BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [ ] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 26 May 2011

Case Number: T 1852/07 - 3.5.05

Application Number: 03780959.7

Publication Number: 1576763

IPC: H04L 9/18

Language of the proceedings: EN

Title of invention:
Data division method and device using exclusive or calculation

Applicant:
NTT Communications Corp.

Headword:
Data division method and device/NTT

Relevant legal provisions:
EPC Art. 83, 84, 111(1), 123(2)

Relevant legal provisions (EPC 1973):
EPC Art. 106, 107, 108

Keyword:
"Clarity and support - (yes, after amendment)"
"Extension of subject-matter - (no, after amendment)"
"Sufficiency of disclosure - (yes)"
"Remittal to the department of first instance for further prosecution"

Decisions cited:
J 0010/07

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1852/07 **-** 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 26 May 2011

Appellant: NTT Communications Corp.
1-6, Uchisaiwai-cho 1-chome
Chiyoda-ku
Tokyo 100-8019 (JP)

Representative: HOFFMANN EITLE
Patent- und Rechtsanwälte
Arabellastrasse 4
D-81925 München (DE)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 16 July 2007 refusing European patent application No. 03780959.7 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chair: A. Ritzka
Members: P. Corcoran
F. Blumer

Summary of Facts and Submissions

I. This is an appeal against the decision of the examining division to refuse the European patent application No. 03 780 959.7, originally filed as international application PCT/JP2003/016389 and published as WO 2004/057461. The decision was announced in oral proceedings held on 27 June 2007 and written reasons were dispatched on 16 July 2007.

II. The decision under appeal was based on a main request comprising a set of claims 1 to 7 filed with the letter of 15 May 2007 and a first auxiliary request comprising claims 1 to 7 filed during oral proceedings on 27 June 2007.

III. According to said decision, the subject matter of the independent claims of the main request did not meet the requirements of Article 84 EPC and the subject matter of the independent claims of the auxiliary request did not meet the requirements of Article 123(2) EPC

IV. With respect to the independent claims of the main request, the examining division objected *inter alia* to the use of the terms "data division" and "divided data" on the basis that the so-called "division" was in fact a complex mathematical function involving an encryption process rather than a simple arithmetical division (cf. decision: item 1.1 of the Reasons, p.5).

V. Further objections were raised under Article 84 EPC relating to the formulation "such that the original data can be recovered from a prescribed number of the

divided data, which is less than the desired number of division" as recited in claims 1, 6 and 7.

It was objected that it was not possible to recover the original data "from a prescribed number of the divided data which is less than the desired number of divisions" in all cases (cf. decision: item 1.2 of the Reasons, p.6). In particular, with respect to the case where n = 2, it was stated that it was not possible to carry out the claimed invention. On this basis, the examining division found that the aforementioned claims did not clearly define the scope of protection for which it was possible to carry out the invention.

VI. In item 1.3 of the Reasons (cf. decision: p.6-7), it was further objected that the formulation referred to in V. above defined a feature in terms of a result to be achieved, namely that it was possible to reconstruct the original data from the knowledge of a subset. It was also noted in this regard that the application only described the recovery method for some examples involving 3 or 4 divisions. It was merely indicated that the data could be recovered "similarly" for greater values of n but it was not disclosed how this was to be performed for a number of division greater than or equal to 5.

VII. The examining division further found that the subject-matter of claim 1 and the further independent claims of the main request failed to meet the requirements of Article 84 EPC with respect to clarity because said claims did not define which inherent property of the "division" enabled subsequent recovery based on a

number of "divided data" less than the desired number of "data divisions".

VIII. In an ***obiter dictum*** to the impugned decision (cf. decision: "Remarks", p.9), it was stated that the objection under Article 84 EPC could also be considered as an objection due to insufficient disclosure of the invention under Article 83 EPC. In this regard, the examining division alleged that the disclosure of the recovery method was limited to some examples for 3 or 4 divisions accompanied by a further statement to the effect that the data could be recovered "similarly" for higher values of n. In particular, it was stated that the applicant had not disclosed how to recover the data for n >= 5 nor had an example of recovery for 3 "divided data" been disclosed for n = 4.

