Code de distribution interne :

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

Liste des données pour la décision du 15 décembre 2025

N° du recours :	T 0558/21 - 3.5.06
N° de la demande :	10738013.1
N° de la publication :	2443787
C.I.B. :	G06F7/72, H04L9/28, G06F7/58, G06F17/10
Langue de la procédure :	FR

Titre de l'invention :
Cryptographie sur une courbe elliptique

Titulaire du brevet :
Idemia Identity & Security France

Opposantes :
Bundesdruckerei GmbH
GIESECKE & DEVRIENT GmbH

Référence :
Calcul cryptographique sur courbe elliptique/IDEMIA

Normes juridiques appliquées :
CBE Art. 52(1), 52(2), 52(3), 54, 56, 83, 84, 101(3)b), 113(1), 116, 123(2), 123(3)
CBE R. 80
RPCR 2020 Art. 11, 13(2), 15a(1)

Mot-clé :
Procédure orale - requête de tenue de la procédure orale par visioconférence (refusée)
Vice substantiel de procédure - violation du droit d'être entendu (non)
Modifications - admises (oui)
Interprétation de la revendication 1 - sous-étape mentionnée dans la revendication n'est pas limitative
Exclusion de la brevetabilité - (non)
Activité inventive - effet technique (oui) - non-évidence au regard de l'état de la technique documenté pas contestée en recours

Décisions citées :
G 0003/14, G 0001/19, T 0072/95, T 0027/97, T 0641/00, T 0052/02, T 0619/02, T 0914/02, T 0258/03, T 0154/04, T 0471/05, T 0930/05, T 0756/06, T 1326/06, T 1358/09, T 2230/10, T 0556/14, T 0697/17, T 1924/17, T 0761/20, T 0540/21

Exergue :
1. Sur la pertinence de l'appartenance d'une invention à un « domaine technique » pour son caractère technique et pour l'identification des caractéristiques qui y contribuent, cf. points 29 et 42.

2. Sur la contribution technique d'une méthode mathématique de génération d'un point sur une courbe elliptique utilisé dans une application cryptographique, cf. point 40.

3. Sur la détermination des caractéristiques d'une invention qui contribuent à son caractère technique dans le cadre de l'approche COMVIK, cf. point 41.

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

N° du recours : T 0558/21 - 3.5.06

D E C I S I O N
de la Chambre de recours technique 3.5.06
du 15 décembre 2025

Requérante : (Opposante 1)	Bundesdruckerei GmbH Oranienstr. 91 10958 Berlin (DE)
Mandataire :	Richardt Patentanwälte PartG mbB Wilhelmstraße 7 65185 Wiesbaden (DE)
Intimée : (Titulaire du brevet)	Idemia Identity & Security France 2, Place Samuel de Champlain 92400 Courbevoie (FR)
Mandataire :	Regimbeau 20, rue de Chazelles 75847 Paris Cedex 17 (FR)
Partie de droit : (Opposante 2)	GIESECKE & DEVRIENT GmbH Prinzregentenstrasse 159 81677 München (DE)

Décision attaquée : **Décision intermédiaire de la division d'opposition de l'office européen des brevets postée le 18 mars 2021 concernant le maintien du brevet européen No. 2443787 dans une forme modifiée.**

Composition de la Chambre :

Président	M. Müller
Membres :	M. Domingo Vecchioni
	A. Jimenez

Exposé des faits et conclusions

I. L'opposante 1 a formé un recours contre la décision intermédiaire de la division d'opposition notifiée le 18 mars 2021 concernant le maintien du brevet européen n° 2 443 787 dans une forme modifiée.

II. Parmi les documents de l'état de la technique pris en considération en première instance, les documents suivants ont été de nouveau examinés dans la procédure de recours:

D1: M. Ulas, "Rational points on certain hyperelliptic curves over finite fields", arXiv:0706.1448v1 [math.NT] 11 juin 2007,

D2: A. Shallue et C.E. van de Woestijne, "Construction of rational points on elliptic curves over finite fields", ANTS 2006, LNCS 4076, 2006, pages 510-526,

D3: T. Icart, "How to hash into elliptic curves", Cryptology ePrint Archive: Report 2009/226, 24 mai 2009, http://eprint.iacr.org/2009/226.pdf

D4: M. Skalba, "Points on elliptic curves over finite fields", Acta Arithmetica, 117.3, 2005, pages 293-301,

D9: E. Bach et al., Algorithmic Number Theory: Efficient Algorithms, MIT Press, 1996, pages 155-157, 194, 195,

D20: H. Cohen, A Course in Computational Algebraic

Number Theory, Springer, 2000, pages 27-28,

D21: D. Hankerson et al., Guide to Elliptic Curve Cryptography, Springer, 2004.

III. La division d'opposition avait jugé que le brevet, tel que modifié selon la requête principale, satisfaisait aux exigences de la règle 80 CBE ainsi que des articles 83, 84 et 123(2) et (3) CBE. Elle avait en outre conclu que les objets des revendications indépendantes 1, 6 et 9 n'étaient pas exclus de la brevetabilité au titre de l'article 52(2) et (3) CBE, qu'ils étaient nouveaux et qu'ils impliquaient une activité inventive au sens des articles 52(1), 54 et 56 CBE.

IV. La requérante (opposante 1) a, dans son acte de recours, sollicité l'annulation de la décision contestée et la révocation du brevet. Dans son mémoire exposant les motifs du recours, elle a en outre requis le renvoi de l'affaire à la première instance, conformément à l'article 11 RPCR.

Cette demande de renvoi est fondée sur l'existence alléguée de vices substantiels de procédure en première instance, qui auraient entraîné la violation du droit d'être entendu de la requérante.

La requérante a également contesté le raisonnement de la division d'opposition au regard des articles 52(2) et 56 CBE en ce qui concerne les revendications indépendantes du brevet tel que maintenu.

V. L'opposante 2, partie de droit à la procédure de recours, n'a pas pris position sur le fond et n'a

formulé aucune requête au cours de la procédure de recours.

VI. Dans sa réponse au recours, l'intimée (titulaire du brevet) a indiqué maintenir « toutes les requêtes déposées en 1ère instance », à savoir la requête principale (correspondant au brevet tel que maintenu) ainsi que les requêtes subsidiaires 1 à 5.

VII. À la suite d'une citation à une procédure orale, la chambre a exposé son avis provisoire dans une notification établie conformément à l'article 15(1) RPCR.

VIII. Par lettre reçue le 4 décembre 2025, l'intimée a déposé six nouvelles requêtes subsidiaires 6 à 11.

IX. La requérante et la partie de droit ont informé la chambre, par lettres reçues respectivement les 1er décembre 2025 et 8 décembre 2025, qu'elles ne participeraient pas à la procédure orale.

X. Par notification du 11 décembre 2025, la chambre a fait part de son opinion préliminaire positive sur la requête subsidiaire 8.

XI. La procédure orale s'est tenue le 15 décembre 2025. L'intimée, seule partie présente, a fait de la requête subsidiaire 8 sa nouvelle requête principale. Après délibération, la décision de la chambre a été prononcée.

