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

DECISION
of 24 October 2001

Case Number: T 0559/98 - 3.5.2

Application Number: 89301776.4

Publication Number: 0331352

IPC: G07B 17/02

Language of the proceedings: EN

Title of invention:
Franking system

Patentee:
Neopost Limited

Opponent:
Pitney Bowes, Inc.

Headword:
-

Relevant legal provisions:
EPC Art. 56, 123(2)

Keyword:
"Added subject-matter - (no)"
"Inventive step - (yes)"

Decisions cited:
-

Catchword:
-

Case Number: T 0559/98 - 3.5.2

DECISION
of the Technical Board of Appeal 3.5.2
of 24 October 2001

Appellant: (Opponent)	Pitney Bowes, Inc. World Headquarters, One Elmcroft Rd. Stamford/ Connecticut 06926 0700 (US)
Representative:	Avery, Stephen John Hoffmann Eitle Patent- und Rechtsanwälte Arabellastrasse 4 D-81925 München (DE)
Respondent: (Proprietor of the patent)	Neopost Limited South Street Romford Essex RM1 2AR (GB)
Representative:	Boden, Keith McMurray Fry Heath & Spence The Old College 53 High Street Horley Surrey RH6 7BN (GB)

Decision under appeal: **Interlocutory decision of the Opposition Division of the European Patent Office posted 6 April 1998 concerning maintenance of European patent No. 0 331 352 in amended form.**

Composition of the Board:

Chairman:	R. G. O'Connell
Members:	J. Cannard
	P. H. Muehlens

Summary of Facts and Submissions

I. This is an appeal by the opponent as sole appellant from the interlocutory decision of the opposition division proposing to maintain European patent No. 331 352 in amended form.

II. The amended patent as approved by the opposition division includes independent method and apparatus claims 1 and 13 which are worded as follows:

"1. A method of franking mail items in a franking machine in which encrypted data is printed in machine readable form on the mail items comprising the steps of generating a pseudo-random number relating to a franking transaction; forming a data block containing at least said pseudo-random number and data relating to a postal charge for said mail item; encrypting said data block; printing in machine readable form on the mail item (10) data (12) representing said encrypted data block together with identification data identifying a location at which the mail items are franked and with identification data identifying said franking machine, and carrying out, at a postal authority location, the steps of machine reading the printed data representing the identification data and the encrypted data block (12); selecting from a record of decryption keys a decryption key corresponding to said identification data identifying said franking machine; utilising said selected decryption key to decrypt said encrypted data block read from the mail item (10) and checking validity of the pseudo-random number contained in said data block."

"13. Franking apparatus including a franking machine having printing means (16) to print encrypted data in machine readable form on mail items having means (18) to generate a pseudo-random number for each franking transaction; means (18) to form a data block by combining said pseudo-random number with a postal value selected for franking the mail item; means for encrypting said data block; and in which the printing means (16) is operated to print in machine readable form on the mail item franking data representing said data block together with identification data identifying a location at which the mail item is franked and identification data identifying said franking machine, and having at a postal authority location, reading means to read the printed franking data representing said data block and the identification data; means to select from a record of decryption keys a decryption key corresponding to the identification data identifying said franking machine; means operable to utilise said selected decryption key to decrypt said data block read from the mail item and means to check the validity of the pseudo-random number."

Claims 2 to 12 and 14 to 16 are dependent on claims 1 and 13 respectively.

III. The following prior art documents from the proceedings before the opposition division remain relevant to the present appeal:

D1: EP-A-0 132 782

D2: GB-A-2 173 738

D4: GB-A-2 174 039

D5: US-A-4 629 871

D6': GB-A-2 190 044

IV. In a communication accompanying a summons to oral proceedings the board pointed out *inter alia* that the appellant's argument on inventive step as set out in the statement of grounds of appeal appeared to combine four documents, viz D1, D2, D4 and D5.

V. At oral proceedings before the board on 24 October 2001 the appellant, in addition to developing the attack on inventive step foreshadowed in the statement of grounds of appeal, objected - for the first time in the appeal procedure - that claims 1 and 13 as approved by the opposition division in the decision under appeal included wording which represented subject-matter which extended beyond the content of the application as filed and accordingly contravened Article 123(2) EPC.