IX. Notice of appeal was received at the EPO on 29 August 2007 with the appropriate fee being paid on the same date. A statement setting out the grounds of appeal was received at the EPO on 25 October 2007. With the statement setting out the grounds of appeal the appellant filed a new main request and a new auxiliary request, both requests comprising claims 1 to 7.

X. In a communication accompanying a summons to oral proceedings to be held on 26 May 2011 the board expressed reservations as to whether the appellant's requests complied with the requirements of the EPC, in particular the requirements of Article 84 EPC. The appellant was advised that should it succeed in overcoming the board's objections in this respect, the board was inclined to remit the case to the department of first instance for further prosecution.

XI. In its communication the board made reference *inter alia* to the following documents:

D5: A. SHAMIR: "How to Share a Secret", Communications of the ACM, Vol. 22, No. 11, pp. 612-613, November 1979.

D6: G. J. SIMMONS: "An Introduction to Shared Secret and/or Shared Control Schemes and Their Application", Chapter 14 of "Contemporary Cryptology" (ed. G.J. Simmons), pp.441-497, 1992 IEEE Press, ISBN 0-7803-5352-8.

D5 is cited on p.1 l.25-28 of the published application.

D6 is a textbook extract cited by the board as evidence of the relevant general knowledge of the skilled person

XII. The board further noted that it was not inclined to concur with the examining division's comments to the effect that the application failed to provide a sufficient disclosure of the invention and expressed the preliminary opinion that the application disclosed the claimed invention in a manner sufficiently clear and complete for it to be put into practice as required by Article 83 EPC.

XIII. With a letter of reply dated 26 April 2011, the appellant filed a new request comprising claims 1 to 7 to replace the requests on file.

XIV. At the oral proceedings held as scheduled on 26 May 2011, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1 to 6 filed during the oral proceedings as a sole request.

The further documents on which the appeal is based, i.e. the text of the description and the drawings, are as follows:

Description, pages:

2, 6-11, 13-18, 20-44, 46-55 as published;
1, 3, 5 as filed with the letter dated 21 April 2006;
4, 12 as filed with the letter dated 27 July 2006;
19, 45 as filed during the oral proceedings before the board.

Drawings, sheets:

1/13-13/13 as published.

XV. Claim 1 of the appellant's request reads as follows:

"A data division method implemented by a computer, for dividing original data into as many divided data as a specified number n of divisions, comprising the steps of:

generating a plurality of original partial data by dividing the original data by a prescribed processing unit bit length;

generating a plurality of random number partial data each having a length equal to the prescribed processing unit bit length, from a random number having a length less than or equal to a bit length of the original data, the plurality of random number partial data being generated in correspondence to the plurality of original partial data;

generating a plurality of divided partial data that constitute each divided data by using exclusive OR

calculation of the original partial data and the random number partial data; and

generating the divided data in the specified number of divisions from the plurality of divided partial data, such that the original data can be recovered from a prescribed number of the divided data, which is less than the specified number of divisions, wherein the original data can be recovered from (n+1) [*sic*] sets of divided data if n is an odd number or (n/2)+1 sets of the divided data is an even number [*sic*] such that two divided data for which a difference in the number of calculations is one or the n-th divided data and any other divided data are contained among them; and

wherein when the original data, the random number, the divided data, the specified number of divisions and the processing unit bit length are denoted as S, R, D, n ≥ 3 and b, respective1y, variab1es i (= 1 to n) and j (= 1 to n—1) are used as variables, each one of (n-1) sets of the original partial data, (n-1) sets of the random number partial data, n sets of the divided data D, and (n-1) sets of divided partial data of each divided data are denoted as S(j), R(j), D(j), and D(i,j), respectively, each original partial data S(j) is generated as b bits of data from bx(j-l)+1-th bit of the original data S while changing a variable j from 1 to n—1, U[n,n] is an nxn matrix with u(i,j) indicating a value of i—th row and j-th column given by:

