Internal distribution code:

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

Datasheet for the decision of 18 March 2016

Case Number: T 0698/12 - 3.5.03

Application Number: 06013441.8

Publication Number: 1873671

IPC: H04L29/00

Language of the proceedings: EN

Title of invention:
A method for protecting IC Cards against power analysis attacks

Patent Proprietor:
Incard SA

Opponent:
Giesecke & Devrient GmbH

Headword:
Protecting IC Cards against power analysis attacks/INCARD

Relevant legal provisions:
EPC Art. 56, 84, 123(2)

Keyword:
Clarity (yes)
Added subject-matter (no)
Inventive step (yes; following amendment)

Decisions cited:
G 0003/14, T 1018/02

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: T 0698/12 - 3.5.03

D E C I S I O N
of Technical Board of Appeal 3.5.03
of 18 March 2016

Appellant: (Opponent)	Giesecke & Devrient GmbH Prinzregentenstrasse 159 81677 München (DE)
Respondent: (Patent Proprietor)	Incard SA 39, Chemin du Champ des Filles 1204 Plan-Les-Ouates (Geneva) (CH)
Representative:	Bosotti, Luciano Buzzi, Notaro & Antonielli d'Oulx Via Maria Vittoria, 18 10123 Torino (IT)
Decision under appeal:	**Interlocutory decision of the Opposition Division of the European Patent Office posted on 26 January 2012 concerning maintenance of the European Patent No. 1873671 in amended form.**

Composition of the Board:

Chairman	F. van der Voort
Members:	T. Snell
	S. Fernández de Córdoba

Summary of Facts and Submissions

I. This appeal was lodged by the opponent against the interlocutory decision of the opposition division that European patent No. 1 873 671 as amended in accordance with the main request met the requirements of the EPC. In substance, the decision concludes that claim 1 as amended complies with Article 123(3) EPC and that its subject-matter involves an inventive step with respect to the documents cited by the opponent, in particular D4.

II. The following documents are relevant to this decision:

D1: DE 199 36 939 A; and
D4: WO 03/039065 A.

III. In the statement of grounds of appeal, the appellant argued that claims 1 and 7 did not comply with Articles 123(2) and (3) EPC, and that the subject-matter of claims 1 and 7 respectively did not involve an inventive step with respect to the combination of documents D4 and D1.

IV. In a reply to the statement of grounds, the respondent (proprietor) contested these arguments.

V. In a communication accompanying a summons to oral proceedings, the board raised objections concerned with Article 84 EPC, Articles 123(2) and (3) EPC and Article 52(1) in combination with Article 56 EPC.

VI. In a written response before the oral proceedings, the respondent filed claims of a new main request, as well as claims of first to third auxiliary requests.

VII. In a written reply, the appellant indicated that the amendments to claims 1 and 7 of the main request had overcome the issues concerned with Articles 84 and 123(2) EPC, and partially those based on Article 123(3) EPC. However, the objections based on Articles 52(1) and 56 EPC and, partially, those based on Article 123(3) EPC were maintained.

VIII. Oral proceedings were held on 18 March 2016.

At the oral proceedings the respondent withdrew all requests on file and filed a new request as sole request.

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

The respondent requested that the decision under appeal be set aside and that the patent be maintained in amended form on the basis of the claims according to the sole request filed during the oral proceedings.

At the end of the oral proceedings, the chairman announced the board's decision.

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

"Method for protecting data against power analysis attacks, comprising at least a first phase of executing a cryptographic operation (OP) for ciphering said data in corresponding encipher data through a secret key (ESK), comprising at least a second phase of executing an additional cryptographic operation (AOP) for ciphering additional data in corresponding encipher additional data through an additional secret key (ERK), said additional data and said additional secret key

(ERK) being randomly generated so that an execution of said first phase and second phase is undistinguishable by said power analysis attacks,
characterized in that

a sequence of said cryptographic operations (OP) are interleaved by said additional cryptographic operations;

the number and the disposition of said at least second phase of executing said additional cryptographic operations (AOP) between a couple of said at least first phase of executing said cryptographic operations (OP) are randomly managed;

the number and the disposition in the whole ciphering algorithm of said additional cryptographic operations (AOP) interleaving said sequence of said cryptographic operations (OP) are not predetermined but are randomly managed."