VI. The appellant opponent's arguments can be summarised as follows:

1. *Added subject-matter (Article 123(2) EPC)*

The wording "identification data identifying a location at which the mail items are franked and with identification data identifying said franking machine" in claim 1 had no basis in the application as filed. The latter specifically taught that the decryption key was selected in accordance with the license number of the franking machine. Hence the wording of the claim represented an impermissible generalisation of the original disclosure.

2. *Inventive step*

It was difficult to identify the objective technical problem in the present case. The subjective problem mentioned at column 1, lines 42 to 48 of the opposed patent of making a franking machine secure was too general to be of any help. Neither was it clear how the invention as claimed achieved the aims referred to in the introductory part of the description, particularly since the terms of the claim did not correspond closely to the embodiment described and illustrated, eg in Figure 2.

Document D1, the closest prior art, disclosed a method of franking a mail item in which data was printed on the item in machine readable form in a manner allowing the postal authority to verify whether or not the franking imprint was authentic. To this end the data was printed on the item both in clear (plaintext) and in encrypted form. At the receiving station the postal authority read the plaintext, (re)encrypted the read data using the same encryption scheme as was used by a licensed franking machine and compared the two encrypted versions to check the authenticity of the franking imprint. The data printed on the item could include the postal fee, the destination zip code, the date, the package count, the serial number of the sending station, ie data identifying the franking machine, and origin zip code as well as a verification in encrypted form (D1, page 17, lines 12 to 24). In D1, the most relevant disclosure was that relating to the bar code embodiment described at page 39, line 5 to page 40, line 14 with reference to Figures 1, 3c, 4c and 5. As shown in Figure 1 a data seed word was used in sending (24) and receiving (28) stations. A base seed word was altered by the date, fee and serial number of the sending station (page 17, lines 12 to 20) and the encryption was accomplished by coding circuitry 130 (Figure 5, page 30). In this embodiment the date formed the address for the ROM 138 where the base seed word was stored but the selection of the seed word was not restricted to the date (page 30, line 16 ff). As mentioned explicitly at page 31, lines 19 to 24 of D1 other forms of encryption were envisaged, the scrambling performed by the feedback shift register 130 being one illustrative example. At the receiving station a duplicate of coder 88, (Figure 4c) (re)encrypted the plaintext using the same base seed number as that used in the originating franking machine; in this respect the base seed number was the analogue of an encryption/decryption key.

A comparison of the franking method specified in claim 1 of the opposed patent with that disclosed in D1 showed that both involved franking machines with an encryption operation and used a pseudorandom number (output of ROM 138 in D1 was a pseudorandom number). Thus the data block in D1 contained a pseudorandom number and the scrambling of the data block in feedback shift register 130 was an encryption operation. In D1 data for identifying the franking machine were present in the bar code print; this was used to generate a seed number which corresponded to a decryption key. Hence the only difference between claim 1 and D1 was that in D1 the encryption operation was repeated whereas in claim 1 a decryption operation was performed. The opposition division found in the decision under appeal that encryption/ decryption/plaintext comparison as in claim 1 and encryption/encryption/codetext comparison as in D1 were obvious alternatives, but went on to find the subject-matter of claim 1 inventive because D1 allegedly did not disclose the selection of a particular encryption-decryption key in dependence on the franking machine identity. In this respect however the opposition division erred because it failed to take into account the fact that in D1 the verification process carried out by the postal authority also relied on identifying the individual franking machine in order to determine which seed word to employ for the (repeated) encryption process to enable the necessary comparison to be carried out.

It should be noted that neither claim 1 nor claim 13 mentioned an encryption key.

It was true that the output of ROM 138 in D1 was predictable once the addressing input was known, but this applied equally to any pseudorandom number generator - once the generation rule was known the pseudorandom number output was predictable. In D1 the ROM 138 generated a pseudorandom number at the level of security required, viz that appropriate for the typical value of a mail item; it was not plausible to argue that the seed word ROM 138 could not be regarded as a pseudorandom generator.