u(i,j) = 1 when i+j ≤ n+1
u(i,j) = 0 when i+j > n+1

P [n,n] is an nxn matrix with p(i,j) indicating a value of i-th row and j-th column given by:

p(i,j) = 1 when j = i—1
p(i,j) = 1 when i = n, j = 1
p(i,j) 0 otherwise

c(j,i,k) is defined as a value of i-th row and k-th column of an (n-1)x(n-1) matrix U[n-1,n-1]xP[n-1,n-1]^(j-1), where U[n-1,n-1]xP[n-1,n1]^(j-1) denotes a product of a matrix U[n-1,n-1] and (j-1) sets of a matrix xP[n—1,n-1], and Q(j,i,k) is defined as Q(j,i,k) = R(k) when c (j,i,k) = 1 and Q(j,i,k) = 0 when c(j,i,k) = 0,

each divided partial data D(i,j) is generated by:

$$D(i,j) = S(j)*\left(\prod_{k=1}^{n-1} Q(j,i,k)\right) \text{ when } i < n$$

$$D(i,j) = R(j) \text{ when } i = n$$

while changing a variable i from 1 to n and changing a variable j from 1 to n-1 for each variable i, where

$$\prod_{k=1}^{n-1} Q(j,i,k) = Q(j,i,1)*Q(j,i,2)*\cdots\cdots*Q(j,i,n-1)$$

and * denotes the exclusive OR ca1culation; and

depositing the divided data into a plurality of deposit servers (7a, 7b, 7c)."

Claims 5 and 6 are further independent claims directed respectively towards a corresponding data division device and computer program product.

XVI. During oral proceedings before the board, the appellant initially proposed incorporation of the following text passage into claim 1: "wherein the original data can be recovered from (n+1)/2 sets of divided data if n is an odd number or (n/2)+1 sets of the divided data if n is an even number and two divided data for which a difference in the number of calculations is one or the n-th divided data and any other divided data are contained among them" (emphasis added).

The board suggested that substitution of "such that" for "and" (as emphasised above) would improve the clarity of the text passage. The amended version of the text passage submitted with the appellant's final request reads as follows: "wherein the original data can be recovered from (n+1) [***sic***] sets of divided data if n is an odd number or (n/2)+1 sets of the divided data is an even number [***sic***] such that two divided data for which a difference in the number of calculations is one or the n-th divided data and any other divided data are contained among them"

XVII. At the end of the oral proceedings the chair announced the board's decision.

Reasons for the Decision

1. *Admissibility*

1.1 The appeal complies with the provisions of Articles 106 to 108 EPC 1973 which are applicable according to J 0010/07 (cf. Facts and Submissions, item IX. above). Therefore it is admissible.

2. *Observations re amendments submitted during oral proceedings*

2.1 It is noted that the amended version of the text passage which was submitted with the appellant's final request during oral proceedings (cf. Facts and Submissions, item XVI. above) contains a number of deficiencies which appear to be due to inadvertent omissions from the initially submitted version of said text passage.

2.2 In particular, the specification of "wherein the original data can be recovered from (n+1) sets of divided data if n is an odd number" (emphasis added) is not consistent with the description according to which (n+1)/2 sets of divided data must be acquired in order to ensure that recovery is possible if n is an odd number (cf. published application: p.39 l.30 - p.40 l.9 and p.52 l.13-27).

2.3 Likewise, having regard to the above-cited passages of the description, the formulation "or (n/2)+1 sets of the divided data is an even number" is evidently intended to read "or (n/2)+1 sets of the divided data if n is an even number" (emphasis added).

