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

Liste des données pour la décision du 28 mai 2013

N° du recours : T 0390/09 - 3.5.05

N° de la demande : 02703661.5

N° de la publication : 1358733

C.I.B. : H04L9/06

Langue de la procédure : FR

Titre de l'invention :
Procédé sécurisé de calcul cryptographique à clé secrète et composant mettant en œuvre un tel procédé

Titulaire du brevet :
STMicroelectronics SA

Opposant :
Giesecke & Devrient GmbH

Référence :
Masquage de clés/STM

Normes juridiques appliquées :
CBE 1973 Art. 56

Mot-clé :
Activité inventive - requête principale (oui)

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 0390/09 - 3.5.05

D E C I S I O N
de la Chambre de recours technique 3.5.05
du 28 mai 2013

Requérante I : (Opposante)	Giesecke & Devrient GmbH Prinzregentenstrasse 159 81677 München (DE)
Requérante II: **(Titulaire du brevet)**	STMicroelectronics SA 29, Boulevard Romain Rolland 92120 Montrouge (FR)
Mandataire	Zapalowicz, Francis Casalonga & Partners Bayerstrasse 71/73 80335 München (DE)

Décision attaquée : **Décision intermédiaire de la division d'opposition de l'office européen des brevets postée le 26 novembre 2008 concernant le maintien du brevet européen No. 1358733 dans une forme modifiée.**

Composition de la Chambre :

Présidente : A. Ritzka
Membres : K. Bengi-Akyuerek
G. Weiss

Exposé des faits et conclusions

I. Les présents recours de la requérante I (l'opposante) et la requérante II (la titulaire) sont formés contre la décision intermédiaire de la division d'opposition, postée le 26 novembre 2008, de maintenir le brevet litigieux No. 1358733 tel qu'il a été modifié selon une deuxième requête subsidiaire en tenant compte des motifs d'opposition invoqués par l'opposante (article 100 a), ensemble articles 54 et 56 CBE 1973).

II. La décision attaquée avait fait référence *inter alia* aux documents suivants:

D2: WO-A-99/48239;
D3: DE-A-198 22 217.

III. L'acte de recours de la requérante I a été reçu le 26 janvier 2009 et la taxe de recours a été acquittée le même jour. Le mémoire exposant les motifs du recours a été reçu le 24 mars 2009. La requérante I a demandé l'annulation de la décision attaquée et la révocation du brevet, d'une part, pour défaut d'activité inventive (article 56 CBE 1973) au vu de D2 et/ou D3 et, d'autre part, l'objet de la revendication 1 de la deuxième requête subsidiaire allant au-delà du contenu de l'objet de la demande telle que déposée (article 123(2) CBE). En outre, à titre subsidiaire, elle a demandé la tenue d'une procédure orale.

IV. L'acte de recours de la requérante II a été reçu le 2 février 2009 et la taxe de recours a été acquittée le 30 janvier 2009. Le mémoire exposant les motifs du recours a été reçu le 3 avril 2009. La requérante II a demandé l'annulation de la décision attaquée et, à titre de requête principale, le maintien du brevet

litigieux sur la base du jeu de revendications tel que délivré ou, à titre de première requête subsidiaire, sur la base d'un jeu de revendications modifiées déposé avec le mémoire exposant les motifs du recours. En outre, subsidiairement, elle a demandé la tenue d'une procédure orale.

V. Par lettre en date du 30 juillet 2009, la requérante II a soumis ses observations au mémoire exposant les motifs du recours de la requérante I et a déposé des nouveaux jeux de revendications modifiées en tant que première à septième requêtes subsidiaires.

VI. Une citation à une procédure orale devant avoir lieu le 28 mai 2013 a été envoyée par la chambre le 21 décembre 2012. En annexe à la citation selon l'article 15(1) RPCR, la chambre a communiqué ses observations concernant l'article 123(2) CBE, l'article 84 CBE 1973 et la question de la nouveauté et l'activité inventive (article 52(1) CBE) eu égard aux documents D2 et D3.

