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

Datasheet for the decision of 17 October 2012

Case Number: T 1350/08 - 3.5.05

Application Number: 04727431.1

Publication Number: 1616405

IPC: H04L9/30

Language of the proceedings: EN

Title of invention:
Apparatus to generate parameter for NTRU, NTRU decryption and encryption system, apparatus, method and program implementing said parameter generating unit

Applicant:
Panasonic Corporation

Headword:
NTRU cryptosystem/PANASONIC

Relevant legal provisions:
EPC Art. 83, 84, 111(1)
EPC R. 43(2)

Keyword:
Sufficiency of disclosure - (yes, after amendment)
Claims - clarity and conciseness (yes, after amendment)
Remittal to the first instance for further prosecution

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T1350/08 - 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 17 October 2012

Appellant: (Applicant)	Panasonic Corporation 1006, Oaza Kadoma Kadoma-shi Osaka 571-8501 (JP)
Representative:	Pautex Schneider, Nicole Véronique Novagraaf International SA Chemin de l'Echo 3 1213 Onex (CH)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted 3 March 2008 refusing European patent application No. 04727431.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair: A. Ritzka
Members: K. Bengi-Akyuerek
F. Blumer

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, posted on 3 March 2008, refusing European patent application No. 04727431.1 on the grounds of insufficiency of disclosure (Article 83 EPC), lack of clarity (Article 84 EPC), and lack of conciseness (Article 84 and Rule 43(2) EPC) with regard to a main request and two auxiliary requests.

The following documents were referred to in the decision under appeal:

D1: J.H. Silverman: "NTRU Cryptosystems Technical Report: Wraps, Gaps, and Lattice Constants", pages 1-6, 15 March 2001;

D2: J.H. Silverman, W. Whyte: "NTRU Cryptosystems Technical Report, Report #18, Version 1: Estimating Decryption Failure Probabilities for NTRUEncrypt", pages 1-17, June 2003;

D3: N. Howgrave-Graham et al.: "The Impact of Decryption Failures on the Security of NTRU Encryption", pages 1-22, August 2004;

D4: J.H. Silverman: "NTRU Cryptosystems Technical Report: Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem", pages 1-14, 9 March 1999.

II. Notice of appeal was received on 22 April 2008. The appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 1 July 2008. The appellant requested that the decision of the examining division be set aside and that a patent be granted on the basis of a new set of claims (claims 1 to 19) according to a sole request submitted with the statement setting out the grounds of appeal.

In addition, oral proceedings were requested as a precautionary measure.

III. A summons to oral proceedings scheduled for 6 December 2012 was issued on 9 July 2012. In an annex to this summons, pursuant to Article 15(1) RPBA, the board gave its preliminary opinion on the appeal. In particular, objections were raised under Article 84 EPC and the appellant was informed that the case could be remitted to the department of first instance if these objections were overcome.

IV. With a letter of reply dated 21 September 2012, the appellant filed amended claims according to a sole request (claims 1 to 19) and requested that the scheduled oral proceedings be cancelled.

V. With a communication dated 17 October 2012, the appellant was notified that the scheduled oral proceedings were cancelled.

VI. Claim 1 of the sole request reads as follows:

"A parameter generation apparatus for generating an output parameter that is a set of parameters causing no decryption error for an NTRU cryptosystem, the parameter generation apparatus comprising:

an error-free output parameter generation unit operable to generate the output parameter (p, q, d, and df) that meets a conditional expression, in the output parameter p being a non-negative integer, q being a non-negative integer, d being a non-negative integer that is for specifying the number of coefficients of value 1 in a random number polynomial r, and df being a non-negative integer that is for specifying the number of coefficients of value 1 in a private key polynomial

f, the conditional expression being derived from predetermined error condition information indicating a condition for causing no decryption error, and the conditional expression be [sic] being represented as