2.4 In view of the foregoing, the board judges that the aforementioned text passage of claim 1 is intended to be formulated as follows: "wherein the original data can be recovered from (n+1)/2 sets of divided data if n is an odd number or (n/2)+1 sets of the divided data if n is an even number such that two divided data for which a difference in the number of calculations is one

or the n-th divided data and any other divided data are contained among them" (emphasis added).

Such a formulation would be consistent with the above-cited passages of the description and, likewise, with the initially submitted version of said text passage (cf. Facts and Submissions, item XVI. above).

3. *Observations re the subject-matter of the application*

3.1 The present application relates to a type of data processing technique known in the art as a "threshold scheme" (cf. D5: 1. Introduction) or a "shared secret scheme" (cf. D6: 1. Introduction).

3.2 A scheme of the aforementioned type is intended to permit sharing of a specific item of data among a finite set of participants. The original data item, i.e. the "secret", is divided or decomposed into "pieces", also called "shares", which are distributed among the participants (cf. D5: 1. Introduction; D6: 1. Introduction). The original secret can be recovered subsequently from predetermined sets of shares.

3.3 The scheme disclosed in D5 is a so-called "(k, n)-threshold scheme" according to which n shares are generated. By combining a predetermined "threshold" number of shares, k, the original secret can be recovered. The scheme of D5 is based on polynomial interpolation (cf. D5: 2. A Simple (k, n) Threshold Scheme; D6: 1. Introduction).

3.4 According to the present application, such polynomial interpolation techniques for the generation of shares

and recovery of the secret are computationally expensive and, thus, impractical in cases where the secret comprises a very large amount of data (p.2 l.4-28). The present application therefore proposes a scheme according to which a sequence of n "divided data" items, i.e. D(1) ... D(n), are generated based on the use of exclusive OR calculations (cf. p.10 l.8-30; p.53 l.35 - p.54 l.18).

3.5 The general principles underlying the invention are disclosed by way of a general form of the definition formula for generating the divided data, a general form of the division rules for dividing the original data and general division processing in the case where the number of divisions is n (cf. p.20 l.29-32; p.36 l.23-26; p.40 l.10 - p.42 l.34).

Specific embodiments are disclosed for the following cases:

n = 2 (cf. p.44 l.21 - p.45 l.28);
n = 3 (cf. p.47 l.16 - p.50 l.20);
n = 4 (cf. p.50 l.21 - p.51 l.24).

It is further indicated that the aforementioned general principles can be applied "similarily" in cases where n is equal to or greater than 5 (cf. for example, p.51 l.33 - p.52 l.27).

4. *Article 84 EPC*

4.1 Claim 1 is directed towards a data division method implemented by a computer for dividing original data into as many divided data as a specified number n of divisions.

4.2 Having regard to the disclosures of D5 and D6, the board finds that it is not appropriate to construe the term "division" as used in claim 1 in the narrow sense of an arithmetical division operation. In the given context, the expression "data division method" as used in claim 1 is to be interpreted as denoting a method for performing a sequence of data processing operations to generate a plurality of "divided data" items from an original data item such that the original data item can be reconstituted or "recovered" using pre-determined subsets of the "divided data" items. Such an interpretation of the subject-matter of claim 1 is consistent with the disclosures of D5 and D6.

4.3 The term "divided data" as used in claim 1 is thus judged to be substantially identical in meaning to the term "piece" as used in D5 or "share" as used in D6. In the given context, said term is to be understood as denoting an item of data which is generated from the original data and which can be used subsequently in combination with other predetermined items of "divided data" to effect the recovery of the original data.

4.4 Using wording substantially identical to that of dependent claim 7 as originally filed, claim 1 specifies details relating to the generation of the divided data, including the generation of the "divided partial data" D(i,j) that constitute each divided data. The board is satisfied that the wording of claim 1 in this respect is consistent with the general form of the division rules for dividing the original data as disclosed, for example, on p.36 l.23 - p.37 l.25 of the description and that the notation used in the claim

corresponds to that used in the description (cf. p.10 l.31 - p.14 l.12).