Document D4, page 3, lines 68 to 74 taught that key-based decryption was an option so long as the key was derivable from information printed on the envelope.

The use of the word "combining" in claim 13, in contrast to "containing" in claim 1 implied that the pseudorandom number and the data were linked together to form the data block.

The load value (in D1, Figure 5) may be a meaningless number - but one could repeat the steps of addition modulo 2 in the output of ROM 138, form another word (load) and compare it. In principle the code output from register 130 could be decrypted.

Hence D1 disclosed (i) use of a pseudorandom number, (ii) a block containing a pseudorandom number + data, (iii) encryption, (iv) selecting a key corresponding to the franking machine identity, and (v) comparing data. The only difference, therefore, was encryption instead of decryption at the receiving station - an obvious alternative, either from common general knowledge in the art or from D4.

VII. The respondent proprietor argued essentially as follows:

1. *Article 123(2) EPC*

This issue had not been mentioned in the statement of grounds of appeal nor in subsequent written submissions. As could be seen from the minutes of the oral proceedings before the opposition division the present version of claim 1 arose from a suggestion from the opponent that the former claim 9 should be combined with the former claim 1. The appellant was merely repeating an objection which had already been answered by the opposition division.

2 *Inventive step*

The subject-matter of claim 1 involved several clear distinctions over D1:

(i) In D1 there was no decryption at the receiving station.

(ii) D1 did not disclose generation of a pseudorandom number in the sense in which this term was used in the opposed patent and in the relevant art, viz a sequence of unpredictable numbers produced by an algorithm. The base seed word used in D1 did not meet this definition since it was formed by a small set of numbers stored in a ROM which was addressed non-randomly.

(iii) In the franking method specified in claim 1 the pseudorandom number was not transmitted in plaintext. As pointed out in D4 (page 3, lines 68 to 72) there were in general two possibilities, encryption/decryption or use of seed numbers where encryption is performed twice. D1 used the latter, claim 1 specified the former. The franking method of claim 1 provided two layers of security, encryption with a key and the pseudorandom number.

(iv) D1 did not form a data block containing a pseudorandom number. The load word for the coding circuit 130 in D1 was derived from a seed word and data. A pseudorandom number could not be derived from the encrypted data printed on the franking item; the load word was a meaningless value which did not enable a validity check to be carried out.

(v) Claim 1 specified a selection from a list of decryption keys of a decryption key uniquely corresponding to a particular machine; in D1 there was no key-based decryption.

The fact that D4 (page 3, lines 68 to 72) contrasts key-based encryption/decryption and encryption/(re)encryption should not be interpreted to mean that the encryption/decryption/plaintext-comparison of claim 1 was simply an obvious alternative to the encryption/encryption/codetext-comparison of D1. D4 did not teach the two levels of security provided by the franking method specified in claim 1.

Starting from D1 several steps were required to arrive at the claimed invention, thus:

- eliminate the seed word and introduce the pseudorandom number

- eliminate the modulo-2 addition (141 to 143) and use the combination of a pseudorandom number and data

- eliminate the shift register 130 and use a key-based encryption.

The invention underlying the opposed patent depended on the possibility of decryption of the load value in D1. Starting from D1 it was impossible to extract information from the load. To reverse the system in D1 one had to provide a data block containing a pseudorandom number and to perform a decryption; this was not suggested in D1.

The appellant opponent’s objection that an encryption key was not mentioned in claim 1 was not cogent; the decryption key mentioned therein implicitly defined an encryption key.

The respondent proprietor was prepared, if necessary, to amend claim 13 by replacing "combining" by "containing".

VIII. The appellant opponent requested that the decision under appeal be set aside and that the patent be revoked.

IX. The respondent proprietor requested that the appeal be dismissed and that the patent be maintained in the amended form approved by the opposition division.

Reasons for the Decision

1. The appeal is admissible.

2. *Added subject-matter (Article 123(2) EPC*

This issue was addressed in the decision under appeal at points 3 and 18. It was not touched on in the written appeal procedure but at oral proceedings the appellant registered his continuing disagreement with the finding of the opposition division without adducing any new argument by way of refutation. For its part the board has nothing to add to the reasoning and finding of the opposition division on this point in the decision under appeal which it approves and adopts.