2·p·d+2df-1<q/2,

all coefficients in a polynomial (p·r×g+f×m) being in a range from —q/2 to q/2 when the output parameter meets the conditional expression, the polynomial (p·r×g+f×m) being derived by computing the random number polynomial r, a random polynomial g, the private key polynomial f and a plaintext polynomial m, the random polynomial g being used for generating a public key polynomial h in the NTRU cryptosystem,

wherein the error-free output parameter generation unit includes:

a provisional parameter generation unit operable to generate a set of provisional parameters that meets the conditional expression prior to the generation of the output parameter; and

an output parameter generation unit operable to generate the output parameter, using the set of provisional parameters, based on a lattice constant that is calculated from the set of provisional parameters, security determination information and security level information SLI, the security determination information indicating a decryption time estimation equation EF to calculate decryption time T required for a third party to decrypt an NTRU encrypted text using an LLL algorithm, and the security level information SLI indicating a desired security level required against decryption of the NTRU encrypted text using the LLL algorithm by the third party."

The further independent claims 14 and 17 are directed towards a corresponding method, while claims 16 and 19 are directed to a corresponding computer program.

Reasons for the Decision

1. Admissibility of the appeal

The appeal complies with the provisions of Articles 106 to 108 EPC (cf. point II above) and is therefore admissible.

2. Sole request

This request was filed in response to the objections raised in the board's communication under Article 15(1) RPBA and is therefore admitted into the proceedings under Article 13(1) RPBA.

The claim set of this request differs from the claim set of the second auxiliary request underlying the appealed decision *inter alia* in that independent claims 1, 14, and 17 as amended further specify that

(a) the output parameters p and q are non-negative integers, d is a non-negative integer that is for specifying the number of coefficients of value 1 in a random number polynomial r, and df is a non-negative integer that is for specifying the number of coefficients of value 1 in a private key polynomial f;

(b) all coefficients in a polynomial (p·r×g+f×m) are in a range from -q/2 to q/2 when the output parameter meets the conditional expression, the polynomial (p·r×g+f×m) is derived by computing the random number polynomial r, a random polynomial g is used for generating a public key polynomial h in the NTRU cryptosystem, the private key polynomial f and a plaintext polynomial m;

(c) the security determination information indicates a decryption time estimation equation EF to calculate

decryption time T required for a third party to decrypt an NTRU encrypted text using an LLL algorithm;

(d) the security level information SLI indicates a desired security level required against decryption of the NTRU encrypted text using the LLL algorithm by the third party.

Feature (a) is based on the disclosures of page 3, lines 7-10; page 14, lines 14-16; page 14, lines 24-25, and page 15, lines 2-3 of the application as filed.

Feature (b) has its basis on page 15, lines 13-19 of the original application.

Feature (c) is supported by the disclosure of page 16, lines 27-31, while feature (d) is based on page 16, lines 3-10 of the application as filed.

Hence, the above amendments comply with Article 123(2) EPC.

2.1 Article 83 EPC

The board judges that the application meets the requirements of Article 83 EPC, for the following reasons:

2.1.1 The examining division held that the then pending independent claims did not comprise a formula which defined the encryption parameters for the encryption process used in the considered NTRU cryptosystem that yielded the desired effect of performing NTRU decryption without failures. Therefore, the skilled person could not carry out the invention in the whole range claimed, thus contravening Article 83 EPC. In

particular, the two specific conditions taught on page 7, line 15 and page 15, line 16 of the original description under which the respective polynomial coefficients should be selected in order to achieve the desired effect were missing in some of the independent claims (cf. appealed decision, section 2.1).

2.1.2 The appellant has amended the claims such that all the objected independent claims now comprise the conditions under which the respective polynomial coefficients are selected, i.e. that the conditional expression is represented as $2 \cdot p \cdot d + 2df - 1 < q/2$ and that all the coefficients in a polynomial $(p \cdot r \times g + f \times m)$ are in a range from $-q/2$ to $q/2$ when the output parameter meets the conditional expression.

