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 6 December 2011

Case Number: T 1552/08 - 3.5.05

Application Number: 98954922.5

Publication Number: 0935859

IPC: H04L 9/06

Language of the proceedings: EN

Title of invention:
Methods and apparatus for enhanced security expansion of a secret key into a lookup table for improved security for wireless telephone messages

Applicant:
LUCENT TECHNOLOGIES INC.

Headword:
Enhanced cryptoprocessing of messages/LUCENT

Relevant legal provisions:
EPC Art. 54(2), 54(3)
RPBA Art. 15(3)

Relevant legal provisions (EPC 1973):
EPC Art. 54(4), 84

Keyword:
"Clarity and support by the description - main and auxiliary request (no)"
"Novelty - main request (no)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1552/08 **-** 3.5.05

D E C I S I O N
of the Technical Board of Appeal 3.5.05
of 6 December 2011

Appellant: LUCENT TECHNOLOGIES INC.
600 Mountain Avenue
Murray Hill NJ 07974-0636 (US)

Representative: Sarup, David Alexander
Alcatel-Lucent Telecom Limited
Unit 18, Core 3, Workzone
Innova Business Park
Electric Avenue
Enfield EN3 7XU (GB)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 1 April 2008 refusing European patent application No. 98954922.5 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman: A. Ritzka
Members: M. Höhn
G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division, dispatched on 1 April 2008, refusing European patent application No. 98954922.5 because of lack of clarity (Article 84 EPC 1973) and novelty (Articles 52(1) EPC and 54(2) EPC 1973) having regard to the disclosure of

D1: US 5594797 A1.

II. The notice of appeal was submitted on 16 May 2008. The appeal fee was paid on the same day. The statement setting out the grounds of appeal was submitted on 1 August 2008. The appellant requested that the appealed decision be set aside and that a patent be granted on the basis of the sets of claims according to the main request or the auxiliary request submitted with the statement setting out the grounds of appeal.

III. A summons to oral proceedings to be held on 6 December 2011 was issued on 19 September 2011. In an annex accompanying the summons the board expressed its preliminary opinion that the subject-matter of the independent claims of both requests did not fulfil the requirements of Article 84 EPC 1973. The subject-matter of the independent claims of the main request furthermore did not appear to be novel having regard to the disclosure of D1 or either of

D2: WO 9840984 A1 and
D3: US 5159634.

Prior art publication D3 was introduced into the proceedings by the board of its own motion according to Article 114(1) EPC 1973, since it was referred to in the introductory portion of D1 and was therefore relevant for the interpretation of D1. The board gave its reasons for the objections and that the appellant's arguments were not convincing.

IV. With a letter dated 26 October 2011 the appellant informed the board that the appellant would not be attending the oral proceedings set for 6 December 2011.

V. Independent claim 1 according to the main request reads as follows:

"1. A method of enhanced cryptoprocessing of messages in a call, for use in a CMEA encryption system employed in a wireless telephone system, comprising the steps of:
generating each of a first offset and a second offset;
permuting inputs to a tbox function using the first offset and the second offset to produce a first permutation result; and
performing the tbox function on the first permutation result."

Independent claim 13 according to the main request reads as follows:

"13. A wireless telephone set for securely transmitting messages, comprising:
a transceiver (502);
an input/output interface (504);
a key generator (508) for generating one or more keys to be used during a call; and

an encryption/decryption processor (506) for receiving from the input/output interface a message to be encrypted or decrypted together with identification of the message as appropriate using a CMEA process including a tbox function permuted by one or more secret offsets, the encryption/decryption processor being further operative to return the encrypted or decrypted message to the input/output interface for further routing."

Independent claim 12 according to the auxiliary request reads as follows:

"12. A wireless telephone set for securely transmitting messages, comprising:
a transceiver (502);
an input/output interface (504);
a key generator (508) for generating one or more keys to be used during a call; and
an encryption/decryption processor (506) for receiving from the input/output interface a message to be encrypted or decrypted together with identification of the message as appropriate using a CMEA process including a tbox function permuted by one or more secret offsets, the encryption/decryption processor being further operative to return the encrypted or decrypted message to the input/output interface for further routing, wherein a first secret offset for an nth message of a call is expressed by the equation $offset1_n = ((2K_1 + 1) * CT_{n-1} + K_2) \bmod 64K)>>8$, where K_i i odd, are 15-bit secret values and K_i, i even, are 16-bit secret values, all constant for the call, and CT_{n-1} is the first two octets of the (n-1)th ciphertext message, and wherein a second secret offset for an nth

message of a call is expressed by the equation $offset2_n = (((2K_3 + 1) * CT_{n-1} + K_4) \bmod 64K)>>8$, where K_i, i odd, are 15-bit secret values and K_i, i even are 16-bit secret values, all constant for the call, and CT_{n-1} is the first two octets of the (n-l)th ciphertext message, and wherein mod 64K is mod 65,536."

