

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 30 mai 2000

N° du recours : T 0027/97 - 3.5.1

N° de la demande : 88400670.1

N° de la publication : 0286489

C.I.B. : H04L 9/30

Langue de la procédure : FR

Titre de l'invention :

Procédé et contrôleur pour cryptographier un message selon un algorithme à clé publique

Titulaire du brevet :

FRANCE TELECOM, et al

Opposant :

Koninklijke Philips Electronics N.V.

Référence :

Cryptographie à clés publiques/FRANCE TELECOM

Normes juridiques appliquées :

CBE Art. 52(1), 52(2)(c), 52(3), 56, 100(a)

Mot-clé :

"CBE art. 52(2) - inventions brevetables - invention exclue de la brevetabilité (non)"

"CBE art. 56 - activité inventive (non)"

Décisions citées :

-

Exergue :

-



N° du recours : T 0027/97 - 3.5.1

D E C I S I O N
de la Chambre de recours technique 3.5.1
du 30 mai 2000

Requérant : Koninklijke Philips Electronics N.V.
(Opposant) Groenewoulsseweg 1
NL - 5621 BA Eindhoven (NL)

Mandataire : Strijland, Wilfred
INTERNATIONAL OCTROOIBUREAU B.V.
Prof. Holstlaan 6
NL - 5656 AA Eindhoven (NL)

Intimée : FRANCE TELECOM
(Titulaire du brevet) 6, Place d'Alleray
F - 75015 Paris (FR)

Mandataire : Cabinet Martinet & Lapoux
BP 405
F - 78055 Saint-Quentin-en-Yvelines Cédex (FR)

Décision attaquée : Décision intermédiaire de la division d'opposition de l'Office européen des brevets signifiée par voie postale le 20 octobre 1996 concernant le maintien du brevet européen n° 0 286 489 dans une forme modifiée.

Composition de la Chambre :

Président : P. K. J. van den Berg
Membres : R. R. K. Zimmermann
P. H. Muehlens

Exposé des faits et conclusions

- I. Le recours concerne le brevet européen n° 0 286 489 délivré le 4 novembre 1992 (Bulletin 92/45) sur la base de la demande de brevet européen n° 88 400 670.1 et concernant un procédé et un contrôleur pour cryptographier un message selon un algorithme à clé publique.
- II. La requérante a fait opposition et requis la révocation complète du brevet européen, entre autres aux motifs que l'objet de la revendication 1 n'était pas brevetable au regard de l'article 52(1) et (2) CBE et n'impliquait pas d'activité inventive, eu égard notamment à la publication E.V. Krishnamurthy, "On Range-Transformation Techniques for Division", IEEE Trans. Computers, février 1970, pages 157-160 (= document D3).

La requérante, sans s'appuyer sur un motif correspondant d'opposition, a fait des objections aux fautes apparemment existantes dans la formulation de l'algorithme divulgué. En réponse, l'intimée a soumis des modifications du brevet, en particulier par la production d'une nouvelle revendication 1 qui se lit comme suit :

"Procédé pour crypter ou décrypter un message représenté sous la forme d'un mot numérique (X) ayant une valeur entière élevée (2^{512}) par le calcul d'une exponentiation modulo N du dit message, N étant un entier, l'exponentiation modulo N étant calculée en effectuant une suite d'opérations A.B modulo N, où A et B sont des variables de calcul ayant des valeurs entières dépendantes de la valeur numérique du message et représentées par des mots numériques à nb bits, nb étant

