BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

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

D E C I S I O N
du 10 novembre 2005

N° du recours : T 0233/03 - 3.4.03

N° de la demande : 00925433.5

N° de la publication : 1180260

C.I.B. : G07F 7/10

Langue de la procédure : FR

Titre de l'invention :
Procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme de cryptographie à clé secrète et dynamique

Demandeur :
GEMPLUS

Opposant :
-

Référence :
Procédé de contre-mesure/GEMPLUS

Normes juridiques appliquées :
CBE Art. 54, 56, 83, 84

Mot-clé :
"Nouveauté, activité inventive, description suffisante, clarté (oui, après modification)"

Décisions citées :
-

Exergue :
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

N° du recours : T 0233/03 - 3.4.03

D E C I S I O N
de la Chambre de recours technique 3.4.03
du 10 novembre 2005

Requérant : GEMPLUS
Avenue du Pic de Bretagne,
Parc d'Activités de Gémenos
F-13881 Gémenos Cédex (FR)

Mandataire : -

Décision attaquée : **Décision de la division d'examen de l'Office européen des brevets signifiée par voie postale le 4 octobre 2002 par laquelle la demande de brevet européen n°00925433.5 a été rejetée conformément aux dispositions de l'article 97(1) CBE.**

Composition de la Chambre :

Président : R. G. O'Connell
Membres : G. Eliasson
J. P. Seitz

Exposé des faits et conclusions

I. Le présent recours est formé par le demandeur de la demande européenne n° 00 925 433.5 à l'encontre de la décision rendue le 4 octobre 2002 par la division d'examen la rejetant pour description insuffisante (article 83 CBE), manque de clarté (article 84 CBE) et manque de nouveauté (article 54 CBE) au vu du document suivant :

D1 : WO 97 36 264 A.

II. En réponse à une notification de la Chambre convoquant le requérant demandeur à une procédure orale, celui-ci a déposé par lettre du 7 octobre 2005 reçue le 12, de nouvelles revendications 1 à 6.

III. Par télécopie du 10 novembre 2005, la Chambre a notifié au requérant que la procédure orale était annulée.

IV. Le requérant demande l'annulation de la décision attaquée et la délivrance d'un brevet sur la base des documents suivants :

Requête principale :

Revendications :

n° 1 à 6 de la requête principale déposées par lettre du 7 octobre 2005 ;

Description :

pages 1 à 6 et 8 à 19 de la demande telle que publiée ;

page 7 déposé par lettre du 24 mars 2005 ;

Dessins :

Feuilles n° 1/7 à 7/7 de la demande telle que publiée.

V. Le libellé des revendications indépendantes 1 et 6 de la requête principale est le suivant :

"1. Procédé de contre-mesure pour un premier composant électronique (C) communiquant avec un second composant électronique (T) et mettant en œuvre un algorithme cryptographique A à clé secrète K de taille k bits, la mise en œuvre du procédé de contre-mesure comprenant une évolution de la valeur K[i] de ladite clé lors des utilisations successives de l'algorithme A, i étant le nombre d'exécutions de l'algorithme A,

caractérisé en ce que

- le premier composant électronique (C)
  - calcule la valeur K[i] de la clé à partir de la précédente valeur K[i-1] de ladite clé au moyen d'une fonction f telle que K[i]=f(K[i-1],
  - transmet le nombre i au second composant électronique (T),

et en ce que

- le second composant électronique (T) possède un raccourci de calcul pour calculer la valeur K[i] de la clé secrète à partir de K[0] sans avoir à générer les i-1 valeur de clés séparant K[0] et K[i]."

"6. Composant électronique (T) apte à communiquer avec un second composant électronique (C) au moyen d'un algorithme cryptographique A à clé secrète K, la valeur K[i] de ladite clé K évolue lors des utilisations successives de l'algorithme A à partir

de la précédente valeur K[i-1] de ladite clé au moyen d'une fonction f telle que K[i]=f(K[i-1]), i étant le nombre d'exécutions de l'algorithme A,
caractérisé en ce que
le composant électronique (T) comporte un moyen pour réaliser un raccourci de calcul pour calculer la valeur K[i] de la clé secrète à partir de K[0] sans avoir à générer les i-1 valeur de clés séparant K[0] et K[i], la valeur de i étant transmise par ledit second composant électronique (C)."

Motifs de la décision

1. Le recours est recevable.

2. *Modifications et clarté - Requête principale*

2.1 La revendication 1 de la requête principale reprend les revendications 1 à 3 de la demande telle que déposée. Les revendications 2 à 5 sont basées respectivement sur les passages en page 9, lignes 13 à 20, lignes 4 à 13, lignes 21 à 30 et lignes 31 à 32 de la demande telle que déposée.

La revendication indépendante 6 est basée sur les passages en page 7, lignes 15 à 17, 25 à 31 et page 8, lignes 22 à 27 de la demande telle que déposée.