Claim 7 reads as follows:

"IC Card comprising a secret key (ESK) for protecting data against power analysis attacks by executing at least a cryptographic operation (OP) enciphering said data in corresponding encipher data, comprising means for generating additional data and additional secret keys (ERK) in order to execute an additional cryptographic operation (AOP) enciphering said additional data in corresponding encipher additional data, said cryptographic operation (OP) and said additional cryptographic operation (AOP) being undistinguishab1e by said power analysis attacks, characterized in that said means provides that

a sequence of said cryptographic operations (OP) are interleaved by said additional cryptographic operations;

the number and the disposition of said at least second phase of executing said additional cryptographic operations (AOP) between a couple of said at least first phase of executing said cryptographic operations (OP) are randomly managed;

the number and the disposition in the whole ciphering algorithm of said additional cryptographic operations (AOP) interleaving said sequence of said cryptographic operations (OP) are not predetermined but are randomly managed."

Reasons for the Decision

1. Introductory remarks

The present patent concerns a method of protecting IC cards against power analysis attacks when carrying out cryptographic operations. Such attacks in general consist of performing an analysis of power consumption when the cryptographic algorithm is run a great number of times (cf. paragraph [0008] and [0009]). In order to combat such attacks, the patent describes a method based on interleaving additional cryptographic operations ("AOPs") randomly within the sequence of true cryptographic operations ("OPs").

2. Claim 1 - interpretation and compliance with Articles 84, 123(2) and 123(3) EPC

2.1 It should first be noted that the appellant did not raise objections based on Articles 84, 123(2) or 123(3) EPC with respect to the request on file. The board has however examined these matters ex officio (Article 114(1) EPC), bearing in mind of course that, in respect of Article 84 EPC, only amendments carried out post grant are to be examined (cf. G 3/14).

2.2 The last two features of claim 1 read as follows:

a) "the number and the disposition of said at least second phase of executing said additional cryptographic operations (AOP) between a couple of said at least first phase of executing said cryptographic operations (OP) are randomly managed;" and

b) "the number and the disposition in the whole ciphering algorithm of said additional cryptographic operations (AOP) interleaving said sequence of said cryptographic operations (OP) are not predetermined but are randomly managed.".

2.3 As claim 1 as amended includes all the features of claim 1 as granted, noting in particular that feature a), which had been modified during the opposition procedure, has been reintroduced in its original wording, its scope is narrower than claim 1 as granted. Consequently, claim 1 now complies with Article 123(3) EPC.

2.4 In order to determine compliance with Articles 84 and 123(2) EPC, features a) and b) require interpretation, both individually and in combination.

2.5 In feature a), the term "between a couple", which is linguistically ambiguous but already present in claim 1

as granted, is understood in the sense of "between any two OPs".

2.6 In feature b), the term "in the whole ciphering algorithm" is understood to mean the algorithm consisting of the total number of OPs and AOPs. Consequently, this feature implies that the total number of AOPs is chosen randomly. This feature is supported by paragraph [0069] as originally filed (referring to the published application EP 1 873 671 A), where it is stated that "the overall processing time T is a random variable depending on how many additional cryptographic operation *[sic]* AOP are included in the whole ciphering algorithm", together with paragraphs [0050] and [0051], from which it follows that the initial number of additional operations n^1_f is a random number. Feature b) also requires that the disposition of the AOPs in the whole ciphering algorithm is randomly managed. This is supported by paragraph [0046] combined with paragraphs [0056] to [0058] of the application as filed, which show that determining whether the next operation, including the first operation, is an OP or an AOP is randomly managed.

2.7 With respect to the presence in claim 1 of two features a) and b) both concerned with random management of the number and disposition of AOPs, the board takes the view that features a) and b) have to be construed in combination as referring to an algorithm for randomly managing the number and disposition of AOPs which has to fulfil two conditions simultaneously. This interpretation is consistent with the description in paragraphs [0048] to [0068] which disclose a single algorithm.

2.8 Although claim 1 could theoretically be construed in other ways which are not disclosed in the application as filed, e.g. by interpreting a) and b) as independent features carried out using separate algorithms, and/or by construing a) and b) as sequential steps of the method, these interpretations make no real sense in the present context, since it would be illogical to carry out step a) independently of knowing the total number and disposition of AOPs determined by step b). In accordance with case law, a claim should not be interpreted in a way which is illogical or does not make sense (cf. e.g. T 1018/02, point 3.8 of the reasons). Consequently, as these alternative (undisclosed) interpretations are technically implausible, there is no infringement of either Article 123(2) EPC (added subject-matter) or Article 84 EPC (clarity).