VII. Par lettre en date du 16 avril 2013, la requérante II a déposé des revendications modifiées à titre de requêtes subsidiaires 4A à 7A, en réponse à la notification selon l'article 15(1) RPCR de la chambre quant à l'article 123(2) CBE et à l'article 84 CBE 1973.

VIII. La procédure orale s'est tenue le 28 mai 2013, au cours de laquelle seule la requête principale a été discutée. Concernant les requêtes finales des parties, la requérante I a demandé l'annulation de la décision attaquée et la révocation du brevet alors que la requérante II a demandé l'annulation de la décision attaquée et le maintien du brevet, à titre principal, sur la base du jeu de revendications tel que délivré

ou, à titre subsidiaire, sur la base des jeux de revendications déposés par lettres en date du 30 juillet 2009 et du 16 avril 2013 en tant que requêtes subsidiaires 1 à 4, 4A, 5, 5A, 6, 6A , 7 et 7A. A la fin de la procédure orale, la décision de la chambre a été prononcée.

IX. La revendication 1 selon la requête principale s'énonce comme suit:

"Procédé sécurisé de calcul cryptographique pour fournir une donnée de sortie (MS) à partir d'une donnée d'entrée (ME) et d'une clé secrète (K_0), le procédé comprenant plusieurs étapes de calcul de clé (ET2), chacune fournissant une clé dérivée actualisée (M'_1, M'_i) à partir d'une clé dérivée précédemment calculée (M'_{i-1}) par l'étape de calcul de clé précédente selon une loi de calcul de clé connue, une première clé dérivée actualisée (M'_1) étant obtenue à partir de la clé secrète (K_0),

le procédé étant caractérisé en ce qu'il comprend également une seule étape de masquage (ET1), effectuée avant la première étape de calcul de clé (ET2), pour masquer la clé secrète (K_0) de sorte que chaque clé dérivée actualisée (M'_1, M'_i) soit différente à chaque mise en œuvre du procédé."

Motifs de la décision

1. Recevabilité des recours

Les recours satisfont aux exigences des articles 106 à 108 CBE et de la règle 99 CBE (voir points III et IV

ci-dessus). Les recours sont donc recevables.

2. REQUÊTE PRINCIPALE

Cette requête est identique à la requête principale traitée dans la décision attaquée et correspond au jeu de revendications tel que délivré.

2.1 Article 52(1) CBE: nouveauté et activité inventive

La chambre juge que la revendication 1 de cette requête satisfait aux exigences de l'article 52(1) CBE pour les raisons suivantes.

2.1.1 La chambre partage l'avis de la division d'opposition selon lequel le document D2 est considéré comme l'état de la technique le plus proche, parce que D2 appartient au même domaine technique et vise à atteindre le même objectif que l'invention, c'est-à-dire la sécurisation des données chiffrées contre des attaques de type "Simple Power Attack" (SPA) où un fraudeur essaie d'obtenir des informations secrètes à partir de la détection des signaux électromagnétiques lors de l'opération d'un procédé cryptographique.

2.1.2 En utilisant la terminologie de la revendication 1, D2 divulgue un procédé sécurisé de calcul cryptographique (voir page 2, lignes 25-28 et l'unique figure), pour fournir une donnée de sortie ("information chiffrée C") à partir d'une donnée d'entrée ("bloc message M") et d'une clé secrète permutée ("K2"). Le procédé cryptographique de type DES (Data Encryption Standard) selon le mode de réalisation général a lui-aussi plusieurs étapes de calcul de clé (voir page 3, lignes 9-18 et l'unique figure, étapes 120, 130 et 140) qui sont exécutées au total à seize reprises selon un

"groupe d'opérations 270" (voir page 3, ligne 31 à page 4, ligne 2 et l'unique figure, bloc 270). Dans ce contexte, une première clé dérivée actualisée ("K5") est également obtenue à partir de la clé secrète permutée ("K2") par l'application d'une loi de calcul de clé connue, c'est-à-dire la "rotation 130" et la "permutation 140" (d'après l'unique figure, étapes 130 et 140). De plus, le procédé comprend une étape de masquage ("transformation aléatoire 120") réalisée pour le masquage de la clé secrète au moyen d'un nombre aléatoire (voir page 3, lignes 9-14 et l'unique figure, étape 120).