un entier prédéterminé, ce procédé étant destiné à être utilisé dans des systèmes électroniques traitant des messages à l'aide d'algorithmes à clé publique de type RSA, caractérisé en ce que pour effectuer chacune des opérations $A \cdot B \text{ modulo } N$, le mot numérique représentant la variable A est fractionné en $J + 1$ mots à tb bits, $a_0, \dots, a_i, \dots, a_J$, tb est un entier prédéterminé supérieur à 1, N est un entier compris dans l'intervalle $[2^{nb}, 2^{nb} + 2^{nb-(tb+1)}]$ et représenté par un mot numérique, et $J + 1$ un entier égal ou immédiatement supérieur à nb/tb , en ce que successivement chacun des mots a_i , où i est un entier compris entre 0 et J , est multiplié par le mot numérique représentant la variable B pour former un mot de produit de multiplication qui est ajouté à un mot numérique de somme T représentant une somme cumulée des produits de multiplication antérieurs réduite modulo N , et en ce que la réduction modulo N du mot de somme T est réalisée en lui soustrayant un mot de produit $d_i \cdot N$, où d_i est un mot numérique constitué des $tb + 1$ bits de poids fort du mot de somme T , à chaque fois que le mot de somme représente une valeur supérieure ou égale au produit représenté par le mot de produit $d_i \cdot N$.

III. La Division d'opposition a estimé que la brevetabilité de l'invention ne serait pas exclue par le paragraphe 2 de l'article 52 CBE car l'invention résolvait un problème technique, à savoir le traitement des mots numériques d'une longueur très élevée au moyen d'un microprocesseur de faible encombrement, en un temps acceptable. Aucun des documents produits par l'opposant ne concernait un procédé de cryptographie. En plus l'intervalle défini pour l'entier N ne découle pas de l'état de la technique. Le document D3 proposait déjà des limites à imposer au diviseur choisi pour effectuer un calcul de division, mais les limites résultant de la

revendication 1 seraient "plus favorables"; en conclusion, l'activité inventive serait "indéniable". Considérant établie la brevetabilité de l'invention revendiquée la division d'opposition a rendu une décision intermédiaire avec cette teneur le 29 octobre 1996.

- IV. La requérante a formé un recours contre la décision le 24 décembre 1996 et a payé la taxe de recours le jour même. Le mémoire exposant les motifs du recours était déposé le 24 décembre 1996. La requérante citait, comme l'état de la technique le plus proche, la publication Shoji Miyaguchi, "Fast encryption algorithm for the RSA encryption system", 1982 IEEE (= document D4), un document déjà mentionné sur la première page du fascicule du brevet européen. Une procédure orale devant la Chambre de recours à laquelle les représentants des parties ont participé s'était tenue le 30 mai 2000.
- V. La requérante demande l'annulation de la décision contestée et la révocation du brevet.

L'intimée demande le rejet du recours.

- VI. La requérante a avancé pour l'essentiel les arguments suivants :

Le libellé de la revendication 1 englobait des méthodes de cryptographie sur le plan purement intellectuel qui étaient exclues de brevetabilité par l'article 52(2) et (3) CBE. La référence à l'utilisation dans des systèmes électroniques ne confère pas un caractère technique à l'objet de la revendication 1.

Le document D4 présentait l'état de la technique le plus

proche et divulguait en particulier un algorithme cryptographique de type RSA en utilisant des multiplications modulo un entier et une décomposition des facteurs en tranches des bits de nombre fixe pour effectuer l'exponentiation modulo un entier.

L'objet de la revendication 1 se distinguait du procédé décrit dans le document D4 seulement par la méthode qui permettait d'effectuer l'opération modulo l'entier N. Cette méthode serait fondée sur une approximation du quotient, à savoir par choisir comme quotient le mot d_i formé par un nombre des bits de poids fort du mot qui représentait le dividende. Mais cette méthode ne fonctionnait pas comme prétendu dans tout l'intervalle défini dans la revendication 1 pour l'entier N. En outre, cet intervalle serait seulement plus restreint que le régime proposé en formule (8) du document D3 ; il s'agit là d'une différence insignifiante.

VII. La Chambre, elle aussi a attiré l'attention sur cet argument que l'étendue de l'intervalle pour l'entier N semblait simplement plus restreinte que dans l'état de la technique, différence qui ne faisait pas apparaître l'évidence d'une importance technique. La Chambre a signalé que la signification technique d'une caractéristique serait importante pour l'appréciation de l'activité inventive.

VIII. L'intimée a fait valoir que l'application d'une méthode de cryptographie dans un système téléinformatique elle-même a un caractère technique, comparable au codage et décodage des données pour lesquelles la brevetabilité est reconnue en général par la pratique de l'OEB.