2.1.3 The board is therefore satisfied that the objections raised under Article 83 EPC are overcome and that the present invention is therefore sufficiently disclosed.

2.2 Article 84 EPC: Clarity

Owing to the amendments made in response to the clarity objections raised by the examining division (cf. appealed decision, section 2.2) and by the board (cf. section 4.2 of the board's communication under Article 15(1) RPBA), the board is satisfied that those objections no longer apply.

For these reasons, the board concludes that the present claims are clear within the meaning of Article 84 EPC.

2.3 Article 84 EPC: Conciseness

In the board's judgment, the present claim set is concise in compliance with Article 84 and Rule 43(2)

EPC, the reasons being as follows:

2.3.1 The examining division found that the former claim set of the application was not concise under Article 84 EPC in conjunction with Rule 43(2) EPC, *inter alia* since it contained more than one claim directed to encryption and decryption systems (cf. appealed decision, section 2.3, item viii).

2.3.2 The appellant has amended the set of claims such that it now comprises five independent claims in different categories, namely, one independent apparatus claim (i.e. claim 1), two independent process claims (i.e. claims 14 and 17), and two independent product claims (i.e. claims 16 and 19).

Since the above process and product claims are directed to complementary encryption and decryption functions, they are allowable under Rule 43(2)(a) EPC.

In this context, claims 11 to 13 (directed to an "encryption system", an "encryption apparatus", and a "decryption system", respectively) are dependent claims according to Rule 43(4) EPC, since they contain a reference to claim 1 and thus include all the apparatus features of a "parameter generation apparatus" as defined in claim 1 while specifying additional features related to additional units.

2.3.3 Therefore, the board holds that the present claim set is concise within the meaning of Article 84 EPC and admissibly contains more than one independent claim in the same category under Rule 43(2) EPC.

2.4 Article 52(1) EPC: Novelty and inventive step

The board is not in a position to pass final judgment on the questions of novelty and inventive step, for the following reasons:

2.4.1 The examining division did not decide on the matters of novelty and inventive step in the first-instance proceedings.

Rather, in an *obiter dictum* under the heading "Remarks with respect to inventive step: Article 56 EPC" of the decision under appeal, only a very general statement was provided as to the matter of inventive step, referring to the reasoning set out in the communication accompanying the summons to oral proceedings. According to that reasoning, the subject-matter of the claims of the main and auxiliary requests did not involve an inventive step under Article 56 EPC in view of documents D1 to D3.

2.4.2 However, it is conspicuous to the board that the cited documents D2 and D3 are non-patent documents being published after the application's priority date and therefore cannot be considered as state of the art under Article 54(2) and (3) EPC. Furthermore, no substantive assessment of inventive step for the claimed subject-matter, e.g. using the established "problem-and-solution approach", was carried out during the first-instance proceedings.

3. Remittal to the department of first instance

In view of the substantial amendments made to the claims, the grounds for refusal under Articles 83 and 84 EPC given in the appealed decision no longer apply in the present case. Consequently, since the grounds for the decision to refuse the present application have

been overcome (which, by the way, should normally have led the examining division to rectify its decision under Article 109(1) EPC), and since the appellant requested the cancellation of the scheduled oral proceedings, the board is in a position to decide the present appeal without holding oral proceedings.

As, however, a complete assessment of novelty and inventive step for the claimed subject-matter was not carried out during the first-instance proceedings (cf. point 2.4 above), the board concludes that under the present circumstances it is not appropriate to take a definitive decision on the matters of novelty and inventive step.

For these reasons, the board decides to exercise its discretion to remit the case to the department of first instance for further prosecution under Article 111(1) EPC, on the basis of claims 1 to 19 submitted with the letter dated 21 September 2012.

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 claims 1 to 19 submitted with the letter dated 21 September 2012.

The Registrar: The Chair:

L. Fernández Gómez A. Ritzka

Decision electronically authenticated