De surcroît, puisque la transformation aléatoire 120 selon une variante du mode de réalisation général enseignée dans D2 peut être utilisée comme une étape préalable aux étapes du groupe d'opérations exécutées à plusieurs reprises (voir page 5, ligne 31 à page 6, ligne 4 ainsi que la revendication 6) et, par conséquent, être effectuée avant les nombreuses étapes de calcul de clé (correspondant aux étapes 130 et 140 effectuées plusieurs fois), la chambre partage l'avis de la division d'opposition et de la requérante I que la transformation aléatoire 120 d'après une telle variante de réalisation de D2 constitue une seule étape de masquage qui est effectuée avant la première étape de calcul de clé (c'est-à-dire l'étape de rotation 130 selon D2).

2.1.3 La requérante II a argumenté à cet égard que D2 ni divulgue ni suggère un mode de réalisation qui prévoie un masquage unique d'une clé secrète, effectué avant la première ronde, puisque, selon le mode de réalisation général, la clé K2 qui est dérivée de la clé secrète initiale K1 était masquée et non pas la clé secrète K1 elle-même. La clé K2 n'était donc pas une clé secrète.

Par ailleurs, le masquage de K2 dans D2 avait lieu *après* la "permutation 110" qui était la première étape de calcul de clé selon D2 contrairement au procédé selon la revendication 1 qui spécifie que l'étape de masquage est effectuée *avant* la première étape de calcul de clé. De plus, D2 comme indiqué à la page 5, lignes 21-30 et à la revendication 6 prévoyait que l'étape de transformation aléatoire pourrait être effectuée sur les blocs messages M, M1 ou M2, c'est-à-dire sur le chemin de données, plutôt que seulement sur les clés, c'est-à-dire sur le chemin de clés (cf. mémoire exposant les motifs du recours, section III.4).

La chambre ne peut cependant pas se rallier à cette argumentation. Dans la mesure où la clé secrète selon le libellé de la revendication 1 n'est pas définie de façon plus détaillée et qu'ainsi il n'est pas indiqué si une telle clé était initialement dérivée à partir d'une autre clé ou non, la clé K2 selon D2 peut également être considérée comme couverte par le terme "clé secrète", même si elle est générée à l'aide d'une permutation de la clé K1 (voir page 3, lignes 6-8 et l'unique figure, étape 110). D'autre part, la chambre constate que, selon la revendication 1, les étapes de calcul de clé sont définies comme celles qui fournissent une clé dérivée actualisée à partir d'une clé dérivée précédemment calculée, c'est-à-dire que les étapes de calcul de clé sont exécutées à chaque ronde d'itérations, et que d'après cette définition, la permutation 110 selon D2 ne peut pas faire partie des étapes de calcul de clé et ne correspond donc pas à la première étape de calcul de clé. Ainsi, selon D2, une clé secrète K2 générée est ensuite masquée par l'étape de la transformation aléatoire. Puisqu'en plus D2 enseigne une variante du mode de réalisation général selon laquelle la transformation aléatoire au moyen

d'une unique génération d'un paramètre de masquage ("nombre aléatoire") est effectuée avant la première étape de calcul de clé (voir page 5, ligne 31 à page 6, ligne 4), D2 expose également une seule étape de masquage. En outre, la chambre considère que la seule étape de masquage de D2 ("transformation aléatoire 120") selon le mode d'emploi en question représenté par l'unique figure s'applique sans ambiguïté à la détermination de la clé masquée K3 à partir de la clé secrète K2 (correspondant au chemin de clés) au lieu du chemin de données.

2.1.4 La différence entre l'objet de la revendication 1 et le procédé selon D2 réside ainsi en ce que chacune des étapes de calcul de clé fournit une clé dérivée actualisée à partir d'une clé dérivée précédemment calculée par l'étape de calcul de clé précédente selon une loi de calcul de clé connue.