Concernant l'activité inventive l'intimée a réfuté que

l'invention découlait d'une manière évidente de l'état de la technique. L'antériorité la plus pertinente était le document D4 duquel l'invention se distinguait essentiellement par une combinaison de caractéristiques qui s'appuyait sur l'application d'une multiplication par tranche d'un groupage des bits et d'une méthode permettant d'effectuer l'opération modulo l'entier N. Cette méthode de calcul modulo N permettrait de déterminer les chiffres du quotient directement en avant, sans la nécessité d'une tentative de soustraction où d'une restauration du reste. Aucun des documents ne mentionnait ni un tel calcul modulo N ni cette combinaison de caractéristiques. Le document D3 ne concerne ni un procédé de cryptographie ni le calcul de modulo un entier, mais seulement une technique de division. La possibilité que la méthode de l'invention ne fonctionnait pas dans tout l'intervalle revendiqué et la mesure dans laquelle les limites se distinguaient de l'état de la technique n'auraient aucune influence sur l'appréciation de l'activité inventive. L'effet technique réalisé par le choix de l'entier N était la manière prédéterminée dans laquelle le chiffre de quotient pouvait être déterminé par avance.

Motifs de la décision

1. Le recours répond aux conditions énoncées aux articles 106 à 108 CBE ainsi qu'aux règles 1(1) et 64 CBE ; il est donc recevable.

2. Quant au fond, la question à trancher dans le cas d'espèce est à examiner si l'objet de la revendication 1 est exclu de brevetabilité sous l'article 52(2) et (3) CBE ou dénuée d'activité inventive au sens de

l'article 56 CBE comme le soutient la requérante.

3. *Exclusion de brevetabilité*

La requérante a tiré du libellé de la revendication l'argument que malgré la définition concernant la destination du procédé d'être utilisé dans des systèmes électroniques l'étendue de la revendication englobe des méthodes purement intellectuelles ainsi que l'objet revendiqué doit être considéré exclu de brevetabilité par sous-paragraphe c) de l'article 52(2) CBE. La Chambre ne partage pas cette interprétation de la revendication. Selon la Chambre, la revendication 1 définit comme l'objet de la protection un procédé pour crypter ou décrypter un message représenté sous la forme d'un mot numérique à l'aide d'algorithmes à clé publique de type RSA, le procédé étant destiné à être utilisé dans des systèmes électroniques. Cette définition indique clairement qu'il s'agit d'une méthode dans le domaine de l'informatique électronique et des télécommunications qui n'est pas exclue de brevetabilité sous l'article 52(2) et (3) CBE, même si un algorithme abstrait où une méthode mathématique forment la base de l'invention.

4. *L'activité inventive*

Le document D4 forme, de l'avis de la requérante et aussi de l'intimée, l'état de la technique le plus proche pour l'objet de la revendication 1. Considérant que l'intimée a référé au document D4, sans opposer l'introduction tardive de ce document dans la procédure, et que ce document semble être en effet l'antériorité la plus pertinente, la Chambre l'estime approprié d'admettre ce document à la procédure malgré qu'il ne

fut pas présenté en dû temps.

- 4.1 Le document D4 décrit un procédé pour crypter ou décrypter un message comme défini dans la première partie de la revendication 1. En particulier, le document décrit un procédé qui est destiné à être utilisé dans des systèmes électroniques traitant des messages à l'aide d'algorithmes à clé publique de type RSA (voir p. ex. l'abrégé, page 672) qui sont fondés sur un calcul de l'exponentiation modulo un entier effectué par une suite de multiplications modulo l'entier ("exponentiation by repeated squaring and multiplication", voir document D4, page 673, paragraphe 2.1 et en particulier les termes $M_1 \times M_2$ modulo n).