VI. The appellant requested in writing that the appealed decision be set aside and that a patent be granted on the basis of the sets of claims according to the main request or the auxiliary request submitted with the statement setting out the grounds of appeal.

VII. Oral proceedings were held on 6 December 2011 in the absence of the appellant. After due deliberation on the basis of the written submissions in the statement setting out the grounds of appeal and of the requests, the board announced its decision.

Reasons for the Decision

1. Admissibility

The appeal complies with the provisions of Articles 106 to 108 EPC (see Facts and Submissions, point II above). Therefore the appeal is admissible.

2. Non-attendance at oral proceedings

In its letter of 26 October 2011 the appellant announced that it would not be attending the oral proceedings. The board considered it expedient to

maintain the date set for oral proceedings. Nobody attended the hearing on behalf of the appellant.

Article 15(3) RPBA stipulates that the board shall not be obliged to delay any step in the proceedings, including its decision, by reason only of the absence at the oral proceedings of any party duly summoned who may then be treated as relying only on its written case.

Thus, the board was in a position to take a decision at the end of the oral proceedings.

3. In the first instance proceedings, the application was refused based on lack of clarity of the term "permutation" used in independent claims 1 and 13 and based on lack of novelty of these claims with regard to the disclosure of D1.

MAIN REQUEST:

Clarity and support by the description - Article 84 EPC 1973

4. The applicant provided a written statement of a professor of Cambridge university and a reference to a standard textbook in order to overcome the objection under Article 84 EPC 1973. The examining division, however, was not convinced by this material.

4.1 Prof. Anderson's letter (dated 20 June 2007, received on 27 June 2007) was submitted in order to prove that the use of the terms "permutation" and "permute", even if not used according to its mathematical definition,

were common in the art of cryptography before the priority date of the present application.
Prof. Anderson argued that "A permutation has the added property that it is a bijection, that is each input value is mapped to a unique output value" (see points 3 and 5 of the letter) and wrote about "the use of the word 'permutation' as a synonym for 'bijection'" which would have been commonly used in the field of cryptography for a quarter of a century at least (see point 4 of the letter). It was referred to the text book "cipher's systems" of H. Beker and F. Piper, pages 254-255, which were attached.

The board accepts this interpretation that a "permutation" is to be interpreted as synonym for a bijection which is in accordance with e.g. D2 disclosing that a permutation means that "each input has one-to-one mapping to the output (see page 9, lines 20 to 22).

4.2 But even if this statement is accepted, that a "permutation" is to be interpreted as synonym for a bijection, claim 13 is not considered to be clearly understandable if being understood as a bijection. In particular the expression "a tbox function permuted by one or more secret offsets" implies that the function is permuted rather than the input values as disclosed at page 6, line 29 to page 7, line 1 of the description. Claim 13 therefore lacks clarity in contrast to the requirements of Article 84 EPC 1973.

4.3 In addition, claim 13 merely requires one offset value ("one or more secret offsets"). However, the board is not convinced that the alternative using a single

offset is supported by the description pursuant to Article 84 EPC 1973, since it is disclosed all over the description to use "offsets" (plural). The explicit embodiments use either two or four secret offset values. During the appeal proceedings, the appellant did not present any convincing counterargument and, hence, did not overcome this objection.

Novelty - Article 54(2) EPC

5. For assessing novelty the terms "permutation" and "offset" can be interpreted in their broadest manner. According to the standard textbook "Applied cryptography" by B. Schneier, which was submitted during the first instance proceedings, a permutation can be considered to be a transposition (see page 237, paragraph 4) which interpretation appears to be broader than a bijection requiring that each input value is mapped to a unique output value.
The term "offset" is also a broad term, which therefore can be interpreted in a broad manner, since claims 1 and 13 do not specify by wording or by a formula how exactly the inputs to the tbox function are permuted. The board further agrees with the examining division's argument that an "offset" is merely a random number.

5.1 In point 2.1 of the reasons of the decision under appeal the examining division argued that D1 disclosed the following features:
A method of enhanced tbox processing for each message in a call for use in a CMEA encryption system employed in a wireless telephone system, comprising the steps of: (see figure 1),

generating a first and a second offset; (see figure 5(A) see variables Z and I, initialization step A2 and A4 and A5),
permuting inputs to a tbox function using the first and second offset to produce a permutation result; and (see figure 5(A) Z xor I performing a tbox function on the permutation result (see figure 5(A)A3 "tbox(Z xor I)").