Par conséquent, l'objet de la revendication 1 de la requête principale est considéré comme nouveau par rapport à D2 (article 54 CBE 1973).

2.1.5 Concernant le problème technique objectif à résoudre par la revendication 1, la requérante II a argumenté que le problème technique était d'augmenter la protection contre les attaques de type SPA. Cependant, pour la chambre, un tel problème est considéré comme trop large. La chambre fait sienne la formulation du problème objectif retenue par la division d'opposition dans la décision attaquée (cf. section II.3.d.iii) et par la requérante I (cf. mémoire exposant les motifs du recours de la requérante I, page 5, dernière ligne), selon laquelle le problème technique objectif est de déterminer la clé dérivée au début de chaque ronde d'itérations des étapes de calcul de clé

correspondantes.

2.1.6 D'après le raisonnement de la division d'opposition sur lequel la requérante I a basé son argumentation à la procédure orale devant la chambre, l'homme du métier chercherait des possibilités pour la détermination itérative de la clé K3 à partir de l'enseignement de D2 qui ne dit rien sur la relation entre la clé générée K5 de la ronde précédente et la clé K3 au début de la ronde suivante. Pour l'homme du métier, les interprétations possibles concernant la détermination de K3 au début de chaque ronde sont que (i) la clé K3 prend, à chaque ronde, la même valeur ou (ii) que K3 prend la valeur donnée par K5 de la ronde précédente. Dans la mesure où l'emploi d'une même valeur de K3 à chaque ronde selon la possibilité (i) n'est pas efficace en termes de sécurité, ces considérations inciteraient l'homme du métier à choisir la possibilité (ii) afin de mettre la valeur de K3 à jour comme il le connaît du procédé cryptographique de type DES. Par conséquent, l'homme du métier parviendrait à l'objet de la revendication 1 sans appliquer une activité inventive (cf. décision attaquée, sections II.3.d.iv, II.4.e, II.4.f).

Cependant, la chambre ne peut pas suivre ce raisonnement qui est basé sur des considérations *ex post facto*. D'après le mode de réalisation général de D2, seuls les blocs messages M1 et M2 de la ronde actuelle sont dérivés des blocs messages R5 et M1 de la ronde précédente dans un cycle d'exécution d'opérations (voir page 3, ligne 31 à page 4, ligne 2 et l'unique figure, étape 260), c'est-à-dire après chaque ronde de seize rondes en tout du groupe d'opérations 270 représenté par une ligne hachurée dans l'unique figure de D2. Puisque D2 - comme correctement constaté dans la

décision attaquée - n'indique rien sur la relation entre les clés correspondantes des rondes successives, cela signifie, d'après la chambre, que la clé générée K5 dans la ronde actuelle dépend certes de la clé secrète masquée K3 de cette ronde, mais que D2 ne contient aucune indication que K5 pourrait dépendre ou être dérivable de la clé K5 déterminée dans la dernière ronde. Cela n'est de toute façon pas nécessaire en ce cas, car un masquage de la clé secrète K2 par la transformation aléatoire 120 afin d'améliorer la sécurité du système en question a déjà été effectué dans D2.

Ainsi, au cas où l'homme du métier prendrait comme point de départ ladite variante du mode de réalisation général, la clé secrète masquée K3 serait calculée seulement une fois, à savoir au début de chaque cycle et ensuite resterait constante dans le cadre des quinze rondes suivantes. Concernant la clé dérivée K5, cela impliquerait aussi que K5 serait dérivée de la même clé K3 dans chaque ronde d'un cycle de seize rondes au moyen d'une rotation 130 et d'une permutation 140 prédéterminée. Afin de résoudre le problème technique mentionné ci-dessus, l'homme du métier ne déterminerait dans ce cas qu'une fois la clé K5 à partir de la clé K3 par l'application de la loi de calcul connue (c'est-à-dire la rotation 130 et la permutation 140 selon D2) et l'utiliserait ensuite également dans les rondes suivantes sans modifications. Il assurerait ainsi le stockage de la clé K5 qui a été déterminée lors de la première ronde en empêchant l'exécution d'étapes superflues, afin d'utiliser la même clé K5 dans les quinze rondes suivantes du cycle correspondant au lieu de calculer itérativement la clé K5 dans la ronde actuelle à partir de la clé K5 des rondes précédentes. L'homme du métier parviendrait donc à une solution

différente de celle de la revendication 1 à partir du mode de réalisation de D2 en question parce que l'enseignement de D2 l'éloignerait de l'objet revendiqué.