2.2 Les revendications 1 à 6 de la requête principale sont de même claires. En particulier, le terme "procédé de contre-mesure" employé dans la revendication 1 est connu dans l'état de la technique comme indiquant la protection d'un algorithme de cryptographie à clé

secrète contre les attaques des tiers mal intentionnés tendant à la décrypter.

2.3 Dans la décision attaquée, la division d'examen a été d'avis que la demande ne satisfaisait pas aux exigences des articles 83 et 84 CBE. Ces objections concernaient les revendications 10 à 15 telles que déposées, supprimées dans la requête principale.

2.4 En conséquence, la Chambre est d'avis que la demande selon la requête principale satisfait aux conditions des articles 84 et 123(2) CBE.

3. *Nouveauté et activité inventive - requête principale*

3.1 Le document D1 qui est considéré comme l'état de la technique le plus proche, décrit un premier composant électronique 3 apte à communiquer avec un second composant électronique 2 au moyen d'un algorithme cryptographique à clé secrète K (voir figure 3, page 17, lignes 3 à 20). La valeur courante de la clé Kn+1 évolue lors des utilisations successives de l'algorithme cryptographique à partir de la précédente valeur Kn de la clé secrète au moyen d'une fonction 32, 33, (par exemple l'algorithme appelé DES Data Encryption Standard), telle que Kn+1 soit une fonction de Kn et Nn, constitutif du nombre d'exécutions de l'algorithme cryptographique (voir page 15, lignes 15 à 19). Les deux composants électroniques 2, 3 mémorisent dans une mémoire reprogrammable la nouvelle valeur du nombre Nn+1 d'exécutions de l'algorithme et la nouvelle valeur Kn+1 de la clé secrète.

3.2 Le dispositif défini dans la revendication 6 indépendante de la requête principale se distingue du dispositif connu en ce que le composant électronique comporte un moyen pour réaliser un raccourci de calcul pour calculer la valeur K[i] de la clé secrète à partir de K[0] sans avoir à générer les i-1 valeur de clés séparant K[0] et K[i], la valeur de i étant transmise par ledit second composant électronique.

En cela donc le dispositif de la revendication 6 est nouveau au sens de l'article 54 CBE.

3.3 La demande décrit deux exemples de raccourcis de calcul :
- En cas d'évolution de la valeur

$$K[i] = K[i-1]^{P} \bmod z,$$

z étant un nombre premier ayant une taille égale à celle de la clé, le raccourci consiste en $K[i]=K[0]^{(P^i)}$, la valeur P^i étant calculée modulo $\varphi(z)$ (φ étant la fonction d'Euler) (voir page 9, lignes 4 à 24).

- Et un autre mode de réalisation dans lequel pour la fonction

$$K[i]=K[i-1]*c \bmod z,$$

le raccourci est $K[i]=K[0]*c^i \bmod z$ (voir page 9, lignes 25 à 30).

3.4 Comme observé par le requérant, en cas d'une désynchronisation en ce sens que le nombre Nn d'exécutions de l'algorithme cryptographique mémorisé dans le premier composant électronique 3 selon le document D1 ne serait pas égal à celui mémorisé dans le second composant électronique 2, le premier devrait alors rattraper le nombre d'itérations pour recalculer la valeur de la clé. Cette resynchronisation pourrait

compliquer le procédé puisque le nombre Nn d'exécutions ne serait pas transmis par le second composant électronique 2.

En outre, dans le dispositif selon la revendication 6, le (premier) composant électronique reçoit la valeur i du nombre d'exécutions de l'algorithme A par le second composant électronique et à partir de K[0] calcule la valeur K[i] en employant un raccourci de calcul.

Au vu du document D1, le problème technique à résoudre par l'invention est donc de réduire le temps nécessaire à la mise en œuvre du procédé si les premier et deuxième composants sont désynchronisés.

3.5 Puisque ni le document D1 ni aucun des autres documents cités dans le rapport de recherche ne divulgue ou ne suggère pas l'utilisation d'un raccourci de calcul mis en œuvre par le premier composant T, aucun d'entre eux ne comporte ainsi d'indication conduisant l'homme du métier à la solution selon l'invention.

Le dispositif selon la revendication 6 de la requête principale implique donc une activité inventive au sens de l'article 56 CBE.

3.6 Le procédé selon la revendication 1 de la requête principale contient toutes les caractéristiques de la revendication 6 et implique donc de même une activité inventive pour ces mêmes raisons.

Dispositif

Par ces motifs, il est statué comme suit :

1. La décision attaquée est annulée

2. L'affaire est renvoyée à l'instance du premier degré afin de délivrer un brevet sur la base des documents suivants :

Revendications :

n° 1 à 6 de la requête principale déposées par lettre du 7 octobre 2005 ;

Description :

pages 1 à 6 et 8 à 19 de la demande telle que publiée ;

page 7 déposé par lettre du 24 mars 2005 ;

Dessins :

Feuilles n° 1/7 à 7/7 de la demande telle que publiée.

Le Greffier : Le Président :

D. Meyfarth R. G. O'Connell