Code de distribution interne:
(A) [ ] Publication au JO
(B) [ ] Aux Présidents et Membres
(C) [X] Aux Présidents

D E C I S I O N
du 2 février 1994

N° de recours: T 0578/92 - 3.4.1

N° de la demande: 89400083.5

N° de la publication: 0325506

IPC: G07F 7/10

Langue de la procédure: FR

Titre de l'invention:
Système de sécurité pour protéger des zones de programmation d'une carte à puce

Demandeur:
SGS-Thomson Microelectronics S.A.

Opposant:
-

Référence:
Cartes à microplaquettes

Normes juridiques relevantes:
CBE Art. 56

Mot-clé:
"Activité inventive (déniée)"

Décisions citées:
T 15/81

Exergue:

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

N°. du recours : T 0578/92 - 3.4.1

D E C I S I O N
de la Chambre de recours technique 3.4.1
du 2 février 1994

Requérant : SGS-Thomson Microelectronics S.A.
7, Avenue Galliéni
F - 94250 Gentilly (FR)

Mandataire : C. Schmit
Cabinet Ballot-Schmit
7, rue le Sueur
F - 75116 Paris (FR)

Décision attaquée : **Décision de la division d'examen 063 de l'Office européen des brevets du 25 février 1992 par laquelle la demande de brevet n° 89400083.5 a été rejetée conformément aux dispositions de l'article 97(1) CBE.**

Composition de la Chambre :

Président : G.D. Paterson
Membres : Y. van Henden
U. Himmler

Exposé des faits et conclusions

I. La demande de brevet européen n° 89 400 083.5, publiée sous le n° 0 325 506, a été rejetée par décision de la division d'examen.

Le rejet a été prononcé au motif que, vu l'état de la technique ressortant des documents
D1 : US-A-4 105 156, et
D2 : WO-A-86/04170,
l'objet de nouvelles revendications 1 à 8 reçues avec lettre de la demanderesse en date du 14 novembre 1991 n'impliquait pas d'activité inventive.

II. La demanderesse a formé un recours contre la décision de la division d'examen et, avec le mémoire en exposant les motifs, a remis un nouveau jeu de cinq revendications.

La première de ces revendications s'énonce comme suit :

"Système de sécurité (A, B) pour protéger des zones (3) mémoires programmables d'une carte (2) à puce (1), ce système comportant un verrou logique (4), ouvert avant la programmation des dites zones mémoires, et qu'on peut fermer après cette programmation, comportant
- une clef (7) d'accès en programmation,
- dans la carte, une fonction (10) de programmation protégée par cette clef d'accès en programmation,
- dans la carte des moyens (10) pour recevoir la clef de programmation et pour ensuite permettre la programmation de ces zones (3) de la mémoire de la carte,
- cette clef étant chiffrée (13) par des moyens (11) de chiffrage et étant stockée sous forme chiffrée dans la carte,

- ce système comporte,
  un dispositif (14) de chiffrement de la clef d'accès en programmation pour introduire une clef chiffrée dans la carte,
- des moyens pour invalider définitivement (20) la carte lorsqu'une fausse clef d'accès en programmation lui est introduite,

caractérisé en ce que

- la fonction clef d'accès en programmation comporte des moyens pour n'autoriser qu'une seule fois la lecture ou la présentation de la clef de programmation chiffrée dans la carte",

une faute d'accord affectant le participe "introduite" étant ici corrigée. Les revendications 2 à 5 sont rattachées à la première.