Aussi, l'indication de l'utilisation d'un algorithme cryptographique de type DES dans D2 n'entraînerait pas l'homme du métier vers un autre mode de réalisation, car soit le mode d'emploi général soit le mode d'emploi varié sont déjà basés sur des opérations de calcul de type DES (voir page 2, lignes 25-28 et page 5, lignes 13-15). Par ailleurs, l'homme du métier n'aurait aucune incitation à étendre l'enseignement de D2 à l'exécution des étapes de calcul de clé itératives en utilisant des nombres aléatoires distincts pour le masquage, du fait que la minimisation du nombre des nombres aléatoires générés est indiquée comme un avantage particulier dans le cas d'une carte à puce selon D2 (voir page 6, lignes 4-7).

2.1.7 D'autre part, la chambre est d'avis que le document D3, soit considéré isolément soit pris en considération avec D2, ne peut pas rendre évident l'objet de la revendication 1 pour l'homme du métier dans le domaine de la cryptographie. Bien que D3 vise également à combattre des attaques de type SPA (voir colonne 1, lignes 55 à 64 et colonne 3, lignes 44-48) et bien que le procédé décrit utilise aussi des clés secrètes masquées (voir colonne 4, lignes 55-64 et la figure 4), un concept fonctionnel distinct est retenu dans ce document. D'après le procédé sécurisé selon D3, en effet, les clés secrètes ("K1","K2","K3") ainsi que des paramètres de masquage ("Z1","Z2","Z3") ne sont pas actualisés itérativement et, de ce fait, les paramètres de masquage ne contribuent donc pas à l'actualisation itérative des clés respectives dans le sens de la

caractéristique distinctive indiquée au point 2.1.4 ci-dessus. Une étape de masquage unique exécutée avant les étapes de calcul de clés itératives n'est pas prévu dans le procédé de D3. De plus, selon D3, seules les données destinées à être sécurisées subissent des étapes successives de calcul et de masquage par des fonctions linéaire et non linéaire ("f", "g"), des clés secrètes diverses et des paramètres de masquage au lieu de prévoir l'application des chemins de calcul séparés pour l'actualisation itérative des clés et des données selon la revendication 1.

Par conséquent, l'homme du métier ne prendrait pas en considération l'enseignement de D3 pour améliorer le procédé sécurisé selon D2 et résoudre le problème technique posé sans faire preuve d'activité inventive.

2.1.8 Concernant la question de l'activité inventive et, plus particulièrement, la caractéristique distinctive mentionnée au point 2.1.4 ci-dessus, la requérante I a déclaré durant la procédure orale qu'elle suivait le raisonnement retenu par la division d'opposition.

2.1.9 Au vu de ce qui précède, l'objet de la revendication 1, laquelle est la seule revendication indépendante de la requête principale, implique une activité inventive au regard de D2 et/ou D3. La requérante I n'a pas fait référence aux autres documents pour l'appréciation de la nouveauté et l'activité inventive ni dans le mémoire exposant les motifs du recours (voir section I) ni durant la procédure orale.

3. Pour ces motifs, la chambre a jugé qu'il n'y a aucune raison de ne pas maintenir le brevet comme délivré selon la requête principale. Dans ces conditions, il n'y a pas lieu de considérer plus avant les requêtes

subsidiaires de la requérante II.

Dispositif

Par ces motifs, il est statué comme suit

1. La décision attaquée est annulée.

2. Le brevet est maintenu sans modifications.

La Greffière : La Présidente :

L. Fernández Gómez A. Ritzka

Décision authentifiée électroniquement