**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 14 avril 2023

**N° du recours :** T 0540/21 - 3.5.05

**N° de la demande :** 10738014.9

**N° de la publication :** 2443789

**C.I.B. :** H04L9/30, G06F7/72, H04L9/28, G06F17/10, G06F7/58

**Langue de la procédure :** FR

**Titre de l'invention :**
Cryptographie sur une courbe elliptique simplifiée

**Titulaire du brevet :**
Idemia Identity & Security France

**Opposantes :**
Giesecke & Devrient GmbH
Bundesdruckerei GmbH

**Référence :**

**Normes juridiques appliquées :**
CBE Art. 52(2), 54, 56, 83, 112(1), 113(1)
CBE R. 103(1)a)

**Mot-clé :**
Vice substantiel de procédure - violation du droit d'être entendu (non)
Activité inventive - (oui)
Possibilité d'exécuter l'invention - (oui)
Saisine de la Grande Chambre de recours - (non)
Remboursement de la taxe de recours - (non)

**Décisions citées :**
T 0027/97, T 1326/06, T 0556/14

**Exergue :**

Europäisches Patentamt
European Patent Office
Office européen des brevets

**Beschwerdekammern**

**Boards of Appeal**

**Chambres de recours**

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

**N° du recours : T 0540/21 - 3.5.05**

**D E C I S I O N**
**de la Chambre de recours technique 3.5.05**
**du 14 avril 2023**

| | |
|---|---|
| **Requérante :** (Opposante 2) | Bundesdruckerei GmbH<br>Oranienstr. 91<br>10969 Berlin (DE) |
| **Mandataire :** | Richardt Patentanwälte PartG mbB<br>Wilhelmstraße 7<br>65185 Wiesbaden (DE) |
| **Intimé :** (Titulaire du brevet) | Idemia Identity & Security France<br>2, Place Samuel de Champlain<br>92400 Courbevoie (FR) |
| **Mandataire :** | Regimbeau<br>20, rue de Chazelles<br>75847 Paris Cedex 17 (FR) |
| **Partie de droit :** (Opposante 1) | Giesecke & Devrient GmbH<br>Patent und Lizenzen<br>Prinzregentenstrasse 159<br>81677 München (DE) |

**Décision attaquée :** **Décision de la division d'opposition de l'Office européen des brevets postée le 19 mars 2021 par laquelle l'opposition formée à l'égard du brevet européen n° 2443789 a été rejetée conformément aux dispositions de l'article 101(2) CBE.**

**Composition de la Chambre :**

| | |
|---|---|
| **Présidente** | A. Ritzka |
| **Membres :** | P. Cretaine |
| | F. Blumer |

## Exposé des faits et conclusions

I. Le présent recours est formé par l'opposante 2 à l'encontre de la décision de la division d'opposition, postée le 19 mars 2021, de rejeter les oppositions contre le brevet européen No. EP-B-2 443 789. Les oppositions étaient fondées sur les motifs des articles 100 a) et 100 b) CBE, et s'appuyaient en particulier sur les documents suivants:

D1: A. Shallue et al: "Construction of rational points on elliptic curves over finite fields", Computer Science, vol. 4076, Germany, 1er janvier 2006, pages 510 à 524,

D2: M. Skalba: "Points on elliptic curves over finite fields", Linear Algebra and its Applications, vol. 117, no. 3, 1er janvier 2005, pages 293 à 301, et

D3: M. Ulas: "Rational points on certain hyperelliptic curves over finite fields", Cornell University Library, NY, 11 juin 2007, pages 1 à 9.

II. L'acte de recours de la requérante (opposante 2) a été déposé le 11 mai 2021 et la taxe de recours a été acquittée le même jour. Le mémoire exposant les motifs du recours a été reçu le 27 juillet 2021. La requérante a demandé avec son acte de recours l'annulation de la décision attaquée et la révocation du brevet.
La requérante a de plus demandé avec son mémoire de recours le renvoi de l'affaire à la première instance, conformément à l'article 11 RPCR, et, à titre subsidiaire la tenue d'une procédure orale. Le renvoi de l'affaire en première instance a été demandé en raison de la présence alléguée de vices substantiels de

procédure en première instance ayant entraîné la violation du droit d'être entendu de la requérante.

III. L'opposante 1, partie de droit à la procédure de recours, n'a pas pris position ni formulé de requête en réponse au dépôt du recours.