3. *Inventive step*

3.1 Closest prior art

It is common ground and accords also with the judgement of the board that document D1 is the closest prior art. It is also common ground that the method of franking mail specified in claim 1 and that disclosed in D1 have at least the following features in common:

(i) the franking machine prints both plaintext transaction data on the mail item and a further, encrypted, text which is uniquely determined by the plaintext by a procedure which is intended to be kept secret from persons not authorised by the postal authority.

(ii) the authenticity of the franking impression on the mail item is checked by determining that the plaintext and the further, encrypted, text correspond in accordance with the secret algorithm.

It is further common ground that the claim 1 method and D1 differ in at least the following respect:

In D1 the plaintext is read from the mail item at the postal authority location and is transformed into an encrypted text using a procedure which duplicates that employed in the franking machine; this regenerated encrypted text is then compared with the encrypted text read from the mail item to check authenticity of the franking impression.

By contrast, in the method according to claim 1 the further, encrypted, text is read from the mail item and, using a procedure which inverts that employed in the franking machine, decrypted data is recovered which is compared with data derived from the plaintext printed on the mail item to check authenticity of the franking impression.

The board accepts, in line with the respondent's contention, that the base seed word, which in D1 (cf Figure 5) is selected by addressing a ROM (read only memory) 138 in accordance with the last digits of the transaction date and is then combined with further transaction data, including the serial number of the sending station (D1, page 8, lines 14 and 15), to form a seed word, cannot be regarded as a pseudorandom number in the sense in which this term is used in claim 1.

The board is persuaded of the correctness of the respondent’s submission that the opposed patent uses the term "pseudorandom number" in the sense in which it is conventionally used in the computer art. This accords with the definition given in the authoritative Webster’s Third New International Dictionary (1981): "Pseudorandom - being or involving entities (as numbers) that are selected by a definite computational process (as one involving a computer) but that satisfy one or more standard tests for statistical randomness."

The significance of the prefix "pseudo" is to distinguish such a sequence of numbers from a truly random sequence which, as was agreed in the oral debate, necessarily involves a real world input. The appellant’s citation of von Neumann’s celebrated remark "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." is apt in this regard.

The numbers generated as the output of ROM 138 in D1 are not produced by an algorithm or computational process in the above sense. They are a sequence of 1 out of 8 selections made by addressing the ROM in accordance with the three least significant bits of the data relating to one or more real world parameters such as the date, the fee, the serial number of the sending station, the count of mailpieces (D1, paragraph bridging pages 30 to 31).

This view is consistent with the output of ROM 138 being designated a base seed word, its further combination by modulo-2 addition with real world parameters (D1, Figure 5) resulting in the seed word proper which forms an input to the feedback shift register 130. Although the operation of the latter is referred to in D1 as encryption it would more conventionally be referred to as generation of a pseudorandom number using the algorithm represented by the feedback connections of the feedback shift register and using the value of LOAD as a seed.

Despite a certain analogy, the board is not persuaded by the appellant's equation of the dependence of the seed number on the franking machine serial number in D1 and the dependence of the decryption key on the franking machine identification data in the method specified in claim 1.

Hence, in the boards' view, the claim 1 method differs from that disclosed in D1 in the following respects:

(i) the use of a pseudorandom number in the strict sense of this term of art as an input to a key-based encryption process;

(ii) the use of a decryption procedure at the postal authority location which inverts rather than duplicates the encryption procedure used in the franking machine;

(iii) validity comparison of a recovered, ie decryptedplaintext pseudorandom number with a locally generated pseudorandom number rather than comparison of encrypted non-pseudorandom seed numbers;

(iv) use of **key-based** invertible encryption rather than one-way encryption;

(v) use of a decryption key specific to the franking machine selected from a record of decryption keys.

3.2 Objective technical problem

Relative to the closest prior art the objective technical problem addressed and plausibly solved by the method of claim 1 is to provide enhanced security, ie to make fraudulent franking more readily detectable.