XII. Les requêtes finales des parties étaient les suivantes:

La requérante (opposante 1) a demandé l'annulation de la décision contestée et la révocation du brevet ainsi

que le renvoi du dossier à la division d'opposition en raison d'un vice substantiel de procédure.

L'intimée (titulaire du brevet) a demandé que la décision contestée soit annulée et que le brevet soit maintenu sur la base des revendications de la requête subsidiaire 8 telle que déposée avec la lettre du 4 décembre 2025, ou sur la base de l'une des requêtes déposées devant la division d'opposition (requête « principale » ou requêtes subsidiaires 1-5) ou de l'une des requêtes subsidiaires 6, 7 ou 9 à 11 déposées avec la lettre 4 décembre 2025.

La partie de droit à la procédure (opposante 2) n'a pas formulé de requêtes dans le cadre de la procédure de recours.

XIII. Les revendications indépendantes 1 et 4 selon la requête subsidiaire 8 sont libellées comme suit :

« 1. 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 secret, sur une courbe elliptique vérifiant l'équation :

$$Y^2 = f(X);$$

et à partir de polynômes $X_1(t)$, $X_2(t)$, $X_3(t)$ et $U(t)$ vérifiant l'égalité de Skalba suivante :

$$f(X_1(t)) \cdot f(X_2(t)) \cdot f(X_3(t)) = U(t)^2$$

dans le corps fini Fq [sic], quel que soit le paramètre t, q vérifiant l'équation q = 3 mod 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 $X_1=X_1(t)$, $X_2=X_2(t)$, $X_3=X_3(t)$ et $U=U(t)$

/ii/ si le terme $f(X_1).f(X_2)$ est un terme au carré dans le corps fini F_q, alors tester si le terme $f(X_3)$ est un terme au carré dans le corps fini F_q et calculer la racine carré du terme $f(X_3)$, le point P ayant pour abscisse X_3 et pour ordonnée la racine carrée du terme $f(X_3)$;

/iii/ sinon tester si le terme $f(X_1)$ est un terme au carré dans le corps fini F_q et dans ce cas, calculer la racine carré du terme $f(X_1)$, le point P ayant pour abscisse X_1 et pour ordonnée la racine carrée du terme $f(X_1)$;

/iv/ sinon calculer la racine carrée du terme $f(X_2)$, le point P ayant pour abscisse X_2 et pour ordonnée la racine carrée 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,

dans lequel :

- les polynômes vérifiant l'égalité de Skalba sont tels qu'il est possible de fixer la valeur de $X_3(t)$ pour tout t possible, tel que $f(X_3(t))$ ne soit jamais un terme au carré dans F_q,
- à l'étape /2/-/ii/, le terme $f(X_1).f(X_2)$ n'est pas un terme au carré dans le corps fini F_q,
- et, à l'étape /2/-/iii/, on teste si le terme $f(X_1)$ est un terme au carré dans le corps fini F_q selon les étapes suivantes :
  - calculer R2' tel que :

$$R'_2 = f(X_1)^{q-1-\frac{q+1}{4}}$$

  - calculer R3' tel que :

$$R'_3 = R'^2_2$$

- calculer R4' tel que :

$$R'_4 = R'_3 \cdot f(X_1)$$

dans lequel, si R_4' [sic] n'est pas égal à 1, à l'étape /2/-/iv/, on obtient la racine carré de $f(X_2)$ selon l'équation suivante :

$$\sqrt{f(X_2)} = R_1 R'_2$$

où

$$R_1 = (f(X_1) \cdot f(X_2))^{\frac{q+1}{4}}$$

»

« 4. Dispositif électronique comprenant des moyens adaptés pour la mise en œuvre d'un procédé d'exécution d'un calcul cryptographique selon l'une quelconque des revendications 1 à 3. »

XIV. Étant donné l'issu du présent recours, il n'y a pas lieu de reproduire le libellé des revendications des autres requêtes.

Motifs de la décision

Requête de tenue de la procédure orale par visioconférence

1. L'intimée et la requérante ont demandé que la procédure orale se tienne par visioconférence.

2. Conformément à l'article 15bis(1) RPCR, la chambre peut décider de tenir une procédure orale au sens de l'article 116 CBE par visioconférence lorsqu'elle le juge approprié, soit sur requête d'une partie, soit d'office.

3. En l'espèce, la chambre a estimé que la tenue d'une procédure orale par visioconférence n'était pas appropriée, compte tenu de la complexité de l'affaire, tant sur le fond que sur le plan procédural, de la

présence initialement attendue des trois parties, ainsi que de la nécessité d'une traduction simultanée. Le fait qu'une autre chambre de recours ait tenu une procédure orale par visioconférence dans une affaire similaire (T 540/21), comme l'a fait valoir l'intimée, ne saurait limiter le pouvoir d'appréciation de la chambre dans la présente affaire.

Pour ces raisons, la chambre a rejeté cette requête par notification du 13 novembre 2025, confirmant que la procédure orale fixée le 15 décembre 2025 se tiendrait en présentiel.

4. La chambre relève que cette décision a été prise avant que la requérante et la partie de droit n'indiquent qu'elles ne participeraient pas à la procédure orale (par leurs lettres reçues respectivement le 1er décembre 2025 et le 8 décembre 2025). L'intimée n'a pas réitéré sa requête de tenue de la procédure orale par visioconférence à la lumière de ce développement et a été représentée à la procédure orale.

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

5. La requérante a fait valoir, en substance, que la division d'opposition n'a pas respecté son droit d'être entendue, au motif que les motifs de la décision contestée n'expliqueraient pas pourquoi certains de ses arguments à l'appui de ses objections fondées sur les articles 52(2) et 56 CBE n'avaient pas été retenues par la division d'opposition.

5.1 Dans son mémoire exposant les motifs du recours, la requérante a affirmé avoir soutenu lors de la procédure orale (en se référant aux points 3.3, 3.3.1, 3.3.2 et

4.1 du procès-verbal de la procédure orale du 4 février 2021) que l'objet de la revendication 1 selon la requête principale ne dépassait pas une simple juxtaposition de cryptographie et d'un composant électronique. Selon elle, en raison de l'emploi du terme « dans » au lieu de « par » dans la revendication 1, les opérations du procédé revendiqué n'étaient pas effectuées par le composant électronique. La cryptographie constituant un sous-ensemble des mathématiques, l'objet revendiqué relèverait ainsi d'une méthode purement mathématique au sens de l'article 52(2) CBE.

La requérante a indiqué avoir été surprise que la division d'opposition réponde à ces arguments essentiels par les motifs exposés au point 33 de la décision contestée, selon lesquels, « selon la pratique établie depuis longtemps à l'OEB, la cryptographie est un domaine technique et n'est pas limité à certains domaines partiels de la cryptographie ».

5.2 Elle a en outre fait valoir que son argument présenté lors de la procédure orale (cf. point 5.20 du procès-verbal), selon lequel l'objet de la revendication 1 n'impliquait pas d'activité inventive, suivant l'approche COMVIK, vis-à-vis d'un composant électronique, les aspects mathématiques n'étant pas techniques et l'étape 3 n'étant pas effectuée dans le composant électronique, n'avait pas été pris en compte dans la décision.