4.5 The final step of claim 1 which specifies depositing the divided data into a plurality of deposit servers is supported, for example, by the following passages of the description: p.7 l.23 - p.8 l.1 and p.18 l.14-29.

4.6 In the board's judgement, the objections raised in the impugned decision with respect to the formulation "such that the original data can be recovered from a prescribed number of the divided data, which is less than the desired number of division" (cf. Facts and Submissions, items V. and VI. above) are no longer applicable in view of the amendments to claim 1.

4.7 In this regard it is noted that the case where n = 2 is now excluded from the scope of claim 1 which has been limited to $n \geq 3$.

4.8 The aforementioned formulation has also been amended with the evident intention of specifying in further detail the constraints governing the recovery of the original data (cf. observations under 2.4 above), ***viz.*** that the original data can be recovered from (n+1)/2 sets of divided data if n is an odd number or (n/2)+1 sets of the divided data if n is an even number such that two divided data for which a difference in the number of calculations is one or the n-th divided data and any other divided data are contained among them.

The board takes the view that such a specification does not amount to a definition of the matter for which protection is sought in terms of a result to be

achieved but rather constitutes a limitation specifying that an original data item can be recovered from a subset of the divided data items provided that said subset has a minimum size such that it includes two divided data items which can be used for recovery.

In the board's judgement, a specification to this effect is supported by the following passages of the description: p.27 l.28-33, p.39 l.6 - p.40 l.9 and p.49 l.24 - p.52 l.27.

4.9 Although the wording of claim 1 relating to the aforementioned specification contains deficiencies (cf. observations under 2. above, in particular 2.2 and 2.3), the board is satisfied that these deficiencies could be overcome by amending the relevant passage of the claim so as to render it consistent with p.39 l.30 - p.40 l.9 and p.52 l.13-27 of the description (cf. observations under 2.4 above).

4.10 Concerning the objection that claim 1 does not define which inherent property of the division enables subsequent recovery of the original data based on a number of divided data less than the desired number of data divisions (cf. Facts and Submissions, items VII. above), the board takes the view that a definition of this kind is not required in the present case in order to ensure compliance with the clarity requirements of Article 84 EPC. Referring to the observations under 4.8 above, the board judges that the limitation to cases where $n \geq 3$ is sufficient in this regard (cf. 4.7 above).

4.11 Claim 1 is directed towards a data division method, and is therefore primarily concerned with the division of the original data prior to recovery. For this reason, the board judges that it is not necessary for the claim to include further details relating to the recovery of the original data.

4.12 In view of the foregoing, the board concludes that, subject to amendment as discussed in 4.9 above, claim 1 of the appellant's request can be considered to define the matter for which protection is sought in a manner compliant with the clarity and support requirements of Article 84 EPC. This finding likewise applies to claims 5 and 6. The question of sufficiency of disclosure under Article 83 EPC is dealt with under item 6. below.

5. *Article 123(2) EPC*

5.1 The passages of the description providing support for the amendments to claims 1, 5 and 6 form part of the application documents as originally filed.

5.2 The board additionally notes that the details recited in claim 1 relating to the generation of the divided data, including the generation of the "divided partial data" D(i,j), are based on dependent claim 7 as originally filed.

5.3 In view of the foregoing, the board is satisfied that, subject to amendment as discussed in 4.9 above, claim 1 can be considered to comply with the requirements of Article 123(2) EPC. This finding likewise applies to claims 5 and 6.

6. *Article 83 EPC*

6.1 In an ***obiter dictum*** to the impugned decision (cf. Facts and Submissions, item VIII. above), the sufficiency of disclosure provided by the present application was called into question. The board finds that an objection under Article 83 EPC is unfounded in the present case for the reasons which follow.