IV. Par lettre datée du 15 novembre 2021, l'intimée (propriétaire du brevet) a demandé à titre principal le maintien du brevet tel que délivré et, à titre subsidiaire, le maintien du brevet sous forme modifiée conformément aux requêtes auxiliaires 1 à 4 déposées le 20 décembre 2018.

V. Par lettre datée du 21 avril 2022, la requérante a réfuté les arguments de l'intimé présentés en réponse aux motifs du recours.

VI. Une citation à une procédure orale a été envoyée le 5 juillet 2022. Dans une notification établie conformément à l'article 15(1) RPCR envoyée le 10 février 2023, la chambre a communiqué aux parties ses constatations préliminaires ne préjugeant en rien de la décision finale sur le recours. La chambre a en particulier fait référence aux objections de la requérante et de la partie de droit qui allaient devoir être successivement examinées durant la procédure orale:
- vices substantiels de procédure et renvoi à la première instance pour non-respect du droit à être entendu,
- objections de manque d'activité inventive basées sur les documents de l'état de la technique cités en première instance et les connaissances générales de l'homme du métier.

La chambre a aussi signalé que, dans le cas où les motifs d'opposition s'opposeraient au maintien du brevet tel que délivré, elle avait l'intention de renvoyer l'affaire en première instance pour examen des requêtes auxiliaires de l'intimé.

VII. Dans sa réponse en date du 24 février 2023 l'opposante 1 (partie de droit) a demandé l'annulation de la décision et la révocation du brevet pour manque d'activité inventive (Articles 100a) et 56 CBE).

VIII. Dans sa réponse en date du 13 mars 2023, l'intimée a demandé de ne pas renvoyer l'affaire en première instance au cas où le brevet ne serait pas maintenu tel que délivré.

IX. Dans sa réponse en date du 13 Avril 2023, la requérante a demandé comme requête auxiliaire que la chambre saisisse la Grande Chambre de recours, conformément à l'article 112 CBE, pour lui soumettre la question de droit suivante:

"Ist Kryptographie patentrechtlich als per se technisch zu bewerten und haben deshalb Erfindungen, die kryptographische Verfahren beinhalten damit bereits die erste Hürde gemäß G0001/19 genommen, sind also patentfahig gemäß Art. 52 EPÜ, ohne dass es der weiteren Angabe von einer Anwendung der Erfindung auf einem technischen Gebiet bedürfte?".

La chambre a traduit cette question en:

"La cryptographie doit-elle être considérée comme technique en soi au regard du droit des brevets et, par conséquent, les inventions impliquant des procédés cryptographiques ont-elles déjà franchi le premier

obstacle conformément à la décision G0001/19, c'est-à-dire qu'elles sont brevetables en vertu de l'article 52 CBE, sans qu'il soit nécessaire d'indiquer une application de l'invention dans un domaine technique?".

La requérante a en outre demandé le remboursement de la taxe de recours pour vice substantiel de procédure ayant entaché la procédure en première instance, à savoir la violation de son droit à être entendue.

X. La procédure orale s'est tenue le 14 avril 2023.

La requérante (opposante 2) a demandé l'annulation de la décision contestée et le renvoi de l'affaire à la première instance pour vice majeur de procédure ou la révocation du brevet. Elle a de plus demandé la saisine de la Grande Chambre de recours pour une question de droit identifiée dans la lettre du 13 avril 2023 et le remboursement de la taxe de recours.

L'opposante 1, partie de droit à la procédure de recours, a demandé l'annulation de la décision contestée et la révocation du brevet.

L'intimée (titulaire du brevet) a demandé à titre principal le rejet du recours, c'est-à-dire le maintien du brevet tel que délivré, ou bien, à titre subsidiaire, le maintien du brevet sous forme modifiée conformément aux requêtes auxiliaires déposées le 20 décembre 2018.

Après mûres délibérations, la décision de la chambre a été prononcée.

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

"Procédé d'exécution d'un calcul cryptographique dans un composant électronique comprenant une étape d'obtention d'un point P(X,Y) à partir d'au moins un paramètre t, sur une courbe elliptique vérifiant l'équation :
$Y^2 = f(X)$ ; et
à partir de polynômes $X_1(t)$, $X_2(t)$ et $U(t)$ vérifiant l'égalité suivante :
$-f(X_1(t)).f(X_2(t))=U(t)^2$
dans le corps fini $F_q$, quel que soit le paramètre t, q vérifiant l'équation $q = 3 \bmod 4$;
ledit procédé comprenant les étapes suivantes :
1) obtenir une valeur du paramètre t ;
2) déterminer le point P en effectuant les sous étapes suivantes:
    i) calculer (11) $X_1 = X_1(t)$, $X_2 = X_2(t)$ et $U=U(t)$
    ii) tester (12) si le terme $f(X_1)$ est un terme au carré dans le corps fini $F_q$ et dans ce cas, calculer (13) la racine carré du terme $f(X_1)$, le point P ayant pour abscisse $X_1$ et pour ordonnée $Y_1$ la racine carré du terme $f(X_1)$;
    iii) sinon calculer (14) la racine carré du terme $f(X_2)$, le point P ayant pour abscisse $X_2$ et pour ordonnée $Y_2$ la racine carré du terme $f(X_2)$;
3) utiliser ledit point P dans une application cryptographique de chiffrement ou de hachage ou de signature ou d'authentification ou d'identification."