III. A la fin du mémoire exposant les motifs de son recours, la requérante exprime l'avis que "la décision de rejet devrait être réformée pour délivrer un brevet sur cette base" - autrement dit : sur la base des nouvelles revendications 1 à 5 ci-dessus mentionnées. A l'appui de cette requête, elle a en substance fait valoir ce qui suit :

Le verrou logique dont il est question dans (D1) n'est fermé qu'après la programmation de la mémoire, et non avant ladite programmation si la comparaison des clefs aboutit à un échec. Selon (D2), les zones mémoires de la puce peuvent être programmées si la comparaison des clefs donne un résultat positif et, dans le cas opposé, la carte est invalidée. Si une tentative de fraude est infructueuse, la carte devient donc inutilisable et, pour cette raison, il est estimé que l'envoi chiffré de la clef de programmation suffit en soi et rend un verrou superflu. Néanmoins, et bien que ses chances de succès

soient réduites, l'utilisateur final peut encore programmer la mémoire s'il a correctement présenté la clef d'accès. En effet, ce n'est qu'après stockage de la dernière donnée qu'est détruite la porte de sortie (21) de la mémoire (13).

L'invention écarte au contraire ce risque du fait qu'on ne peut qu'une seule fois présenter la clef de programmation. En outre, elle se distingue aussi de la combinaison des enseignements de (D1) et (D2) en ce qu'on ne se préoccupe ni de savoir si la puce a ou non été programmée, ce que préconise (D1), ni de savoir si la comparaison a été réussie ou pas - cf. (D2). La présentation de la clef de programmation conduit donc au même niveau de sécurité que l'exécution consécutive des opérations respectivement décrites dans (D1) et (D2). Enfin, il est à noter que ces documents ne rendent pas évident le problème technique résolu par l'invention. En particulier, alors que l'initialisation prévue selon (D1) peut être effectuée en plusieurs étapes, et même recommencée, la présentation unique de la clef n'est pas contournable.

IV. Les arguments opposés par la division d'examen et dont la pertinence n'est pas affectée par les modifications de la revendication principale se résument pour l'essentiel comme indiqué ci-dessous.

Du document (D1) est connu un système de sécurité pour protéger des zones mémoires programmables d'une carte à puce, lequel système comporte : un verrou logique, ouvert avant la programmation desdites zones mémoires et qu'on peut fermer après cette programmation ; une clef d'accès en programmation, spécifique à chaque carte ; dans la carte, une fonction clef d'accès en programmation comportant des moyens (21) qui sont détruits après la

programmation des zones mémoires et, de ce fait, n'autorisent qu'un seul usage de la clef de programmation stockée dans la mémoire ; dans la carte également, une fonction de programmation protégée par cette clef ainsi que des moyens pour recevoir cette dernière et pour ensuite permettre la programmation des susdites zones de la mémoire ; enfin, des moyens pour définitivement invalider la carte lorsqu'une fausse clef d'accès en programmation lui est appliquée un nombre prédéterminé de fois. Le système revendiqué s'en distingue en ce que la clef d'accès en programmation est chiffrée par des moyens de chiffrage (11) et stockée sous sa forme chiffrée dans la carte, et en ce qu'il comporte un dispositif de chiffrement (14) de la clef de programmation pour introduire une clef chiffrée dans la carte, ainsi que des moyens pour invalider définitivement la carte lorsqu'une fausse clef d'accès en programmation est introduite.

Le problème que l'invention vise à résoudre est d'augmenter la sécurité des systèmes connus en ce qui concerne la programmation des zones mémoires. Il ne s'agit cependant là que d'une préoccupation permanente de l'homme du métier.

Suivant le système auquel a trait (D2), une clef de programmation est inscrite dans une mémoire de la carte chez le fabricant, laquelle clef est chiffrée en fonction d'un numéro de fabrication inscrit sur la carte. Chez l'utilisateur, il est procédé à un second chiffrement et l'on vérifie que le résultat de cette opération est conforme à celui mémorisé dans la carte. Pour l'homme du métier partant du système connu de (D1) et s'appliquant à en améliorer la sécurité, il est donc évident de prévoir, extérieurement à la carte, des moyens de chiffrage chez le fabricant et des moyens identiques chez l'utilisateur qui programme la carte. Enfin, il est tout aussi évident

d'invalider la carte dès la première tentative erronée de programmation.

