009, rejetant l'opposition et maintenant le brevet litigieux no. 1399807 comme délivré.

II. L'acte de recours a été reçu le 26 février 2010 et la taxe de recours a été acquittée le même jour. Le mémoire exposant les motifs du recours a été reçu le 3 mai 2010. La requérante demande l'annulation de la décision attaquée et la révocation du brevet pour défaut d'activité inventive (articles 100 (a) et 56 CBE 1973) au vu des documents suivants:

D1: WO 98/52319 A1
D2: WO 99/35782 A1

III. Le motif d'opposition fondé sur l'article 100 (a) CBE 1973 selon lequel le brevet allait au-delà du contenu de l'objet de la demande telle que déposée (article 123 (2) CBE) n'a pas été maintenu par la requérante.

IV. L'intimée-titulaire requiert le rejet du recours et le maintien du brevet.

V. Une citation à une procédure orale a été envoyée par la chambre le 30 juillet 2013. En annexe à la citation, la chambre a communiqué ses observations concernant la question de l'activité inventive eu égard aux documents D1 et D2.

VI. La procédure orale s'est tenue le 22 novembre 2013, au cours de laquelle les requêtes des parties n'ont pas changé.

VII. La revendication 1 du brevet s'énonce comme suit:

"Procédé de brouillage dans un circuit électronique au moyen d'une quantité aléatoire, (r), d'un calcul mettant en oeuvre au moins une opération arithmétique modulaire faisant intervenir au moins une donnée secrète (s) (3), dans lequel:

un premier modulo (n) est multiplié par ladite quantité aléatoire (r);

le résultat (m) de cette multiplication est pris comme modulo de ladite opération arithmétique modulaire; et une réduction modulaire du résultat de ladite opération arithmétique modulaire est effectuée sur la base du premier modulo (n),

caractérisé en ce que ladite quantité aléatoire (r) est effacée dès que ladite multiplication par le premier modulo, (n) est terminée."

VIII. A l'issue de la procédure orale, la présidente a prononcé la décision de la chambre.

Motifs de la décision

1. Le brevet en général concerne des processus numériques d'authentification ou d'identification et, dans ce con-

texte, des calculs qui prennent en compte une donnée secrète, par exemple une clé dans une méthode cryptographique.

1.1 Afin de détecter cette donnée secrète, il est connu que les pirates peuvent utiliser des attaques dites par "canaux auxiliaires", soit des attaques par analyse de la consommation directe ou statistique (voir le brevet, paragraphe 2) soit des attaques temporelles. En observant le comportement d'un processeur qui conduit un calcul sur un paramètre connu (ou "visible") il est possible d'obtenir des informations qui aident à déterminer la valeur secrète utilisée dans le calcul.

1.2 Comme défense contre de telles attaques il est connu de faire intervenir des quantités aléatoires dans un calcul afin de rendre indépendantes les données visibles des données traitées (voir le brevet, paragraphe 3). On exécute le calcul sur des données visibles modifiées par des quantités aléatoires, on obtient un résultat aussi modifié et on arrive au résultat propre du résultat modifié. Cette façon de modifier un calcul afin de le protéger s'appelle une masquage ou une brouillage du calcul.

2. L'objectif principal de l'invention est la protection de la donnée secrète contre des attaques par des canaux auxiliaires (voir le brevet, paragraphe 2). Toutefois les revendications du brevet ne mettent pas l'accent sur des attaques par analyse de la consommation.

2.1 La solution selon la revendication 1 du brevet est un "procédé de brouillage" qui modifie un "calcul mettant en œuvre au moins une opération arithmétique modulaire

faisant intervenir au moins une donnée sécrète (s)" (voir le préambule de la revendication 1). Bien que le reste de la revendication 1 ne mentionne plus cette donnée secrète *s*, la description donne l'exemple d'une opération de forme A'^{s} *modulo n* (paragraphe 7). Selon le procédé le "premier modulo (n)" est multiplié par une "quantité aléatoire (r)" et le résultat, c'est à dire *n*r*, est utilisé au lieu de *n* comme modulo de ladite opération. Le résultat est réduit par le premier modulo *n* afin de compléter l'opération modulaire originale.

2.2 En outre, le procédé selon la revendication 1 est caractérisé en ce que la quantité aléatoire r est effacée dès que la multiplication *n*r* est effectuée.

3. Les parties conviennent que D1 représente l'art antérieur le plus proche.

3.1 D1 vise à améliorer la protection des méthodes du chiffrement à clé publique contre des attaques par canaux auxiliaires, en particulier attaques temporelles et attaques par injection de fautes.