5.3 La requérante en conclut que, selon elle, la division d'opposition n'avait pas suffisamment pris en considération ses arguments dans la décision écrite (cf. lettre du 21 avril 2022).

6. L'intimée a fait valoir dans sa réponse au recours que la décision contestée traitait ces arguments aux points 30 à 33 et 36 à 48. Elle a en outre souligné qu'une éventuelle erreur d'appréciation sur le fond ne saurait constituer un vice de procédure.

7. La chambre relève que, au point 22 de la décision contestée, la division d'opposition a considéré qu'il était implicite dans la revendication 1 que le « composant électronique » *exécute* le « calcul cryptographique » et qu'il doit donc s'agir d'un composant électronique apte à effectuer de telles opérations, et non d'un simple composant passif tel qu'un condensateur ou une résistance. Bien que formulée dans le contexte de l'article 83 CBE, cette interprétation est clairement reprise dans l'ensemble de la décision, en particulier pour l'appréciation au titre des articles 52(2) et 56 CBE. Elle répond ainsi, au moins implicitement, à l'argument de la requérante selon lequel l'objet revendiqué ne constituerait qu'une juxtaposition de caractéristiques.

Au point 32, dans le contexte de l'article 52(2) CBE, la division d'opposition a identifié deux « effets techniques supplémentaires » concrets résultant des étapes mathématiques de la revendication 1.

Au point 33, elle a étayé son affirmation selon laquelle la cryptographie constitue un domaine technique dans la pratique de l'OEB en se référant aux exemples figurant dans les Directives de l'OEB (G-II, 3.3), « crypter, décrypter ou signer des communications électroniques ; générer des clés dans un système cryptographique RSA », en précisant que cette liste n'était pas exhaustive. La chambre note également que cet argument avait été essentiellement développé, par

exemple, par l'intimée lors de la procédure orale (cf. point 3.5.1 du procès-verbal).

La chambre est donc d'avis que la division d'opposition a suffisamment pris en compte les arguments de la requérante mentionnés ci-dessus et que, dans cette mesure, le droit d'être entendu au sens de l'article 113(1) CBE n'a pas été violé.

8. La chambre observe par ailleurs que la division d'opposition n'a pas explicitement abordé, dans la partie de la décision relative à l'article 56 CBE (points 36 à 48), une objection fondée sur l'approche COMVIK prenant pour point de départ un simple composant électronique. Toutefois, au point 35, dans le contexte de l'article 54 CBE, elle a expliqué pourquoi, selon elle, les caractéristiques mathématiques de la revendication 1 contribuent à la résolution d'un problème technique et présentent dès lors un caractère technique. Des « effets techniques supplémentaires » associés aux étapes mathématiques de la revendication 1 avaient également été identifiés auparavant au point 32, dans le contexte de l'article 52(2) CBE.

Dans son analyse de l'activité inventive, la division d'opposition s'est appuyée sur ces considérations pour conclure que les caractéristiques distinctives par rapport aux documents D1, D2 et D4 présentaient un caractère technique (décision contestée, point 45).

La chambre estime que ces motifs permettent de comprendre pourquoi la division d'opposition n'a pas opéré de distinction entre caractéristiques techniques et non techniques dans le cadre de l'examen de l'activité inventive et pourquoi elle n'a notamment pas été convaincue par l'objection de la requérante fondée

sur l'approche COMVIK selon laquelle l'objet de la revendication 1 ne présenterait aucune caractéristique technique allant au-delà du composant électronique.

La chambre note également que le lien entre l'appréciation au titre de l'article 52(2) CBE et celle au titre de l'article 56 CBE semble avoir été explicité par la division d'opposition lors de la procédure orale (cf. points 5.20 et 5.21 du procès-verbal).

Il s'ensuit que la division d'opposition a suffisamment pris en compte les arguments de la requérante et que le droit d'être entendu au sens de l'article 113(1) CBE n'a pas été enfreint.

9. Enfin, la chambre rappelle que, même à supposer que certains motifs de la décision contestée soient erronés sur le fond, cela ne saurait constituer en soi un vice de procédure.

10. La chambre n'est donc pas convaincue par les arguments de la requérante relatifs aux vices substantiels de procédure allégués et conclut qu'il n'y a pas lieu de faire droit à la requête en renvoi de l'affaire à la première instance sans examen du fond (article 11 RPCR).

Admission de la requête subsidiaire 8

11. La requête subsidiaire 8 a été déposée par l'intimée avec sa lettre du 4 décembre 2025.

12. La requête subsidiaire 8 ne diffère de la requête subsidiaire 2 qu'en ce que la revendication 1 précise désormais que le paramètre t est « secret ». La requête subsidiaire 2 avait été déposée lors de la première

procédure orale devant la division d'opposition, tenue le 30 septembre 2015, et a été maintenue dans la réponse au présent recours.

13. Cette précision constitue une réaction prévisible et appropriée à l'argument nouveau soulevé par la chambre dans le cadre de l'objection fondée sur les articles 52(1) et 56 CBE, selon lequel l'effet invoqué par l'intimée ne pouvait être considéré comme technique dès lors que la revendication ne requérait pas que le paramètre t soit un secret à protéger (cf. avis provisoire de la chambre, point 30.5 ainsi que points 30.8, 43 et 45).

14. Ni la requérante ni la partie de droit n'ont demandé que la requête subsidiaire 8 ne soit pas admise, alors même qu'elles étaient informées avant la procédure orale, par notification du 11 décembre 2025, que la chambre envisageait d'annuler la décision contestée et de renvoyer l'affaire à la division d'opposition afin de maintenir le brevet sur la base des revendications selon la requête subsidiaire 8, ainsi que d'une description à y adapter. Elles ont choisi malgré tout de ne pas participer à la procédure orale.

15. Dans ces circonstances, la chambre a exercé son pouvoir d'appréciation en vertu de l'article 13(2) RPCR et a admis la requête subsidiaire 8.

L'invention - Interprétation de la revendication 1

16. La présente revendication 1 concerne un « 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 secret, sur une courbe elliptique vérifiant l'équation

$Y^2 = f(X)$ » et définie sur un corps fini F_q avec $q = 3$ mod 4. Ledit procédé comprend des étapes 1, 2 et 3 détaillées dans la revendication.

Les étapes 1 et 2 calculent les coordonnées du point P(X,Y) sur la courbe elliptique à partir d'un paramètre t donné ("obtenu").

L'étape 3 consiste à « utiliser le point P dans une application cryptographique de chiffrement ou de hachage ou de signature ou d'authentification ou d'identification ».

17. La revendication 1 trouve notamment un support dans le mode de réalisation illustré à la figure 3, décrit aux paragraphes [0096] à [0101].