6.2 In this regard, it is appropriate to recall that the application discloses the general principle that recovery of the original data can be effected using any two sequentially adjacent "divided data" items or by using the n-th "divided data" item, i.e. D(n), in combination with any other "divided data" item from D(1) to D(n-1), (cf. p.49 l.28 - p.50 l.20; p.51 l.25-32; p.52 l.4-12; p.52 l.13-27). Recovery of the original data is explained in more detail for the cases n = 3 (cf. p.22 l.11 ***et seq.***) and n = 4 (cf. p.37 l.26 ***et seq.***).

6.3 The application additionally discloses that a certain minimum number of "divided data" items must be acquired in order to ensure the availability of two "divided data" items that can be used for recovery of the original data, i.e. (n+1)/2 where n is odd and (n/2)+1 where n is even, (cf. p.39 l.30 - p.40 l.9).

Thus, for n = 3 the acquisition of any two "divided data" items suffices to ensure the availability of two "divided data" items which can be used to effect recovery (p.49 l.28 - p.50 l.20) whereas for n = 4 and n = 5 it is necessary to acquire a minimum of three

"divided data" items in order to ensure that recovery is possible (cf. p.51 l.25-32; p.52 l.4-12).

6.4 The board takes the view that, subject to amendment as discussed in 4.9 above, claim 1 can be considered to express the disclosed constraints relating to the recovery of the original data, i.e. that it is necessary to acquire a certain minimum number of "divided data" items in order to ensure the availability of a pair of said items which permit recovery of the original data.

6.5 Concerning the objection that no example of recovery using three "divided data" items has been disclosed for n = 4, the board judges that such an example would lie outside the scope of the present invention in view of the fact that, according to the description, only two "divided data" items are used to carry out the actual recovery of the original data irrespective of the value of n (cf. 6.2 above). The aforementioned objection is thus judged to be irrelevant to the question of compliance with the requirements of Article 83 EPC.

6.6 Concerning the objection that the application does not disclose how to recover the data for cases where n >= 5, it is noted that although specific examples relating to the recovery of the original data are only provided for the cases where n = 3 and n = 4 (cf. 6.2 above), the application discloses that the case where n = 5 is basically the same as the case where n = 4 (cf. p.39 l.15-29; p.51 l.33 - p.52 l.12) and that the division and recovery of the original data can be performed "similarily" in cases where n is greater than 5 (cf. p.39 l.30 - p.40 l.9; p.52 l.13-27).

Having regard to the disclosure of the application concerning the general form of the definition formula and rules for generating the divided data (cf. 3.5 above), the board takes the view that it is not necessary in the given context to provide worked examples for further values of n in order to comply with the requirements of Article 83 EPC. In the board's judgement, the skilled person would not require the exercise of inventive skill to adapt the aforementioned specific examples to cases where n is equal to or greater than 5.

6.7 In view of the foregoing, the board concludes that the application discloses the claimed invention in a manner sufficiently clear and complete for it to be put into practice as required by Article 83 EPC.

7. *Remittal*

7.1 The impugned decision does not address the question of compliance with the further requirements of the EPC, in particular those of Article 52(1) EPC. The board judges that, under the given circumstances, it would not be appropriate to decide this question in the context of the present appeal proceedings. Accordingly, the case is remitted to the department of first instance for further prosecution (Article 111(1) EPC).

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the department of first instance for further prosecution on the basis of the following documents:

   Claims 1-6 as filed during the oral proceedings before the board.

   Description, pages:
   2, 6-11, 13-18, 20-44, 46-55 as published;
   1, 3, 5 as filed with the letter dated 21 April 2006;
   4, 12 as filed with the letter dated 27 July 2006;
   19, 45 as filed during the oral proceedings before the board.

   Drawings, sheets 1/13 - 13/13 as published.

The Registrar: The Chair:

K. Götz A. Ritzka