3.2 D1 présente deux techniques: La "première technique" est conçue de façon à protéger des méthodes qui n'utilisent pas le théorème des restes chinois (CRT) contre des attaques temporelles, et la "seconde technique" vise à protéger des méthodes qui utilisent le CRT contre des attaques temporelles et des attaques par injection de fautes (voir page 9, lignes 3 à 5; page 10, lignes 5 à 10; page 12, lignes 2 à 4; et fig. 1 et 2). Le CRT permet d'accélérer des opérations modulaires à condition que le modulo soit composite *n=p*q* (voir D1,

page 5, ligne dernière à page 6, ligne 4) ce qui est le cas, par exemple, dans la méthode RSA.

3.3 La seconde technique, illustrée dans la figure 2, a deux parties. La première partie (no. 26-30) représente un procédé de brouillage selon les étapes du préambule de la revendication 1 du brevet et met en œuvre la protection contre des attaques temporelles. La deuxième partie (no. 32-36), en effectuant le calcul d'une quantité de deux manières différentes (voir no. 32) et en vérifiant que les résultats sont égaux, met en œuvre la protection contre des attaques par injection de fautes (voir page 9, lignes 3-6).

4. La requérante et l'intimée sont d'accord que la différence entre l'objet de la revendication 1 et la seconde technique selon D1 est la caractéristique d'effacement (voir le point 2.2). Ils reconnaissent aussi tous les deux que cette différence renforce la sécurité de cette technique en rendant plus difficile le piratage de la donnée secrète *s* intervenant dans le calcul (voir le brevet, paragraphe 28).

5. Par rapport à D1 cette caractéristique exige que la quantité aléatoire j soit effacée entre les étapes 26 et 28 de la seconde technique. Cette interprétation a été donnée dans l'annexe à la citation (point 5.3) et n'a pas été contestée par les parties.

5.1 L'intimée fait valoir que selon la seconde technique comme décrite et illustrée dans la figure 2 de D1 la quantité aléatoire doit être conservée pour être réutilisée dans d'autres calculs (voir réponse de l'intimée du 10 novembre 2013, page 2, dernier alinéa, à page 3, premier alinéa).

5.2 En soi, cette observation est juste et la requérante ne l'a pas mise en doute. Elle implique que dans le contexte de la seconde technique complète, c'est-à-dire comprenant toutes les deux parties, il est impossible d'effacer la quantité aléatoire dès que la multiplication selon l'étape no. 26 est effectuée.

5.3 Par conséquent, selon l'intimée, l'intégration d'un effacement comme revendiqué n'est pas évident si l'homme du métier n'a pas de raison l'incitant à séparer les deux parties de la seconde technique.

6. La requérante soutient que l'homme du métier qui, partant du document D1 ne voulait qu'augmenter la protection contre des attaques temporelles, noterait qu'il n'aurait pas besoin des étapes après 30 (voir motifs de recours, page 3, l'avant dernier alinéa).

6.1 L'argument de l'intimée est que l'homme du métier, ayant seulement besoin d'une protection contre des attaques temporelles (timing attacks), utiliserait exclusivement la première technique selon D1 qui est destinée à ce type d'attaques. Pendant la procédure orale, l'intimée a ajouté que la première technique est applicable aux méthodes CRT aussi bien qu'aux méthodes non-CRT.

6.2 L'intimée fait aussi valoir que l'homme du métier ne fait pas preuve d'esprit inventif. Donc, dès lors que D1 ne contient aucune indication que les deux parties pouvaient ou devaient être séparées, l'homme du métier prendrait l'enseignement de D1 en tant que tel et ne considérerait pas de les envisager séparées.

6.3 L'intimée ajoute que "le test final ... est justement l'objet principal de [la seconde technique selon] D1, à

savoir détecter une erreur suite à des attaques temporelles ou par injection de fautes" dans la même méthode, ce qui dissuaderait l'homme du métier de séparer les deux parties de cette méthode (réponse de l'intimée du 10 novembre 2010, page 3, paragraphe 2).

7. La requérante indique que l'application du CRT est bien connue pour accélérer l'exécution d'une opération modulaire. Comme l'explique D1 (page 5, dernière ligne - page 6, ligne 4), si le modulo *n* est égal au produit *p*q* on peut évaluer un terme de forme $x^d \ mod \ n$ environ 4 fois plus vite en évaluant séparément des termes $x^d \ mod \ p$ et $x^d \ mod \ q$ et en combinant les résultats au moyen de CRT.

7.1 Même si la première technique est applicable aux méthodes CRT aussi, l'homme du métier serait conscient que la seconde technique est plus efficace que la première.

7.2 L'homme du métier donc, partant de la seconde technique et visant à la protection contre seulement des attaques temporelles, n'abandonnerait pas forcément la seconde technique pour s'en tenir à la première technique. Plutôt il ne voudrait pas renoncer à l'efficacité de la seconde technique et donc n'hésiterait pas à supprimer les opérations tournées exclusivement vers des attaques par injection de fautes, c'est-à-dire les étapes 32, 34 et 36.