18. Selon la description du brevet, les étapes 1 et 2 sont conçues de sorte que la détermination du point P « consomme le même temps quel que soit le paramètre d'entrée t » ou, plus précisément, « le même nombre d'opérations de même type », les types d'opérations étant le test d'un terme au carré dans F_q ou la détermination d'une racine carrée (paragraphes [0021] et [0022]).

Cela vise à empêcher un attaquant potentiel de déduire le secret associé au paramètre t au moyen d'une analyse du temps de calcul pour la détermination du point P ("timing attack") (paragraphes [0015], [0016], [0023], [0051] et [0064]).

Par ailleurs, la détermination du point P selon les étapes 1 et 2 est également présentée comme étant « efficace car le temps d'opérations lourdes est réduit », une opération « lourde » étant une

exponentiation, tandis que les autres opérations sont considérées comme négligeables au regard du temps requis pour mettre en œuvre d'une exponentiation (paragraphes [0021] et [0027]).

19. "composant électronique"

La requérante a soutenu qu'un « composant électronique » pouvait désigner un composant aussi simple qu'un condensateur ou une résistance, de sorte que les étapes du procédé revendiqué ne seraient pas mises en œuvre par ce composant.

La chambre ne partage pas cette analyse. Elle estime au contraire que la personne du métier comprendrait l'expression « procédé d'exécution d'un calcul cryptographique *dans* un composant électronique » comme impliquant que le calcul cryptographique est exécuté *par* ce composant. Celui-ci ne peut donc pas être un simple composant passif, tel un condensateur ou une résistance, mais doit être un composant électronique apte à exécuter un tel calcul, comme l'a aussi considéré la division d'opposition dans son raisonnement concernant l'article 83 CBE (décision contestée, point 22).

En outre, la chambre considère que le « calcul cryptographique » exécuté dans le composant électronique comprend non seulement les étapes 1 et 2, mais également l'étape 3, dès lors que le procédé revendiqué « comprend » les étapes 1 à 3.

20. « paramètre t secret », « application cryptographique »

L'étape 1 consiste à obtenir une valeur du paramètre t. La revendication 1 spécifie qu'il s'agit d'un paramètre

t « secret », la chambre interprète cette caractéristique comme signifiant que t représente une information qui, dans le contexte de l'application cryptographique mentionnée à l'étape 3, doit être protégée contre un attaquant potentiel (cf. paragraphes [0016], [0051] et [0064]).

La description fournit un exemple d'« application cryptographique » au sens de l'étape 3, à savoir l'authentification par mot de passe selon le protocole PACE (« Password Authenticated Connection Establishment ») (paragraphe [0117]). Dans le contexte de ce protocole, un point P sur une courbe elliptique doit être généré à partir du mot de passe d'un utilisateur, avant d'être utilisé dans le protocole. Le paramètre t est dérivé du mot de passe et représente ainsi lui-même un « secret » (paragraphes [0016] et [0044]).

21. étape 2, "sous étape" 2(ii)

L'étape 2 consiste à déterminer un point P sur la courbe elliptique à partir du paramètre t. La revendication précise que cette étape comprend les sous-étapes 2(i) à 2(iv).

Pour les raisons exposées ci-après, la chambre considère que la « sous-étape » 2(ii) mentionnée dans la revendication ne fait effectivement pas partie du procédé revendiqué, comme l'a relevé la requérante.

21.1 La sous-étape 2(i) consiste à évaluer (calculer) de polynômes $X_1(t)$, $X_2(t)$, $X_3(t)$ et $U(t)$ pour la valeur obtenue du paramètre t. Cela présuppose la

disponibilité de polynômes $X_1(t)$, $X_2(t)$, $X_3(t)$ et $U(t)$ tels que définis dans la revendication 1.

Une première exigence de la revendication 1 est que ces polynômes vérifient l'égalité de Skalba

$$f(X_1(t)) \cdot f(X_2(t)) \cdot f(X_3(t)) = U(t)^2$$

dans le corps fini F_q, quelle que soit la valeur du paramètre t.

Une deuxième exigence est que ces polynômes soient tels qu'« il est possible de fixer la valeur de $X_3(t)$ pour tout t possible, tel que $f(X_3(t))$ ne soit jamais un terme au carré dans F_q ». Cette exigence est satisfaite, par exemple, lorsque le polynôme $X_3(t)$ est constant, $X_3(t) = u$ pour tout t, u étant choisi de telle sorte que f(u) ne soit pas un carré dans F_q, comme cela est possible avec la famille de polynômes d'Ulas décrite au paragraphe [0098] du brevet.

Une troisième exigence est que le terme $f(X_1(t)).f(X_2(t))$ - considéré à la « sous étape » 2(ii) - ne soit « pas un terme au carré dans le corps fini F_q ».

Du fait que les polynômes satisfont l'équation de Skalba, cette troisième exigence est mathématiquement équivalente à la condition selon laquelle le terme $f(X_3(t))$ n'est pas un terme au carré dans F_q. La personne du métier reconnait cette équivalence, laquelle est également mentionnée au paragraphe [0057] du brevet.

La chambre déduit de la combinaison des deuxième et

troisième exigences que les polynômes utilisés dans la revendication 1 sont tels que $f(X_3(t))$ - et, par conséquent, aussi le terme $f(X_1(t)).f(X_2(t))$ - ne soit *jamais* un terme au carré dans F_q, *quelque soit la valeur de t*. Cette situation correspond au mode de réalisation illustré à la figure 3, cf. paragraphes [0096] et [0100] du brevet.

21.2 La revendication 1 mentionne une « sous étape » 2(ii) formulée comme suit : « si le terme $f(X_1).f(X_2)$ est un terme au carré dans le corps fini F_q, alors tester [...] et calculer [...] ». Or, comme expliqué ci-dessus, dans le procédé selon la revendication 1, cette condition ne peut jamais être remplie, pour aucune valeur de t.

La chambre constate en outre que la revendication 1 n'exige pas qu'il soit « testé » ou « décidé », au cours du procédé revendiqué, si le terme $f(X_1).f(X_2)$ est un terme au carré dans le corps fini F_q.

Pour ces raisons, la chambre interprète la revendication 1 comme n'exigeant pas que le procédé revendiqué comprenne effectivement cette « sous étape » 2(ii). Seules les sous-étapes 2(i), 2(iii) et 2(iv) sont mises en œuvre.

Cette interprétation est conforme au mode de réalisation illustré à la figure 3, dans lequel « les étapes 211 à 216 [qui implémentent les sous-étapes 2(iii) et 2(iv)] seulement peuvent être mises en œuvre » (paragraphe [0100] du brevet).

21.3 La chambre relève enfin que la revendication manque manifestement de clarté en ce qui concerne la mention d'une « sous étape » 2(ii) qui n'est en fait pas

réalisée. Toutefois, une objection au titre de l'article 84 CBE ne peut être soulevée, ce défaut de clarté ne résultant pas de modifications apportées au brevet, mais étant déjà présent dans la revendication dépendante 4 telle que délivrée (G 3/14).