Le jeu de revendications tel que délivré comprend une seconde revendication indépendante portant sur un dispositif correspondant (revendication 8).

Étant donné l'aboutissement du présent recours il n'est pas nécessaire de détailler les revendications des requêtes auxiliaires 1 à 4.

## Motifs de la décision

1. Recevabilité du recours

Le recours de la requérante satisfait aux exigences des articles 106 à 108 CBE (voir le point II ci-dessus) et est donc recevable.

2. Requête en renvoi de l'affaire pour vice substantiel de procédure

2.1 La requérante a fait valoir en substance que la division d'opposition n'avait pas respecté son droit à être entendu car les motifs de la décision n'exposent pas pourquoi certains de ses arguments en support de ses objections selon les articles 52 et 56 CBE n'ont pas été acceptés par la division d'opposition.

2.2 La requérante a tout d'abord affirmé avoir été surprise par les motifs de la décision exposés au point 34 de la décision selon lesquels la cryptographie est un domaine technique, alors que selon elle il s'agirait d'un domaine purement mathématique et donc exclu de la brevetabilité selon l'article 52 CBE et la Jurisprudence des Chambres de Recours (voir la dixième édition, juillet 2022, chapitre I.A.2.2.2).

La chambre constate cependant que la communication de la division d'opposition en date du 2 août 2019 (voir le point 22) ainsi que le protocole de la procédure orale devant la division d'opposition (voir les points 5.1 à 5.9 et 6.1) témoignent que la division d'opposition a constamment considéré que la cryptographie est un domaine technique et que cet argument a été débattu entre les parties au cours de la

procédure orale pour décider du caractère technique de l'étape (3) de la revendication 1. La requérante a donc eu pleinement connaissance des motifs avancés au paragraphe 34 avant que la décision écrite ne lui soit notifiée.

2.3 De plus, la requérante a argumenté que ses arguments concernant le caractère non-technique de la revendication 1 n'avaient pas été pris en compte par la division d'opposition. En ce sens la requérante a avancé que la décision ne comprends pas les motifs pour lesquels son argumentation selon laquelle la revendication 1 ne comprend pas de caractéristique technique autre que le composant électronique a été rejetée pour l'évaluation de l'activité inventive. Il apparaît cependant que la décision établit dans plusieurs passages les motifs que la division d'opposition a utilisé pour rejeter cette argumentation, en réponse aux objections de la requérante selon les articles 83 CBE (voir les points 21 à 30), 52(2)a) et (3) CBE (voir les points 32 à 34) et 54 CBE (voir le point 36).

2.4 D'autre part, le fait que la division d'opposition n'ait pas été en accord avec un des arguments de la requérante ne peut constituer en soi un vice de procédure.

2.5 En conclusion, la chambre n'a pas constaté l'existence de vice substantiel de procédure dans la procédure devant la division d'opposition, et a donc décidé en procédure orale de rejeter la demande de renvoi de l'affaire.

3. Articles 83, 52(2)a) et 3), et 54 CBE

La requérante n'a produit ni dans son mémoire exposant les motifs du recours ni en procédure orale d'argument contre la décision attaquée concernant les objections selon les articles 83, 52 et 54 CBE soulevées en première instance. En conséquence, la chambre se range à l'avis de la décision selon lequel le brevet tel que délivré satisfait aux exigences des articles 83, 52 et 54 CBE.

4. Article 56 EPC

4.1 Lors de la procédure orale, il a été admis par les parties que l'objet de la revendication 1 diffère de la divulgation de D2 (Skalba) en ce que:

- l'équation de Skalba $f(X_1(t)).f(X_2(t)).f(X_3(t))= (U(t))^2$ est modifiée en choisissant de fixer $f(X_3(t)) = -1$, soit $-f(X_1(t)).f(X_2(t)) = (U(t))^2$,

- la cardinalité du corps fini dans lequel s'effectue les calculs de la courbe elliptique est fixée à une valeur q vérifiant l'équation $q = 3 \bmod 4$, et

- si le terme $f(X_1(t))$ n'est pas un carré, le point P de la courbe elliptique est déterminé par son abscisse $X_2(t)$ et son ordonnée $\sqrt{f(X_2(t)}$.