Motifs de la décision

1. Selon le préambule de la demande de brevet européen, la présente invention aurait pour objet de mettre à la disposition des domaines autres que celui de la banque des cartes à microplaquettes à fonctionnalité différente - voir colonne 1, lignes 19 à 25.

Bien que l'invention à laquelle se rapporte le document (D1) soit essentiellement décrite en relation avec des applications bancaires, il n'en demeure pas moins que ladite invention s'adresse également à d'autres domaines. Ceci ressort de la revendication indépendante 22, où aucun domaine d'application n'est désigné, ainsi que des alternatives dont la revendication 1 fait état - noter également la présence de la locution adverbiale "*in particular*" dans la toute première phrase.

On ne saurait par suite contester la pertinence du document (D1) dans le cas présent et, de fait, la requérante s'en est abstenue. Il en va par ailleurs de même pour ce qui est du document (D2), où les revendications ne font état d'aucun domaine particulier d'application, et où une application bancaire est simplement décrite à titre d'exemple.

2. Le document (D1) a trait à un système de sécurité visant à la prévention de transactions illicites au moyen de cartes lisibles par machine et portant des données d'identification et d'utilisation - voir paragraphe introductif. Plus précisément, ces cartes sont du type

muni de circuits intégrés comportant des mémoires programmables (13-17) et une unité de traitement (10), c'est-à-dire des "cartes à microplaquettes" - voir : colonne 2, lignes 43 à 46 ; colonne 4, lignes 38 à 41 ; colonne 5, lignes 15 à 23.

La mémoire (13) est programmée via une porte (20) par une unité de programmation (19) - voir : figure 2 ; colonne 4, lignes 46 à 49 ; colonne 5, lignes 23 à 25. Elle contient un code protecteur assurant la sécurité pendant le transport du lieu de fabrication au lieu où elle doit être remise à l'utilisateur - voir colonne 5, lignes 36 à 39 - et il est par ailleurs spécifié que sa programmation est la dernière phase de la fabrication - voir colonne 5, lignes 66 à 68. Le code protecteur, élaboré par un générateur de nombre aléatoire, est en outre imprimé sur un bordereau remis séparément à l'utilisateur sous enveloppe scellée - voir de la dernière ligne de la colonne 5 à la ligne 12 de la colonne 6. Au lieu où elle doit être mise à la disposition du client par l'utilisateur, la carte est introduite dans un dispositif de codage pour l'enregistrement de données spécifiques audit client - voir colonne 6, lignes 13 à 15. A cette fin, le code numérique protecteur indiqué sur le bordereau est communiqué via un bloc d'entrée/sortie (18) à un bloc de traitement (10), lequel le compare au code enregistré dans la mémoire (13) et dont la lecture se fait par l'intermédiaire d'une porte (21). Si le résultat de la comparaison est négatif, l'auto-destruction du circuit intégré se déclenche après un nombre prédéterminé d'essais infructueux. Si ce résultat est positif, le circuit intégré transmet au dispositif de codage un signal autorisant l'entrée de données - voir colonne 6, lignes 13 à 23. Le numéro d'identification personnel du client est enregistré dans la mémoire (14) via une porte

(22), son numéro de compte est enregistré dans la mémoire (15) via une porte (23) et les conditions d'emploi le sont dans la mémoire (16) via une porte (24). Après chaque stockage de données, la porte (20, 22, 23, 24) correspondante est détruite - voir colonne 6, lignes 2 à 4 et 24 à 37 ; voir aussi colonne 6, lignes 55 à 59, d'où il ressort que, suivant le mode de réalisation décrit en relation avec la figure 3, une porte destructible (26) est également prévue pour prévenir toute modification ultérieure des données de départ contenues dans la mémoire (17). Enfin, la porte (21) autorisant la lecture du code enregistré dans la mémoire (13) est détruite après chargement de la dernière mémoire - voir colonne 6, lignes 37 à 43.