22. sous-étapes 2(iii) et 2(iv)

22.1 Les sous-étapes 2(iii) et 2(iv) déterminent d'abord lequel des termes $f(X_1(t))$ et $f(X_2(t))$ est un carré dans F_q en ne testant que $f(X_1(t))$ (puisque, en vertu de l'égalité de Skalba et du fait que $f(X_3(t))$ n'est pas un carré, l'un des deux termes $f(X_1(t))$ et $f(X_2(t))$ doit nécessairement être un carré). Elles consistent ensuite à calculer les coordonnées du point P(X,Y) sous la forme $(X_i,\sqrt{f(X_i)})$, avec i=1 ou 2, en fonction du résultat de ce test.

22.2 L'homme du métier sait, au regard de ses connaissances générales, que dans un corps fini F_q avec $q = 3 \bmod 4$, tester si un élément est un carré et le calcul d'une racine carré peuvent chacun être mis en œuvre au moyen d'une exponentiation (cf. D20, page 27, et D9, page 155, corollaire 7.1.2 et preuve ; voir aussi les paragraphes [0012] et [0024] du brevet).

Le choix des polynômes définis par la revendication 1 combiné avec la mise en œuvre particulière des sous-étapes 2(iii) et 2(iv) telle que spécifiée dans cette revendication implique que la détermination du point P soit réalisée *en effectuant au maximum deux exponentiations*, quelle que soit la valeur du paramètre t - au lieu des quatre exponentiations qu'exigerait une approche naïve, comme indiqué au paragraphe [0095] du brevet.

La chambre relève qu'une réduction à une seule exponentiation, mentionnée aux paragraphes [0097] et [0101] du brevet, n'est obtenue que dans le mode de réalisation de la revendication dépendante 2, en combinaison avec les calculs représentés à la figure 3.

Règle 80 CBE, articles 83, 84, 123(2) et (3) CBE

23. La revendication 1 de la présente requête correspond à la revendication indépendante 6 du brevet maintenu sous forme modifiée par la division d'opposition, à laquelle a simplement été ajoutée la précision selon laquelle le paramètre t est « secret ».

Les revendications 2 à 4 correspondent respectivement aux revendications 7 à 9 du brevet maintenu.

Les revendications 1 et 2 à 5 du brevet maintenu ont été supprimées.

24. La requérante et la partie de droit n'ont pas contesté en recours les conclusions de la division d'opposition selon lesquelles le brevet maintenu satisfaisait aux exigences de la règle 80 CBE et des articles 83, 84 et 123(2) et (3) CBE (décision contestée, points 16 à 29), comme relevé par la chambre dans son avis provisoire (point 18). La chambre ne voit aucune raison de s'écarter de ces conclusions.

Comme l'a indiqué l'intimée dans sa lettre du 4 décembre 2025, l'ajout de la caractéristique « t secret » découle directement et sans ambiguïté du passage de la demande telle que déposée (page 3, lignes 1 à 10). Cet ajout restreint la portée de la revendication 1 et répond ainsi au motif d'opposition de défaut d'activité inventive au titre de l'article

100(a) CBE. Il ne remet pas en cause la conclusion quant à l'article 83 CBE.

La suppression des revendications 1 à 5 du brevet maintenu répond également au motif d'opposition de défaut d'activité inventive, article 100(a) CBE.

La chambre conclut dès lors que le présent jeu de revendications satisfait aux exigences de la règle 80 CBE et des articles 83, 84 et 123(2) et (3) CBE, sous réserve d'une adaptation de la description à ce jeu de revendications.

Article 52(2) et (3) CBE

25. La requérante a soutenu, à l'encontre de la revendication 1 du brevet tel que maintenu — similaire sur ce point à la présente revendication 1 — que son objet ne constituait qu'une juxtaposition sans lien fonctionnel de cryptographie, relevant selon elle des mathématiques en tant que telles, et d'un composant électronique, et qu'il était dès lors exclu de la brevetabilité au titre de l'article 52(2) CBE.

La division d'opposition a conclu que cet objet n'était pas exclu de la brevetabilité au titre de l'article 52(2) et (3) CBE, son raisonnement reposant notamment sur la considération selon laquelle la cryptographie constitue un « domaine technique » (décision contestée, points 31 et 33).

26. Comme exposé au point 19 ci-dessus, la chambre interprète la revendication 1 en ce sens que les étapes 1 à 3 sont mises en œuvre par le « composant électronique ».

27. Dès lors, le procédé selon la revendication indépendante 1 présente un caractère technique du seul fait qu'il met en œuvre un moyen technique — à savoir un « composant électronique » — pour l'exécution d'au moins une partie de ses étapes. Il constitue ainsi une « invention » au sens de l'article 52(1) CBE et n'est, par conséquent, pas exclu de la brevetabilité au titre de l'article 52(2) et (3) CBE (cf. T 258/03 Méthode d'enchère/HITACHI, sommaire I et points 3.1 et 4.5 ; T 154/04 Evaluation des performances de vente/DUNS LICENSING ASSOCIATES, point 5(B) et (C) ; G 1/19 Simulation de flux de piétons, points 28 à 30). En particulier, il ne constitue pas une méthode mathématique « en tant que telle » au sens de l'article 52(2)(a) et (3) CBE.

28. Le dispositif selon la revendication indépendante 4, en tant qu'entité physique constituant un moyen technique, n'est pas non plus exclu de la brevetabilité au titre de l'article 52(2) et (3) CBE.

29. La chambre observe que la question de savoir si *la cryptographie* relève des « mathématiques en tant que telles » ou constitue un « domaine technique » n'est pas déterminante pour apprécier si le procédé selon la revendication 1 est exclu de la brevetabilité au titre de l'article 52(2) et (3) CBE.

29.1 À titre d'exemple, un procédé de cryptage d'un message, dont la formulation de la revendication n'exclurait pas une *mise en œuvre entièrement mentale*, engloberait une méthode dans l'exercice d'activités intellectuelles en tant que telles, exclue de la brevetabilité selon l'article 52(2)(c) et (3) CBE, et ne constituerait donc pas une « invention » au sens de l'article 52(1) CBE (cf. T 914/02 Core loading arrangement/GENERAL

ELECTRIC, points 2.3.3 et 2.3.8 ; T 471/05 Designing an optical system/PHILIPS, points 2.1 et 2.2 ; T 1924/17 Data consistency management/ACCENTURE GLOBAL SERVICES, point 19.3).

29.2 En outre, un procédé de cryptage d'un message, revendiqué en tant que procédé *purement abstrait*, sans que l'utilisation d'un moyen technique pour sa mise en œuvre ne soit impliquée par la revendication, serait dépourvu de caractère technique et ne constituerait donc pas davantage une « invention » au sens de l'article 52(1) CBE (cf. T 930/05 Modellieren eines Prozessnetwerks/XPERT, points 3 et 3.1 ; T 471/05, points 2.1 et 2.2 ; T 1924/17, points 19.3 et 19.4 ; G 1/19, point 29).

29.3 Dans la décision T 540/21 Cryptographie sur une courbe elliptique simplifiée/IDEMIA, relative à un cas similaire au cas d'espèce, il est indiqué au point 6 :

« *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 œuvre des méthodes mathématiques (voir La Jurisprudence des Chambres de recours, 10ième édition, juillet 2022, I.A.2.2.2, et en particulier les décisions T0027/97, T1326/06, et T0556/14)* » (soulignement par la chambre).