5.2 The board agrees with this reasoning except for the following considerations. The appellant is correct that according to figure 5A of D1, elements A2-A4, either Z or I has to be considered to be the input value to the tbox function. Therefore only the other (second) value, if regarded as offset, is used for permuting the input to the tbox function.

However, according to D1 the "tbox() is a function which returns a value derived from the function input parameter and the values of KEY[] and CTABLE[] provided as inputs to the transformation" (see column 9, lines 15-17). This implies that values KEY[] and CTABLE[] are used as input parameter for the tbox function. The array KEY[] holds an eight byte key value derived from a BASE_KEY which is a secret number (see D1, column 6, lines 53-65) and, hence, is regarded as a plurality of secret offset values. CTABLE[] is an array of cryptographic key values (see D1, column 6, lines 44-47) and therefore is considered to be a look-up table. Figure 6 of D1 shows how a value of the tbox function is achieved (see also D1, column 10, line 25 onwards).

According to the two formulas T3 and T4

H=H XOR KEY[J] (T3) and
H={H+KEY[J+1]}mod 256 (T4)

the input value Y=H to the tbox function is modified at least two times, i.e. with secret number KEY[J] regarded as a first offset value, and with secret number KEY[J+1] regarded as a second offset value. The modifications transform the input value Y and, according to the broad interpretation of the term "permutation" to be a transposition (see above), permute the input to the tbox function using a first and second offset value according to the second feature of claim 1.

The subject-matter of claim 1 therefore lacks novelty with regard to the disclosure of D1.

6. The above mentioned objection under Article 84 EPC 1973 notwithstanding (see point 4.3 above), claim 13 merely requires one offset value ("one or more secret offsets"). D1 does not explicitly disclose a CMEA process, but in the introductory part it refers to D3, which discloses the CMEA algorithm (see present patent application, page 3, lines 1 to 3). D1 aims to improve the CMEA process including a tbox function. Therefore the tbox function referred to in D1 can be considered to implicitly disclose that a CMEA process is used in connection with the tbox function. Since D1 also discloses the apparatus features of claim 13 in figure 1 and 2 and the corresponding part of the description (i.e. transmitter/receiver, input/output interface, key generator, encryption/ decryption

processor) and that the tbox function used is permuted at least by one secret offset KEY[], the subject-matter of claim 13 also lacks novelty with regard to the disclosure of D1.

7. D2, which is prior art under Article 54(3) EPC and Article 54(4) EPC 1973, explicitly discloses permutation in the form of a bijection (see page 9, lines 20 to 22). Figure 2A, elements 104 and 204, discloses the use of an input value v which is permuted using a value t1box and an 'exor' operation with a value i. The input value is therefore permuted using two separate values. In the board's judgement these values 't1box' and 'i' can be regarded as offset values, because they are random numbers.

The subject-matter of claim 1 therefore also lacks novelty over D2.

8. The above mentioned objection under Article 84 EPC 1973 notwithstanding (see point 4.3 above), claim 13 merely requires one offset value ("one or more secret offsets"). D2 discloses the further features of claim 13, i.e. transmitting and receiving with CMEA functionality (see figure 1, elements 30 and 60), input/output interface (see figure 1, data input and output) and key generators (see figure 1, elements 16 and 86) used for encryption/decryption with a corresponding processor (see figure 1, elements 30 and 70).

According to the present application, a tbox function can either be implemented as a function call or as a look-up table (see description page 3, lines 8-9). Also

D2 discloses the use of a tbox function in the form of look-up tables (see D2, page 10, line 16 onwards). Also the use of a single tbox function is disclosed (see D2, page 11, line 14). According to D2 it is assumed that the input value passed to tbox is a permutation and a tbox function is guaranteed to be a permutation (see D2, page 9, lines 20-27). In a particular embodiment (see D2, page 10, lines 20-24), D2 discloses to initialize tables with a permutation of the 256 possible inputs and to perform key-dependent shuffling, i.e. an offset by a secret random number, and a table index operation. The board considers this embodiment to imply "a CMEA process including a tbox function permuted by one or more secret offsets" according to the last feature of claim 13.

The subject-matter of claim 13 is therefore also anticipated by the disclosure of D2 and lacks novelty.

AUXILIARY REQUEST:

9. Independent claim 12 of this request refers to "a tbox function permuted by one or more secret offsets", which has been objected to under Article 84 EPC 1973 with respect to claim 13 of the main request for the reasons outlined in points 4.2 and 4.3 above. This reasoning equally applies to claim 12 of the auxiliary request.

Claim 12 therefore does not fulfil the requirements of clarity and support by the description according to Article 84 EPC 1973.

10. Thus, none of the requests are allowable.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

K. Götz A. Ritzka