En développant le procédé RSA d'origine comme publié par de Rivest, Shamir et Adleman (cf. le résumé rendu dans le brevet contesté, colonne 1, lignes 12 ff.), le document D4 propose d'exécuter les multiplications par tranches d'un nombre de bits ($M_{2,j}$) et, en alternant avec les multiplications, les réductions modulo l'entier n (voir document D4, page 673, paragraphe 2.2). Là, il est aussi explicitement indiqué que la réduction modulo n nécessite une division par n , une proposition qui découle d'une manière évidente de la définition du calcul modulo un entier et qui est à la base des formules (3) à (5).

Cette réduction modulo- n du produit partiel $M_1 \times M_{2,j}$ est réalisée par la détermination du quotient partiel Q_j et du reste partiel R_j , cette dernière étape du calcul est effectuée par la soustraction du produit $Q_j \times n$ de la somme partielle mise entre parenthèses (formule (5)). Cette somme partielle représente une valeur supérieure ou

égale au produit (voir la définition de l'opération l...m). Comme indiqué au paragraphe 2.3, page 673, le quotient partiel Q_j et le reste partiel R_j sont déterminés approximativement pour réduire le temps perdu dans le calcul.

D'où découlent les caractéristiques suivantes de la revendication 1 si on se rappelle que la désignation concrète des variables de l'algorithme qui est seulement une convention sur le plan mathématique n'a aucune implication directe pour la définition des étapes physiques composant la méthode à protéger. Il s'agit ici des caractéristiques suivantes : "(---) effectuant une suite d'opérations $A.B$ modulo N , où A et B (" M_1 , M_2 ") sont des variables de calcul (---) représentées par des mots numériques à nb bits (document D4 : $nx\grave{e}$), nb étant un entier prédéterminé, (---) pour effectuer chacune des opérations $A.B$ modulo N ($R / M_1 \times M_2 \bmod n$), le mot numérique représentant la variable A est fractionné en $J + 1$ mots (l parts) à tb bits (\grave{e} bits), $a_0, \dots, a_i, \dots, a_J$ ($M_{2,j}$, $j \cdot i + 1$), tb est un entier prédéterminé supérieur à 1, N est un entier et représenté par un mot numérique, et $J + 1$ un entier égal ou immédiatement supérieur à nb/tb , (---) successivement chacun des mots a_i , où i est un entier compris entre 0 et J , est multiplié par le mot numérique représentant la variable B pour former un mot de produit de multiplication qui est ajouté à un mot numérique de somme T (le terme $2^{\acute{e}}R_{j+1}$ en formules (4) et (5)) représentant une somme cumulée des produits de multiplication antérieurs réduite modulo N , et en ce que la réduction modulo N du mot de somme T est réalisée en lui soustrayant un mot de produit $d_i.N$ (le terme $Q_j \cdot xn$ en formule (5)), (---), à chaque fois que le mot de somme représente une valeur supérieure ou égale au produit représenté par le mot de produit $d_i.N$ ".

4.2 Par conséquent l'objet de la revendication 1 se distingue de l'état de la technique décrit dans le document D4 seulement par les caractéristiques suivantes :

(A) d_i est un mot numérique constitué des $tb + 1$ bits de poids fort du mot de somme T, et

(B) l'entier N est compris dans l'intervalle $[2^{nb}, 2^{nb} + 2^{nb-(tb + 1)}]$.

4.3 Ce choix du d_i et N est à considérer comme une approximation numérique du quotient, la restriction de N à l'intervalle revendiqué sert à assurer que la valeur absolue du reste est plus petite que la valeur de N. Selon l'argumentation développée par l'intimée, cette méthode de calcul a l'avantage que le quotient peut être prédéterminé, résultant dans l'avantage technique d'une réduction des étapes de calcul et, par là, du temps de calcul.

Ce sont essentiellement aussi les avantages qui sont réalisés par ledit calcul approximatif proposé dans le document D4. Pour cette raison, lesdites avantages ne peuvent pas servir comme point de départ pour formuler, selon des critères objectifs, le problème technique qui est posé et résolu par l'invention revendiquée. Puisqu'un autre effet technique se basant sur lesdites caractéristiques (A) et (B) ne ressort pas du brevet où de l'argumentation de l'intimée, le problème technique résolu objectivement par l'invention en tant que revendiquée doit être vu dans le but de fournir une alternative à la méthode numérique connue du document D4 permettant de prédéterminer approximativement le quotient dans une division entière.