La présente chambre ne partage cette appréciation que dans la mesure où aucune « invention » au sens de l'article 52(1) CBE n'est exclue de la brevetabilité au

titre de l'article 52(2) et (3) CBE.

29.4 La chambre note que la décision T 27/97 Cryptographie à clés publiques/FRANCE TELECOM est antérieure au développement de la jurisprudence aujourd'hui établie relative aux notions d'« invention » au sens de l'article 52(1) CBE, de « caractère technique » et d'exclusion de la brevetabilité selon l'article 52(2) et (3) CBE, telle qu'établie notamment dans les décisions T 258/03 et T 154/04. À l'époque de la décision T 27/97, l'implication de moyens techniques n'était ni une condition suffisante ni une condition nécessaire pour qu'un procédé revendiqué ne soit pas exclu de la brevetabilité.

Il semble néanmoins ressortir de la décision T 27/97 que la chambre y avait interprété le procédé de cryptage ou de décryptage revendiqué comme étant implicitement mis en œuvre par des moyens techniques, en relevant qu'il s'agissait d'une « méthode dans le domaine de l'informatique électronique et des télécommunications » (T 27/97, point 3).

Enfin, les procédés revendiqués dans les affaires T 1326/06 RSA Schlüsselpaarberechnung/GIESECKE & DEVRIENT et T 556/14 Masking a private key/CERTICOM utilisent des moyens techniques pour leur mise en œuvre, tels qu'un ordinateur ou une carte à puce (« smart card ») (cf. T 1326/06, point 5, et T 556/14, points 10 et 11).

Articles 52(1) et 54 CBE

30. La requérante et la partie de droit n'ont soulevé, en recours, aucune objection au titre du manque de nouveauté. La chambre ne voit pas davantage de raison

de mettre en cause la nouveauté des objets des revendications indépendantes 1 et 4. Il s'ensuit que l'exigence de nouveauté prévue aux articles 52(1) et 54 CBE est remplie.

Articles 52(1) et 56 CBE

31. La présente revendication indépendante 1 correspond à la revendication indépendante 6 du brevet maintenu sous forme modifiée par la division d'opposition, à laquelle a uniquement été ajoutée la précision selon laquelle le paramètre t est « secret ».

32. La division d'opposition a estimé que les motifs qu'elle avait retenus pour reconnaître l'activité inventive de la revendication 1 du brevet maintenu s'appliquaient également à la revendication 6, au motif que le procédé selon cette revendication comportait toutes les caractéristiques de la revendication 1 ainsi que des étapes de calcul supplémentaires (décision contestée, point 48).

La requérante a contesté ce raisonnement, en faisant valoir que le procédé selon la revendication 6 du brevet maintenu, correctement interprété, ne comprenait pas la sous-étape 2(ii) du procédé selon la revendication 1.

La chambre donne raison à la requérante sur ce point, pour les raisons exposées au point 21 ci-dessus, ce qui n'a pas été contesté par l'intimée.

33. Cependant, ni la requérante ni la partie de droit n'ont soulevé, en recours, d'objection de défaut d'activité inventive fondée sur un document spécifique de l'état de la technique à l'encontre de la revendication

indépendante 6 du brevet tel que maintenu, et a fortiori de la présente revendication indépendante 1.

La requérante a uniquement formulé, à l'encontre de la revendication indépendante 6 du brevet maintenu, une objection de défaut d'activité inventive *fondée sur l'application de l'approche COMVIK, sans se référer à un document spécifique de l'état de la technique*, comme relevé par la chambre dans son avis provisoire (points 39.3 et 39.4).

C'est donc exclusivement cette objection qui est examinée en détail ci-après en relation avec la présente revendication 1.

34. L'approche "COMVIK" repose sur le principe selon lequel, pour évaluer l'activité inventive d'une invention de type mixte, c'est-à-dire comportant des caractéristiques techniques et non-techniques, il convient de tenir compte de toutes les caractéristiques qui contribuent au caractère technique de l'invention. Cela inclut des caractéristiques qui, considérées isolément, ne sont pas techniques mais qui, dans le contexte de l'invention, contribuent à produire un effet technique servant à résoudre un problème technique, et, ce faisant, contribuent au caractère technique de l'invention. En revanche, les caractéristiques qui ne contribuent pas au caractère technique de l'invention ne peuvent étayer l'existence d'une activité inventive (T 641/00 Deux identités/ COMVIK, sommaire I ; G 1/19, points 31 à 34).

35. Les caractéristiques du procédé selon la revendication 1 relatives à l'utilisation de fonctions $X_1(t)$, $X_2(t)$, $X_3(t)$ et $U(t)$ vérifiant l'égalité de Skalba, au choix de $q = 3 \bmod 4$, et aux étapes 1 et 2 -

y compris leur mise en œuvre par les calculs spécifiés dans la revendication - définissent une méthode mathématique déterminant, pour une valeur donnée du paramètre t, un point P(X,Y) sur une courbe elliptique.

36. La question qui se pose est de savoir si, *et dans quelle mesure*, cette méthode mathématique sous-jacente à la revendication 1 contribue à la production d'un effet technique permettant de résoudre un problème technique *dans le contexte de l'invention selon la revendication 1*.

37. La division d'opposition a considéré que tel était le cas pour l'ensemble de cette méthode, dans une version de la revendication ne comportant pas la limitation « t secret » (cf. décision contestée, points 35 et 48). Les principaux arguments avancés à l'appui de cette conclusion peuvent être résumés comme suit :

(a) le problème de la détermination d'un point sur une courbe elliptique est bien connu dans le domaine de la cryptographie, de même que les diverses applications cryptographiques dans lesquelles le point obtenu peut être utilisé, une référence étant faite notamment à D21, page 190, section 4.45 (cf. décision contestée, points 23 et 31) ;

(b) la « détermination d'un point sur une courbe elliptique pour une application cryptographique » constitue un effet technique supplémentaire obtenu par le procédé revendiqué, lequel présente par ailleurs un caractère technique en tant que tel (cf. décision contestée, points 32 et 35) ;

(c) selon la pratique établie de l'OEB, la cryptographie est un domaine technique, sans être

limitée aux sous-domaines mentionnés dans les Directives de l'OEB, G-II, 3.3, et l'étape 3 prévoit en outre des applications de chiffrement et de signature (cf. décision contestée, point 33) ;

(d) le procédé est conçu de telle sorte que le nombre d'exponentiations, et donc, dans une certaine mesure, le temps d'exécution du calcul, soient indépendants du paramètre d'entrée t, ce qui rend la détermination du point sur la courbe elliptique moins sensible aux attaques fondées sur l'observation du temps d'exécution (cf. décision contestée, points 29, 31, 32 et 35).