8. L'intimée fait valoir que cet argument suppose que l'homme du métier résoudrait un problème d'efficacité en sus du problème technique objectif résolu par la revendication 1 vis-à-vis de D1, lequel est un problème de sécurité.

9. La chambre accepte que l'effacement de la quantité aléatoire en soi s'adresse à un problème de sécurité et que, dans le contexte de la seconde technique de D1, viennent s'ajouter des considérations d'efficacité de la part de l'homme du métier.

9.1 Cependant, la chambre n'en conclut pas à une substitution du problème du seul fait que l'homme du métier, désireux de réaliser une méthode de protection contre les attaques temporelles encore plus sûre, aurait aussi envisagé de la réaliser de la façon la plus efficace possible, le souci d'efficacité animant généralement l'homme du métier lorsqu'il s'agit de considérer un algorithme.

9.2 Ainsi que l'a soutenu la requérante l'homme du métier, ayant à résoudre ce problème de sécurité, ne se serait pas arrêté à la première technique dans D1 parce qu'elle s'adressait uniquement aux attaques temporelles et aurait ignoré la deuxième simplement parce que, outre les attaques temporelles, elle s'occupait aussi des attaques par injection de fautes. La chambre estime irréaliste de penser que l'homme du métier n'aurait pas cherché à comprendre cette seconde technique qui traitait aussi des attaques temporelles dans un contexte de plus grande efficacité. L'homme du métier se rendrait alors compte que les deux parties de la seconde technique pouvaient être séparées et, pour des raisons d'efficacité, supprimerait la seconde partie pour réduire le temps de calcul nécessaire pour la protection des attaques temporelles.

10. S'agissant de l'effacement, la requérante indique que la description du brevet ne définit pas cette opération en détail, et fait valoir qu'en général il est connu que des quantités aléatoires utilisées dans des opéra-

tions cryptographiques soient effacées dès qu'elles ne sont plus nécessaires (voir motifs de recours, page 3, alinéas 5 et 6). Dans la procédure orale la requérante a ajouté que ce fait était bien connu dans la domaine de la cryptographie, ce qui était divulgué, par exemple, dans le "Handbook of Applied Cryptography" auquel il est fait référence dans le brevet lui-même (paragraphe 34).

10.1 L'intimée réfute cet argument, et fait valoir qu'aucun document n'a été cité lors de la recherche ni par la requérante elle-même pendant toutes les procédures d'opposition ou de recours et suggère qu'un nouveau document ne devrait pas introduit si tardivement.

10.2 La chambre est certes d'accord avec l'intimée et a décidé à ne pas admettre le document offert pendant la procédure orale qui aurait déjà dû être produit devant la division d'opposition ou, au plus tard, avec le mémoire de recours.

10.3 Cependant, la chambre doit reconnaître que cet effacement tel que revendiqué, à savoir sans que ne soit précisé un quelconque mode particulier de sa mise en oeuvre d'où pourrait découler une activité inventive, n'est rien de plus qu'un simple principe général de sécurité, selon lequel il est recommandé d'effacer des secrets dès que possible. Ce principe dans sa généralité n'a besoin d'aucune preuve écrite. Il n'est, par conséquent, pas nécessaire de rechercher si D2 divulgue, ou non, spécifiquement l'effacement des secrets dans le contexte de la cryptographie.

10.4 La sécurité d'un procédé de brouillage dépend, entre autres, du fait que la quantité aléatoire avec laquelle le modulo est modifié reste secrète. Dans ce contexte

la requérante a argué de ce que la modification du modulo dans le procédé de brouillage revendiqué est une forme de cryptage dans laquelle la quantité aléatoire correspond à la clé. Même si, comme l'intimée l'a fait valoir, cette quantité n'est pas une clé cryptographique proprement dite et diffère donc de la valeur secrète comme référé dans la revendication 1 du brevet, la quantité aléatoire est un secret dans un sens plus large qui doit être gardé secret (voir aussi paragraphe 1 du brevet: "clé ou donnée secrète").

10.5 Pour cette raison la chambre considère évident pour l'homme du métier d'effacer la quantité aléatoire dès que possible: Dans la seconde technique ce moment est, ce en quoi les deux parties sont d'accord, après l'étape no. 26, c'est-à-dire dès que la multiplication *j*p* est terminée.

11. La chambre conclut donc que l'objet de la revendication 1 du brevet manque d'activité inventive en vue du document D1 et des connaissances communes de l'homme du métier. La seule requête de l'intimée étant le maintien du brevet sans modification, il suit de ce qui précède que la décision objet du recours doit être annulée et le brevet révoqué.

Dispositif

Par ces motifs, il est statué comme suit

1. La décision objet du recours est annulée.
2. Le brevet est révoqué.

Le Greffier : La Présidente :

B. Atienza Vivancos M. Tardo-Dino

Décision authentifiée électroniquement