4.4 Le domaine de cryptographie est caractérisé par l'utilisation des algorithmes abstraits et complexes dans des systèmes informatiques électroniques. Conformément, l'homme du métier est supposé à maîtriser les techniques numériques et se mettre au courant de l'état actuel et des développements dans cette discipline des mathématiques et, plus généralement, dans des méthodes mathématiques qui sont appliquées sur ordinateurs. Le document D3 appartient donc aux publications qu'il irait consulter pour trouver une solution d'un problème numérique. Le document D3 décrit un calcul général de division permettant de prédéterminer approximativement le quotient dans la division ("deterministic generation of quotient digits"). Selon le document D3, le chiffre quotient est choisi comme le chiffre le plus fort (document D3, page 158, lignes 18 et s.) sous la condition que le diviseur soit compris dans l'intervalle défini par la formule (8) (page 158). Il est évident que le mot numérique représentant le chiffre quotient est déterminé par un nombre fixe des bits de poids fort si la base \hat{a} est une puissance à base 2, la base \hat{a} étant le seul paramètre libre dans cette variante de la méthode si l'on considère le dividende et le diviseur comme prédéterminés.

Le document D4 propose la décomposition du facteur M_2 dans la tranches $M_{2,j}$ de longueur de bits égale, la valeur de ces variables $M_{2,j}$ est égale à la valeur des chiffres du facteur M_2 dans un système de numération à base $2^{\hat{e}}$. Par conséquent, la base $2^{\hat{e}}$ est le premier choix dans l'application du document D3 pour effectuer l'étape de division (formule (4)) dans la méthode de multiplication modulo un entier comme proposé par le document D4. En outre, lorsque $\hat{a}=2^{\hat{e}}$, la formule (8)

(document D3) présente essentiellement l'intervalle défini pour l'entier N dans la revendication 1. Ce résultat, cependant, n'est pas exact car il reste, entre les limites supérieures, une différence.

Malgré des invitations de la Chambre de recours d'indiquer les effets techniques qui sont produits par cette différence, aucune des parties n'a fourni des explications qui pourrait aider à éclaircir cette question. Puisque des caractéristiques qui n'ont pas des effets techniques ne peuvent pas contribuer à l'activité inventive, ladite différence entre l'intervalle revendiqué et la formule (8) (document D3) doit être ignorée dans l'appréciation de l'activité inventive.

En sommaire, aucune des caractéristiques définies dans la revendication 1 n'invoque une activité inventive. Ainsi l'objet de la revendication ne remplit pas la condition d'activité inventive (article 100a) CBE en liaison avec l'article 56 CBE).

- 4.5 L'intimée s'est référée aussi à la combinaison de caractéristiques, à savoir la décomposition des facteurs de la multiplication en tranches de bits et le calcul modulo l'entier N. Cet argument ne tient pas compte du fait qu'une telle combinaison est déjà décrite dans le document D4 et que l'objet de la revendication 1 se distingue de cet état de la technique seulement par la méthode de division et la manière de laquelle le quotient est approché.

L'intimée a fait encore valoir que le document D3 ne concerne non pas une méthode de cryptographie et qu'il n'est donc pas pertinent pour l'objet de la revendication. Un tel argument est applicable pour

apprécier la nouveauté d'une invention revendiquée ;
mais dans le contexte de l'activité inventive les
compétences et la pratique de l'homme du métier doivent
être prises en compte dans son entier. Ceci permet dans
ce contexte à consulter des documents qui ne sont pas
reliés directement à l'objet de l'invention, comme c'est
le cas ici par rapport aux documents concernant des
techniques numériques.

Dispositif

Par ces motifs, il est statué comme suit :

1. La décision contestée est annulée.
2. Le brevet est révoqué.

Le Greffier :

Le Président :

M. Kiehl

P. K. J. van den Berg