3. La porte (21) prévue selon le système connu de (D1) constitue un "verrou logique, ouvert avant la programmation des zones mémoires (13-17) et qu'on peut fermer après cette programmation". Le nombre aléatoire stocké dans la mémoire (13) est, au sens de la demande de brevet en cause, une "clef d'accès en programmation". L'unité de traitement (10) est un "moyen intérieur à la carte, recevant la clef d'accès en programmation et permettant ensuite la programmation des zones (13-17) de la mémoire de la carte". Associée à l'unité de programmation (19), cette unité de traitement remplit, "dans la carte, une fonction de programmation protégée par la clef d'accès en programmation". Enfin, lorsque la comparaison des nombres aléatoires aboutit à un résultat positif, la porte (21) fait office de "moyen pour n'autoriser qu'une seule fois la lecture de la clef de programmation dans la carte".

Le système de sécurité revendiqué par la requérante se distingue donc de celui décrit dans (D1) en ce que :

a) la clef d'accès en programmation est chiffrée par des moyens de chiffrage et stockée sous forme chiffrée dans la carte ;

b) ce système comporte un dispositif de chiffrement de la clef d'accès en programmation pour introduire une clef chiffrée dans la carte, et

c) en ce qu'il comporte des moyens pour invalider définitivement la carte lorsqu'une fausse clef d'accès en programmation lui est introduite.

Sur ce premier point, les conclusions de la Chambre rejoignent donc celles de la division d'examen, dont la requérante n'a pas mis en cause la pertinence dans le mémoire exposant les motifs de son recours.

4. Partant de l'état de la technique révélé par le document (D1), où les applications au domaine de la banque ne sont pas les seules envisagées, le problème objectif que vise à résoudre la présente invention est, comme en a jugé la division d'examen au point II.2.4 de la décision attaquée, d'augmenter la sécurité offerte en ce qui concerne la programmation des zones mémoires programmables de la carte.

Il est toutefois spécifié dans la décision antérieure T 15/81 (JO OEB 1982, 2-6) de la Chambre que, l'élimination d'inconvénients et l'apport d'améliorations constituant l'objectif constant des efforts entrepris par l'industrie, aucun caractère inventif n'est décelable dans ces buts - voir point 3 des motifs. En accord avec l'opinion exprimée par la division d'examen, la Chambre estime par suite qu'on ne saurait percevoir d'activité inventive dans la position du problème que l'invention tend objectivement à résoudre.

5. Le document (D2) concerne également la protection des mémoires programmables de cartes à circuits intégrés. Avant de remettre une carte à un organisme émetteur - c'est-à-dire à un "utilisateur" selon la terminologie adoptée dans (D1) -, le fabricant enregistre dans la mémoire programmable une clef de fabrication (F), calculée à partir du numéro de fabrication (X) de ladite carte et d'une donnée secrète (s) - voir page 4, lignes 4 à 15. A cette fin, le fabricant dispose d'un système (10) comprenant une zone de mémoire (11a) où sont enregistrés un algorithme (P) de calcul des clefs de fabrication (F) et la données secrète (s), une zone mémoire (11b) où sont enregistrés les numéros de fabrication des cartes, et des circuits de traitement (12) - voir page 4, liges 20 à 29.

Une fois cette phase de la fabrication terminée, les organismes émetteurs achètent les cartes et, avant diffusion aux utilisateurs, exécutent des opérations de personnalisation dont l'une est l'encodage de la mémoire (5) du circuit intégré - voir de la page 5, ligne 21, à la ligne 4 de la page 6. Préalablement à cette opération, il est procédé à une vérification de la clef de fabrication (F) inscrite par le fabricant - voir page 9, lignes 12 à 20. Pour ce faire, le système de personnalisation (21) dont dispose l'organisme émetteur comprend une mémoire (22) où sont enregistrés l'algorithme (P) et la données secrète (s), ainsi que des circuits de traitement (23) qui, à partir du numéro de fabrication (X) et de ladite données secrète (s), recalculent la clef de fabrication (F) conformément aux instructions de l'algorithme (P). Enfin, le résultat de ce nouveau calcul est comparé à celui inscrit par le fabricant, et la carte invalidée si les deux clefs sont différentes - voir page 9, lignes 22 à 33, et dernière clause de la revendication 14.