Les simplifications impliquées par ces caractéristiques distinctives permettent, selon l'intimée, l'obtention du point P par un nombre d'opérations constant, à savoir un test de carré et un calcul de racine, et donc dans un temps de calcul largement indépendant des paramètres d'entrée t, ce qui limite la sensibilité aux attaques de type "timing attack" pour retrouver t.

4.2 La requérante a argumenté que l'homme du métier arriverait à la solution donnée par la revendication 1, telle que résumée au paragraphe 42 de la décision, sans exercer une quelconque activité inventive.

4.2.1 Tout d'abord, selon la requérante, l'homme du métier serait incité à adapter l'algorithme de Skalba puisque ce dernier est considéré comme inefficace et non à temps constant par le document D1 (voir la page 511).

Ensuite, la requérante a avancé que le choix de $f(X_3(t)) = -1$ était un choix particulier évident pour l'homme du métier. En effet, selon elle, la revendication 1 est basée sur une simplification de l'égalité de Skalba, comme indiqué à la page 2 de la description, mais en régle générale les polynômes vérifiant l'égalité de Skalba peuvent prendre deux paramètres u et t:
$(X_1(t,u)).f(X_2(t,u)).f(X_3(t,u)) = (U(t,u))^2$.
Toujours selon la requérante, l'homme du métier tirerait de l'enseignement de D3 (voir le passage "Theorem 2.3") qu'un des polynômes de l'égalité de Skalba peut être choisi comme étant égal à u, par exemple $X_3(t,u) = u$ et donc $f(X_3(t,u)) = f(u)$. L'homme du métier choisirait u constant pour minimiser les efforts de calculs et constaterait ensuite que le point $(u, \sqrt{f(u)})$ de la courbe elliptique ne présente pas de valeur cryptographique puisqu'il ne dépend pas de la valeur secrète t. Il exclurait donc que f(u) soit un carré et choisirait la valeur la plus évidente $f(u) = -1$.

4.2.2 Dans une deuxième ligne argumentaire, la requérante a fait valoir que certaines caractéristiques de la revendication 1 n'étaient pas techniques et ne devaient donc pas être prises en compte pour l'appréciation de

l'activité inventive. Selon elle, les étapes (1) et (2) se réduiraient à des calculs mathématiques et l'étape (3) ne définit pas d'application technique d'un procédé cryptographique dans un système électronique puisqu'elle ne précise pas que les applications qui y sont mentionnées sont exécutées par le composant électronique.

4.2.3 De plus la requérante a avancée en procédure orale que la revendication 1 n'excluait pas que le composant électronique soit un calculateur analogique pour lequel l'effet technique allégué par l'intimé, à savoir la réduction de la sensibilité aux attaques de type "timing attack" pour retrouver t, n'était pas obtenu.

4.3 La partie de droit a argumenté par écrit que partant de D3, l'homme du métier effectuerait de manière évidente la sélection de la caractéristique q = 3 mod 4 du corps fini, celle-ci n'étant pas exclue par D3. De plus, l'homme du métier constaterait que la possibilité la plus simple et donc la plus évidente consisterait à fixer le terme constant $g_1(u)$ à -1 dans D3.

4.4 La chambre n'est pas convaincu par les arguments de la requérante et de la partie de droit pour les raisons suivantes.

4.4.1 En ce qui concerne les arguments de la requérante exposés au point 4.2.1 ci-dessus et ceux de la partie de droit exposés au point 4.3 ci-dessus, la chambre partage l'avis de la division d'opposition et de l'intimée selon laquelle le qualificatif "deterministic" attribué dans D1 à l'algorithme ne signifie pas que ce dernier soit exécuté en un temps constant, mais plutôt que les mêmes entrées conduisent toujours aux mêmes résultats, par opposition à un

algorithme non-déterministe. Le problème technique formulé dans la décision n'est donc pas évoqué dans D1, ni dans D2 ou D3, aucun de ces documents ne décrivant un algorithme en temps constant.