38. La requérante a soutenu que la cryptographie ferait partie des mathématiques et ne constituerait pas un domaine technique, et que la revendication 1 serait dépourvue d'activité inventive en ce qu'elle n'apporterait aucune contribution technique vis-à-vis d'un composant électronique.

39. L'intimée a, pour sa part, fait valoir que le problème technique résolu par l'invention consistait à « mettre en œuvre un calcul en temps quasi-constant, c'est-à-dire [de] réaliser toujours le même nombre d'opérations de même type, indépendamment du temps d'exécution de chaque opération », indépendamment de la durée d'exécution de chaque opération, en particulier en ne testant qu'une seule fois si un terme est un carré et en ne calculant qu'une seule fois une racine carrée (lettre du 4 décembre 2025, page 3).

40. Les considérations de la chambre sont les suivantes.

40.1 S'agissant des arguments (a) et (b), la chambre estime que la conception d'une méthode mathématique permettant d'obtenir un point P(X,Y) sur une courbe elliptique

$Y^2=f(X)$ à partir d'au moins un paramètre t est, *en tant que telle*, un problème de nature *non-technique*, appartenant au domaine mathématique de la théorie algorithmique des nombres.

Le seul fait qu'une telle méthode puisse trouver des applications techniques — fussent-elles nombreuses et connues — ne suffit pas, en soi, à lui conférer un caractère technique (G 1/19, point 124).

40.2 La revendication 1 prévoit, à l'étape 3, cinq alternatives d'utilisation du point P dans une « application cryptographique » : « chiffrement », « hachage », « signature », « authentification » ou « identification ».

Or, la revendication ne spécifie pas, à l'étape 3, le rôle concret du paramètre t ni celui du point P dans chacune de ces applications cryptographiques.

40.3 En l'absence de la précision selon laquelle le paramètre t est « secret » (comme c'était le cas pour la revendication 6 du brevet maintenu), il ne serait pas établi que *les étapes 1 et 2* de détermination du point P fasse *partie intégrante* de l'application cryptographique mentionnée à l'étape 3.

Ainsi, comme la chambre l'a exposé en détail dans son avis provisoire (points 30.2 et 30.3), certaines applications cryptographiques de chiffrement - notamment celles fondées sur un échange de clés de type Diffie-Hellman - utilisent un point P sur courbe elliptique (nommé « générateur ») fixe et publique (par exemple défini par une norme).

Dans un tel contexte, le fait que ce point P fixe et

public ait été obtenu *au préalable* à partir d'un paramètre t quelconque (ne représentant pas un secret à protéger) au moyen des étapes 1 et 2 ne contribuerait pas aux effets techniques produits par l'application cryptographique - sauf si ces étapes ne conféraient au point ainsi généré une propriété mathématique spécifiquement pertinente pour l'application cryptographique considérée, ce qui n'a pas été allégué par l'intimée. En outre, empêcher que la valeur du paramètre t puisse être déduite au moyen d'une attaque fondée sur le temps de calcul n'aurait aucune pertinence technique dans un tel contexte car t ne représenterait pas un secret à protéger.

40.4 En revanche, dans la présente revendication 1, il est expressément indiqué que le paramètre t est « secret », ce que la chambre interprète comme impliquant que t représente une information qui, dans le contexte de l'application cryptographique mentionnée à l'étape 3, doit être protégée contre un attaquant potentiel (cf. point 20 ci-dessus).

40.5 La requérante a soutenu, à l'encontre de la revendication 1 du brevet maintenu, que l'effet invoqué par l'intimée et retenu par la division d'opposition (cf. point 39, argument (d)) n'était pas obtenu par le procédé revendiqué, notamment parce que cette revendication ne permettait pas d'inférer le nombre d'exponentiations mises en œuvre aux étapes 1 et 2 — objection que la chambre a suivie dans son avis provisoire (point 30.5).

La chambre estime toutefois que tel est le cas pour la présente revendication 1, laquelle précise en

particulier les calculs mis en œuvre pour réaliser les sous-étapes 2(iii) et 2(iv) (cf. point 22.2 ci-dessus).

40.6 Les étapes 1 et 2, mises en œuvre par le composant électronique, réalisent ainsi une partie de l'application cryptographique - à savoir la transformation d'un paramètre t, représentant un secret à protéger, en un point P sur la courbe elliptique - de manière efficiente, tout en empêchant que ce secret puisse être compromis, au cours de cette transformation, par une attaque fondée sur le temps d'exécution, ce que la chambre considère, en combinaison, comme étant un *effet technique* (voir, pour un cas similaire, T 556/14, point 13.3).

40.7 La chambre estime que, dans la mesure où les étapes 1 et 2 contribuent à un effet technique dans le cadre de l'invention, elles ne sauraient être entièrement ignorées dans l'appréciation de l'activité inventive, contrairement à ce que soutient l'objection de la requérante.

La chambre ne fait donc pas droit à cette objection.

41. *Remarques concernant la séparation entre caractéristiques contribuant et ne contribuant pas au caractère technique de l'invention*

La chambre souligne que, pour parvenir à cette conclusion, elle n'a pas eu à trancher définitivement la question de savoir si les étapes 1 et 2 contribuent *entièrement, dans tous leurs détails mathématiques,* au caractère technique de l'invention.

41.1 Le fait que les étapes 1 et 2 contribuent à l'effet technique identifié au point 40.6 ci-dessus fonde une

présomption selon laquelle ces étapes contribuent, *dans leur ensemble*, au caractère technique de l'invention et *exclut* qu'elles puissent être *entièrement ignorées* dans l'appréciation de l'activité inventive.

41.2 Il n'est toutefois pas exclu que certains détails mathématiques des étapes 1 et 2 - par exemple le fait que les sous-étapes 2(iii) et 2(iv) concernent respectivement les termes $f(X_1)$ et $f(X_2)$ (et non l'inverse) - soient arbitraires au regard de l'obtention de l'effet technique identifié (et de tout autre effet technique) et ne contribuent donc pas au caractère technique de l'invention.

41.3 Cette discussion a eu lieu dans la procédure de recours au regard à la revendication 1 telle que maintenue, la chambre ayant identifiée dans son avis provisoire que certains détails mathématiques du procédé selon cette revendication, *qui subsistaient après comparaison avec une modification évidente de l'enseignement du document D4*, n'avaient pas de pertinence technique et ne pouvait donc pas étayer une activité inventive (cf. avis provisoire, point 36). L'intimée a contesté ce raisonnement, le considérant comme n'étant pas conforme à l'approche COMVIK (lettre du 4 décembre 2025).

41.4 La chambre relève qu'un raisonnement similaire a été adopté dans la décision T 27/97, relative à un procédé pour crypter ou décrypter un message. Ce n'est en effet qu'après comparaison avec une combinaison de deux documents de l'état de la technique que la chambre a constaté qu'un détail mathématique subsistant ne contribuait pas à un effet technique et ne pouvait, dès lors, étayer l'existence d'une activité inventive (cf. T 27/97, point 4.4).