3.3 Solution

Starting from the closest prior art D1, the above problem is solved according to the method specified in claim 1 by replacing what is described in D1 as encrypting a seed number, ie the loading of a base seed number as combined or mixed with transaction data to form a seed number into a feedback shift register to produce a uniquely determined output which is a complex function of the input, by an invertible key-based encryption of a pseudorandom number, the matching decryption key - specific to the franking machine - being available at the postal authority location. The other differences listed at 3.1 above are consequential on this change.

3.4 Obviousness

The board is not persuaded by the appellant's contention that comparison of encrypted text following a duplicated encryption and comparison of plaintext following decryption are obvious alternative approaches which the person skilled in the art would select from using common general knowledge in the art and thus arrive at the claimed invention by simple variation of the D1 teaching. In the judgement of the board, D1 cannot fairly be said to suggest decryption, let alone decryption based on a key specific to the franking machine. The parties expressed opposite views on the invertibility of the so-called encryption step in D1. The board is more persuaded by the respondent's view that it is not, at least not easily, invertible, and there is certainly no hint in D1 that it could or should be inverted. It would be entirely consistent with the approach taken in D1 that the so-called encryption step should be a one-way function whose inversion is computationally infeasible since the security of the system disclosed would be compromised by such inversion if it could be used to recover the base seed number and/or the transaction data. On the other hand if it were invertible only to the point of recovering the seed number this could not be used to make any validating comparison with data on the mail item in the context of the D1 system. As the board reads D1, the security it provides is based on a scrambling of the base seed number and the transaction data to produce a unique resultant code number, which scrambling is, for practical purposes, intended to be irreversible.

The fact that the seed number generated in D1 involves, *inter alia*, the franking machine serial number is, in the judgement of the board, only weakly analogous to the decryption key being selected in accordance with the franking machine identification data as specified in claim 1. The purpose served in D1 is to ensure that the seed number is a function of the franking machine serial number; it is not even used to modulate the so-called encryption of this seed number in the following encryption step, much less used in a decryption step.

As regards the argument based on a combination of D1 and D4, the board notes that D4 (page 3, lines 68 to 74) emphasises the contrast between an encryption/decryption scheme as taught therein and a duplicated encryption scheme involving seed numbers (as taught in D1). In the judgement of the board this teaches away from any idea of combining features of the two schemes by encrypting/decrypting pseudorandom numbers relating to transaction data (as in the opposed claim 1) rather than encrypting/decrypting only raw transaction data (as in D4). Furthermore, although D4 mentions key-based encryption at page 2, lines 8 to 12, there is no mention of the decryption key being selected at the postal authority location in accordance with franking machine identification data. The board accepts the appellant's contention that, in general terms, the superior security of key-based encryption/decryption as compared to the use of a dedicated complex algorithm, such as that implemented by the feedback shift register of D1 operating on a seed number to produce an output sequence, was common general knowledge in the cryptographic art before the priority date of the opposed patent(notoriously for electromechanical telegraph ciphers since the promulgation of Kerchoffs’ principle in 1883, and for computer implemented cryptography at least since the publication of standards such as DES and RSA mentioned in D4 at page 2, lines 69 to 72 and alluded to in D1 at page 31, lines 22 to 24). However, the board judges that it would be an analysis and judgement based on hindsight to conclude that the person skilled in the art, starting from D1 and addressing the relevant objective technical problem, would selectively combine part of the encryption/decryption scheme of D4, ignoring the fact that there raw transaction data is encrypted/decrypted, with a selected part of D1 relating to generation of seed numbers related to transaction data. The ingredients are arguably present in the two documents, but, in the judgement of the board, an inventive step was involved in selecting and combining them to arrive at the subject-matter of opposed claim 1 which involves the key-based encryption/decryption of a pseudorandom number related to transaction data, the key being specific to the franking machine.

4. The board concludes therefore that, having regard to the prior art on file, the claimed franking method is not obvious for the person skilled in the art so that the subject-matter of claim 1 is regarded as involving an inventive step within the meaning of Article 56 EPC. The above arguments and conclusion apply analogously to the apparatus claim 13.

5. In the view of the board, the patent in the version approved by the opposition division and the invention to which it relates meet the requirements of the EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

M. Hörnell R.G. O’Connell