Ensuite, la chambre note que bien que D3 divulgue qu'un des trois termes de l'égalité de Skalba peut être égal à f(u), ce document ne divulgue ni ne suggère que u soit fixé constant, que f(u) ne soit pas un carré, et que f(u) = -1. De plus, le choix de la cardinalité du corps q = 3mod4 est lié au choix de f(u) car -1 n'est jamais un carré dans ce cas de cardinalité. Ces trois choix particuliers permettent d'être certain que l'un des deux termes de l'égalité de Skalba est un carré, de pouvoir calculer le point P éventuellement à partir du deuxième terme de l'égalité sans avoir à le tester pour savoir si c'est un carré ou non, et donc de permettre l'obtention du point P avec un nombre de calculs constant et donc dans un temps constant indépendamment de la valeur de t. L'homme du métier n'est incité par aucun des documents D1, D2 et D3 à effectuer ces trois choix parallèlement, et le type d'argumentation de la requérante, et aussi de la partie de droit, s'appuie essentiellement, selon la chambre, sur la connaissance à posteriori de l'invention.

4.4.2 Pour ce qui est de l'argumentation de la requérante exposée au point 4.2.2 ci-dessus, la chambre partage l'avis de l'intimée en procédure orale que l'étape (3) de la revendication 1 n'a pas été identifiée comme étant une différence par rapport à l'état de la technique. Il n'y a donc pas lieu de discuter sa technicité pour l'évaluation de l'activité inventive. Quand aux étapes (1) et (2), la chambre est d'accord avec les principes exprimés dans la décision (voir les points 32 à 34) que la cryptographie est un domaine

technique et que la détermination d'un point sur une courbe elliptique pour utilisation dans le domaine de la cryptographie présente un caractère technique.

4.4.3 En ce qui concerne l'argument de la requérante selon lequel l'effet technique ne serait pas obtenu sur toute la portée de la revendication 1 (voir le point 4.2.3 ci-dessus), la chambre constate que cet argument n'a pas été avancé dans le mémoire exposant les motifs du recours mais seulement tardivement à la fin de la procédure orale. De plus, l'intimée a argumenté de manière convaincante que même si l'on devait prendre en compte cet argument, il n'en demeure pas moins que quel que soit le composant électronique considéré, la revendication 1 garantit qu'un seul test de carré et un seul calcul de racine suffisent pour l'obtention du point P, contrairement à l'état de la technique. Pour ces raisons, la chambre est d'avis que l'argument doit être rejeté.

4.5 En conclusion, la chambre juge que l'objet de la revendication 1 implique une activité inventive (article 56 CBE) au vu des documents cités.

5. Il s'ensuit que les motif d'opposition selon les articles 100 a) et 100 b) CBE ne s'opposent pas au maintien du brevet.

6. Requête en saisine de la Grande Chambre de recours

La requérante a maintenu en procédure orale sa requête selon l'article 112(1)a) CBE formulée par lettre du 13 avril 2023 (voir le point IX ci-dessus).

La chambre estime qu'il n'y a aucune divergence entre son approche de l'évaluation du caractère technique de

la revendication 1 et la jurisprudence des chambres de recours. En effet la jurisprudence des chambres de recours a établi depuis longtemps que les inventions dans le domaine de la cryptographie n'étaient pas exclues de la brevetabilité au sens de l'article 52(2) CBE, même si elles mettent en oeuvre des méthodes mathématiques (voir La Jurisprudence des Chambres de recours, 10ième édition, juillet 2022, I.A.2.2.2, et en particulier les décisions T 0027/97, T 1326/06, et T 0556/14). Dans le cas présent, l'objet de la revendication 1 consiste en un procédé de détermination d'un point sur une courbe elliptique pour utilisation de ce point dans une application cryptographique. L'utilisation de points de courbes elliptiques dans des procédés de chiffrement est bien connu pour améliorer la sécurité et la vitesse de calcul.

Pour ces raisons, la chambre a décidé en procédure orale qu'une saisine de la Grande Chambre de recours pour répondre à la question posée par la requérante n'était aucunement nécessaire pour pouvoir arriver à une décision dans le présent recours. En conséquence, la requête a été rejetée conformément à l'article 112(1)a) CBE.

7. Remboursement de la taxe de recours

Les conditions de la règle 103(1)a) CBE n'étant pas remplies, la requête en remboursement de la taxe de recours de la requérante est rejetée.

## Dispositif

## Par ces motifs, il est statué comme suit

- Le recours est rejeté.
- La requête en saisine de la Grande Chambre de recours est rejetée.
- La requête en remboursement de la taxe de recours est rejetée.

La Greffière : La Présidente :

K. Götz-Wein A. Ritzka

Décision authentifiée électroniquement