2.9 It is noted that at the oral proceedings the parties interpreted the claim in the same way as set out above.

2.10 The board concludes that claim 1 complies with Articles 84, 123(2) and 123(3) EPC.

3. Claim 1 - inventive step

3.1 It was not in dispute that document D4 represents the closest prior art.

D4, like the patent, discloses a method of protecting IC cards against power analysis attacks when carrying out cryptographic operations, in this case Data Encryption Standard (DES) operations. In D4, the DES algorithm is repeatedly performed on the same message M, **m** times with a true key K and **n** times with false keys (cf. page 7, lines 8 to 13 and page 8, lines 9 to

15)). The m true operations (equivalent to the operations OP of the present patent) and the n false operations (equivalent to the additional operations AOP of the present patent) are performed in a random order (idem). The sequence of m+n operations may be repeated P times, with a limit being set on the number P (cf. page 10, lines 23 to 27). As a further option, in order to introduce temporal uncertainty, the start of each operation may occur at a random time ("les m+n exécutions débutent chacune à un instant aléatoire"; cf. page 5, lines 12 to 17).

3.2 In one example described on page 10, lines 4 to 22 of D4, m=1, so that each iteration consists of n+1 operations. In the first sequence of n+1 operations, the true operation occurs in third place, in the next iteration, it occurs in first place, and in the Pth iteration, it occurs in second place.

3.3 Using the wording of claim 1, D4 discloses a method for protecting data against power analysis attacks, comprising at least a first phase of executing a cryptographic operation (DES) for ciphering said data in corresponding encipher data through a secret key (K) (cf. page 7, lines 9 to 11), comprising at least a second phase of executing an additional cryptographic operation for ciphering data in corresponding encipher additional data through an additional secret key (K'_1, K'_2 ...K'_n)(cf. page 7, lines 8 to 13), said additional secret key (K'_1, K'_2 ...K'_n) being randomly generated so that an execution of said first phase and second phase is undistinguishable by said power analysis attacks (cf. page 11, lines 3 to 7),
wherein
a sequence of said cryptographic operations are

interleaved by said additional cryptographic operations (cf. page 7, lines 8 to 13); and
the number and the disposition of said at least second phase of executing said additional cryptographic operations between a couple of said at least first phase of executing said cryptographic operations are randomly managed (consider the "couple" consisting of the first two true operations in the example discussed in point 3.2 above; it follows from the random order of true and false operations that both the number and disposition of the false operations between this couple of true operations is randomly managed).

3.4 The subject-matter of claim 1 differs from the disclosure of D4 in that, in accordance with claim 1:

(i) The AOPs operate on randomly generated additional data, whereas in D4, the false operations operate on the message M.

(ii) The number and the disposition in the whole ciphering algorithm of said additional cryptographic operations (AOP) interleaving said sequence of said cryptographic operations (OP) are not predetermined but are randomly managed.

3.5 Re (ii): In D4, the numbers m and n are constant for each repetition of the sequence. D4 neither suggests that the number n of false operations nor the total number of repetitions P may be randomly managed.

3.5.1 The appellant argued that because m and n are constant, D4 described a periodic method which made it vulnerable to a differential power attack by statistical analysis. The problem to be solved was therefore to overcome this drawback. In order to solve this problem, the skilled

person, on the basis of common general knowledge, would modify the number n in a random fashion in order to introduce temporal uncertainty.

3.5.2 However, the board notes that the appellant has produced no evidence that introducing temporal uncertainty by varying a number of operations in random fashion belonged to common general knowledge. Furthermore, D4 already proposes a method of introducing random temporal uncertainty, i.e., as stated above, to start each cryptographic operation at random times. Consequently, the skilled person has no obvious motive to seek an alternative solution. It follows that the skilled person starting out from D4 would not obviously arrive at a method incorporating feature (ii).

3.6 Re (i): The appellant argued that this feature was obvious in view of the combination of D4 with document D1. However, considering that the board has concluded that the subject-matter of claim 1 involves an inventive step already because of the presence of feature (ii), there is no need to decide whether this further feature is obvious or not.

3.7 The board therefore concludes that the subject-matter of claim 1 involves an inventive step (Articles 52(1) and 56 EPC).

4. Claim 7

The same reasoning as given in connection with claim 1 applies, mutatis mutandis, to independent claim 7. This point was not contested by the appellant.

5. Dependent claims 2 to 6

The appellant raised no objections in respect of the dependent claims. The board also sees no reason to raise any objection.

6. Conclusion

For the above reasons, the board concludes that claims 1 to 7 meet the requirements of the EPC. Consequently, the patent can be maintained in amended form on the basis of these claims (cf. Article 101(3)(a) EPC). However, the board has not examined the description for conformity with the new claims, and leaves this task to the opposition division.

Order

For these reasons it is decided that:

- The decision under appeal is set aside.

- The case is remitted to the department of first instance with the order to maintain the patent in amended form on the basis of claims 1 to 7 of the sole request filed during the oral proceedings and a description and drawings to be adapted accordingly.

The Registrar: The Chairman:

G. Rauh F. van der Voort

Decision electronically authenticated