41.5 Un tel raisonnement est conforme au principe fondamental de l'approche COMVIK, tel qu'énoncé au sommaire I de la décision T 641/00 (repris dans G 1/19, point 31) :

« Lorsqu'une invention se compose d'un ensemble de caractéristiques techniques et non techniques et qu'elle présente globalement un caractère technique, l'exigence d'activité inventive doit être appréciée en tenant compte de toutes les caractéristiques qui contribuent audit caractère technique, les caractéristiques qui n'apportent pas une telle contribution ne pouvant étayer l'existence d'une activité inventive. »

Ce principe est indépendant du moment auquel, dans l'analyse de l'activité inventive, il est constaté qu'une caractéristique ne contribue pas au caractère technique de l'invention. À cet égard, on notera que la décision T 641/00 cite expressément, à son point 6, la décision T 27/97 comme venant étayer ce principe.

41.6 En théorie, il est toujours possible de déterminer si une caractéristique d'une invention contribue ou non à son caractère technique indépendamment de toute comparaison avec l'état de la technique, car il s'agit d'une propriété inhérente à l'invention (cf. T 1358/09 Classification/BDGB ENTERPRISE SOFTWARE, point 5.4 ; T 2230/10 Context-based information retrieval/PHILIPS, point 3.6 ; T 697/17 SQL Extensions/MICROSOFT TECHNOLOGY LICENSING, points 5.2.1 et 5.2.2 ; T 619/02 Sélection d'odeurs/QUEST INTERNATIONAL, sommaire III ; T 154/04, points 5(E) et 5(F) ; G 1/19, points 38 et 39).

En pratique, il peut toutefois s'avérer difficile

d'identifier de manière exhaustive l'ensemble des caractéristiques d'une invention qui contribuent à son caractère technique et celles qui n'y contribuent pas.

Ainsi, dans la décision T 258/03, point 3.6, il a été observé ce qui suit :

« [Il] est souvent difficile de séparer dans une revendication les caractéristiques techniques et celles qui ne le sont pas, et une invention peut comporter des aspects techniques qui sont "dissimulés" dans un contexte largement non technique. »

La chambre observe que l'inverse peut également se produire, à savoir des aspects non-techniques peuvent être « dissimulés » dans un contexte largement technique.

41.7 Une approche pragmatique dans de tels cas est de ne pas effectuer cette séparation technique/non-technique pour l'ensemble de l'objet revendiqué, mais à passer directement à une comparaison de l'invention avec l'état de la technique et de limiter ainsi cette séparation aux caractéristiques distinctives de l'invention par rapport à l'état de la technique « le plus proche », comme cela a été recommandé à plusieurs reprises dans la jurisprudence (cf., par exemple, T 756/06 Displaying a schedule/FUJITSU, point 5, et T 697/17, point 4.3).

41.8 Cette approche n'est toutefois pas applicable lorsqu'il s'agit de statuer sur le bien-fondé d'une objection de manque d'activité inventive reposant essentiellement sur l'argument selon lequel la quasi-totalité des caractéristiques de l'invention ne contribuerait pas à

son caractère technique, comme c'est le cas en l'espèce.

Une autre approche pragmatique est alors possible, consistant à n'effectuer la séparation technique/non-technique *qu'à un degré de granularité suffisant pour pouvoir rejeter cette objection*, sans pour autant exclure, à ce stade, que l'analyse de l'activité inventive à la lueur de l'état de la technique puisse révéler que certains aspects de l'invention ne contribuent pas à son caractère technique.

41.9 Quelle que soit l'approche suivie, ce qui importe est que, si une caractéristique (ou une combinaison de caractéristiques) est finalement considérée comme justifiant une activité inventive de l'invention, il doit en principe être possible d'établir que cette caractéristique contribue au caractère technique de l'invention indépendamment de toute comparaison avec l'état de la technique (en vu du principe fondamental énoncé dans T 641/00, sommaire I).

42. *Remarques concernant la notion de « domaine technique »*

Au regard de la considération de la division d'opposition que « selon la pratique établie depuis longtemps à l'OEB, la cryptographie est un domaine technique » (cf. point 37 ci-dessus, argument (c)), la chambre souligne qu'un tel argument ne saurait en lui-même être suffisant pour conclure que toutes les caractéristiques d'une invention dans ce domaine contribuent nécessairement au caractère technique de cette invention. La décision T 27/97, discutée au point précédent, illustre ce point. Cf. aussi T 52/02, points 2.1 et 3.8.

Cette considération est valable pour tout « domaine technique » ou « domaine technologique » au sens de l'article 52(1) CBE. La jurisprudence offre de nombreux exemples d'inventions relevant de domaines incontestablement « techniques » mais comportant des caractéristiques qui ne contribuent pas à leur caractère technique (cf., parmi d'autres, T 72/95 Ionizing liquid/IBBOTT, point 5.4, cité dans T 641/00, point 6, et G 1/19, point 33).

De plus, la chambre considère que les notions de « domaine technique » ou « domaine technologique » et d'appartenance à un tel domaine sont trop vagues pour servir de critère définitif. Ce qui importe, c'est dans quelle mesure il y a une contribution à la production d'un effet technique servant à résoudre un problème technique (T 761/20 Automated script grading/UNIVERSITY OF CAMBRIDGE, points 18 à 19.2).

43. *Conclusion sur l'activité inventive*

La chambre a donc rejeté l'objection de la requérante qui n'était fondé sur aucun document spécifique de l'état de la technique.

Ni la requérante ni la partie de droit n'ont soulevé en recours d'autre objection pour défaut d'activité inventive - notamment sur la base d'un document spécifique de l'état de la technique - à l'encontre la revendication indépendante 6 du brevet maintenu et, a fortiori, de la présente revendication indépendante 1.

La chambre relève que, dans son avis provisoire (cf. points 31 à 38), elle avait estimé que la revendication 1 du brevet tel que maintenu était dépourvue d'activité d'inventive en partant du document

D4 (ou, à titre subsidiaire, des documents D1 ou de D2), tant au motif qu'aucun problème technique n'était résolu que compte tenu des connaissances générales de la personne du métier, telles qu'illustrées notamment par les documents D3, D9 et D20. Il n'apparaît toutefois pas que cette objection puisse également s'appliquer à la présente revendication 1 (fondée sur la revendication indépendante 6 du brevet tel que maintenu), ce qui n'a d'ailleurs été soutenu ni par la requérante ni par la partie de droit.

La chambre en conclut que la présente revendication indépendante 1 implique une activité inventive au sens des articles 52(1) et 56 CBE. Il en va de même de la revendication indépendante 4.

Conclusion

44. Le brevet modifié selon la requête subsidiaire 8 satisfait donc aux exigences de la CBE, au sens de l'article 101(3)(b) CBE, sous réserve que la description soit adaptée au jeu de revendications.

Dispositif

Par ces motifs, il est statué comme suit

1. La décision contestée est annulée.

2. L'affaire est renvoyée à la division d'opposition afin de maintenir le brevet sur la base des revendications n°1-4 de la requête subsidiaire 8 déposée avec la lettre du 4 décembre 2025 et une description à adapter.

La Greffière : Le Président :

L. Stridde Martin Müller

Décision authentifiée électroniquement