Le numéro de fabrication (X), comparable au nombre aléatoire dont il est question dans (D1), représente par suite une "clef non chiffrée", tandis que la clef de fabrication (F) est "chiffrée" puisque l'application de l'algorithme (P) est en soi une procédure de chiffrement.

6. Prévoir le chiffrement du nombre aléatoire constituant la clef d'accès en programmation dans le système connu de (D1) est, pour l'homme du métier cherchant à renforcer la sécurité offerte par ce système, une mesure dont le document (D2) rend l'intérêt évident. Rien ne s'oppose en outre à son inclusion dans ledit système connu de (D1). En conséquence, on ne saurait percevoir d'activité inventive dans les clauses (a) et (b) par lesquelles le système revendiqué par la requérante se distingue de celui décrit dans (D1) - cf. paragraphe II.3 de la présente décision.

Ceci étant, la Chambre partage l'avis de la division d'examen quant à l'intérêt que présente l'invalidation de la carte dès la première tentative de fraude. A l'appui de cette thèse, la Chambre fait observer que l'autorisation d'une pluralité d'échecs implicitement envisagée dans (D1) ne peut qu'être un compromis entre le risque de fraude et celui d'erreurs commises par le client lors de l'introduction dans la mémoire (14) de son code personnel d'identification. Or, l'intérêt d'une telle mesure diminue dans la même proportion que le coût de fabrication des cartes à circuits intégrés, lequel s'est considérablement réduit avec la généralisation de l'emploi de ces cartes. Enfin, la requérante a d'elle-même reconnu dans l'exposé des motifs de son recours que, selon (D2), il est aussi prévu d'invalider la carte après le premier essai de programmation frauduleux - voir première page, lignes 7 à 15 du dernier alinéa.

7. Les arguments avancés par la requérante au crédit d'une activité inventive qu'impliquerait néanmoins l'objet de la revendication 1 ne sont finalement pas de nature à convaincre la Chambre.

Il est vrai que ni (D1) ni (D2) ne divulguent de système comportant un verrou logique ayant toutes les propriétés découlant du libellé de la revendication 1. Cependant, comme le montre l'analyse développée aux points II.2 à II.5 de la présente décision, il en va bien de la sorte pour ce qui est du verrou d'un système de sécurité combinant les enseignements de ces deux documents de la façon retenue par la division d'examen. Dans un tel système, en outre, il n'y a pas d'exécution consécutive des opérations respectivement décrites dans (D1) et (D2). Enfin, on ne saurait s'arrêter à l'argument concernant le test envisagé selon (D1) pour savoir si le circuit intégré a déjà été programmé. En effet, le libellé de la revendication 1 ne l'exclut ni explicitement, ni implicitement.

8. Pour ces raisons, la Chambre estime que l'objet de la revendication 1 n'implique pas d'activité inventive.

La revendication 1 n'est donc pas acceptable - article 52(1) CBE en relation avec l'article 56 CBE.

Enfin la Chambre estime, en accord avec la division d'examen, que l'objet des revendications dépendantes 2 à 5 manque aussi à présenter l'activité inventive requise par la CBE et, à cet effet, renvoie le lecteur aux points II.3.1 et II.3.3 à II.3.5 de la décision attaquée.

Dispositif

Pour ces motifs, il est statué comme suit :

Le recours est rejeté.

Le Greffier : Le Président :

M. Beer G.D. Paterson